

POLITYKA OCHRONY DANYCH OSOBOWYCH OŚRODEK POMOCY SPOŁECZNEJ W NIEMCACH

ZATWIERDZAM:

Administrator danych	Data	Podpis
Kierownik Ośrodka Pomocy Społecznej w Niemcach	 30.06.2026 r.	KIEROWNIK..... Ośrodka Pomocy Społecznej w Niemcach

mgr Barbara Ścisiel

*Dokument opracowano jako aktualizację dotychczasowej Polityki Ochrony Danych Osobowych OPS
Niemce i jej załączników.*

Metryka dokumentu

Pole	Treść
Nazwa dokumentu	Polityka Ochrony Danych Osobowych Ośrodka Pomocy Społecznej w Niemcach
Właściciel dokumentu	Administrator danych - Ośrodek Pomocy Społecznej w Niemcach, reprezentowany przez Kierownika OPS
Nadzór merytoryczny	Inspektor Ochrony Danych
Wersja	2.0 - projekt aktualizacji
Data wejścia w życie	
Przegląd okresowy	Nie rzadziej niż raz w roku oraz każdorazowo po zmianie procesu, systemu, podstawy prawnej, dostawcy lub po istotnym naruszeniu ochrony danych

Wersja	Data	Zakres zmian	Zatwierdził
1.0	2018/2019	Wdrożenie pierwotnej Polityki i załączników	Kierownik OPS
2.0	03.07.2026	Aktualizacja pod RODO, ustawy sektorowe OPS, DPIA, KRI, powierzenia, naruszenia, upoważnienia i systemy IT	Do zatwierdzenia KIEROWNIK Ośrodka Pomocy Społecznej w Niemcach <i>mgr Barbara Ścisł</i>

I. POSTANOWIENIA OGÓLNE	3
DEKLARACJA I ZASTOSOWANIE.....	3
DEFINICJE.....	4
ZASADY OCHRONY DANYCH.....	6
ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO DANYCH OSOBOWYCH	7
II. OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH	10
III. PRZEDSIĘWZIĘCIA ZABEZPIECZAJĄCE PRZED NARUSZENIEM OCHRONY DANYCH	11
IV. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH.....	13
DZIAŁANIA KORYGUJĄCE I ZAPOBIEGAWCZE	13
ZGŁASZANIE NARUSZEŃ	13
V. DOSTĘP DO DANYCH OSOBOWYCH.....	13
VI. PRAWA PODMIOTÓW DANYCH	14
OPORozUMIENIA I KONTAKTY ZE STRONAMI ZEWNĘTRZNYMI.....	14
VII. REJESTR CZYNNOŚCI.....	15
VIII. BEZPIECZEŃSTWO OSOBOWE	16
ETAP NABORU PRACOWNIKA I WSPÓŁPRACOWNIKA.....	16
EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH.....	16
ZATRUDNIENIE / WSPÓŁPRACA.....	17
ZAKOŃCZENIE ZATRUDNIENIA / WSPÓŁPRACY.....	17
X. POSTANOWIENIA KOŃCOWE	18
XI. SPIS ZAŁĄCZNIKÓW	19

I. POSTANOWIENIA OGÓLNE

§ 1

DEKLARACJA I ZASTOSOWANIE

1. Polityka została opracowana z uwzględnieniem przepisów prawa właściwych dla działalności Ośrodka Pomocy Społecznej, w szczególności: rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO), ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, ustawy z dnia 12 marca 2004 r. o pomocy społecznej, ustawy z dnia 28 listopada 2003 r. o świadczeniach rodzinnych, ustawy o pomocy osobom uprawnionym do alimentów, ustawy o wspieraniu rodziny i systemie pieczy zastępczej, ustawy o przeciwdziałaniu przemocy domowej, ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, ustawy o narodowym zasobie archiwalnym i archiwach, ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz Krajowych Ram Interoperacyjności.
2. Polityka ma zastosowanie do wszystkich procesów przetwarzania danych osobowych realizowanych przez OPS, w tym procesów prowadzonych w systemach teleinformatycznych, systemach centralnych administracji publicznej oraz dokumentacji papierowej.
3. **Celem** niniejszej Polityki bezpieczeństwa danych osobowych (PODO) jest wypełnienie założeń 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, dalej też zwane **RODO**).
4. Stanowi ona zbiór wymogów, zasad i regulacji ochrony danych osobowych u **Administradora danych osobowych**, którym jest Ośrodek Pomocy Społecznej w Niemcach reprezentowany przez Kierownika Ośrodka Pomocy Społecznej w Niemcach, (zwany dalej **ADO**).
5. Zasady, działania, kompetencje i zakresy odpowiedzialności opisane w niniejszej Polityce Ochrony Danych Osobowych (zwana dalej **PODO** lub **Polityka**), obowiązują wszystkich pracowników i współpracowników ADO.
6. Procedury i dokumenty związane z Polityką będą weryfikowane i dostosowywane w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Przeglądy dokumentacji odbywają się nie rzadziej niż raz w roku.
7. Przeglądy dokumentacji odbywają się nie rzadziej niż raz w roku oraz każdorazowo po istotnej zmianie procesu przetwarzania, systemu informatycznego, podstawy prawnej, dostawcy usług, sposobu udostępniania danych, stwierdzeniu poważnego naruszenia ochrony danych lub po wydaniu nowych zaleceń przez organ nadzorczy.
8. Polityka określa środki techniczne i organizacyjne zastosowane przez ADO dla zapewnienia ochrony danych oraz tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia danych w systemie informatycznym lub w kartotekach papierowych, albo w sytuacji podejrzenia o takim naruszeniu.
9. Polityka została opracowana z uwzględnieniem metod i środków ochrony danych, których skuteczność w czasie ich zastosowania jest powszechnie uznawana. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania

właściwej ochrony wraz z zachowaniem ich integralności i rozliczalności, ze szczególnym uwzględnieniem obowiązujących przepisów prawa dotyczących ochrony danych osobowych.

10. Zakres obowiązywania dokumentu.

- 1) Niniejsza Polityka obowiązuje wszystkich pracowników, współpracowników, a także kontrahentów ADO.
- 2) Każdy z pracowników i współpracowników ma obowiązek zapoznania się z treścią niniejszej Polityki.
- 3) Polityka dotyczy wyposażenia, systemów, urządzeń przetwarzających informacje w formie elektronicznej, papierowej lub jakiegokolwiek innej.
- 4) Nieprzestrzeganie postanowień zawartych w Polityce może skutkować sankcjami w pełnym zakresie dopuszczonym przez stosunek pracy oraz obowiązujące przepisy prawa.
- 5) W celu skutecznego zapoznania pracowników i współpracowników z zasadami zawartymi w niniejszej Polityce wprowadza się zestaw reguł stanowiący wyciąg najistotniejszych zapisów zawartych w Polityce. *Instrukcja Zarządzania Systemem Informatycznym* stanowi Załącznik nr 5 do niniejszej Polityki.

- Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest ADO, a za nadzór i monitorowanie jej przestrzegania odpowiada: **Inspektor ochrony danych (dalej IOD).**

§ 2

DEFINICJE

Adekwatność danych – przetwarzanie danych osobowych w zakresie niezbędnym ze względu na cel zbierania danych.

Administrator Danych Osobowych (ADO) – osoba decydująca o celach i środkach przetwarzania danych osobowych.

Anonimizacja danych osobowych – pozbawienie danych osobowych cech pozwalających na identyfikację osób fizycznych, których anonimizowane dane dotyczą.

ASI – Administrator Systemów Informatycznych, osoba wyznaczona do technicznego zarządzania systemami i bezpieczeństwem dostępu do danych.

- **Bezpieczeństwo informacji** – zapewnienie poufności, integralności i dostępności przetwarzanych danych osobowych.

Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Dane szczególnych kategorii – dane, o których mowa w art. 9 RODO, w szczególności dane dotyczące zdrowia, niepełnosprawności, sytuacji socjalnej ujawniającej stan zdrowia, przemocy domowej lub innych okoliczności wymagających szczególnej ochrony.

Dane z art. 10 RODO – dane dotyczące wyroków skazujących, czynów zabronionych lub powiązanych środków bezpieczeństwa, przetwarzane wyłącznie na podstawie przepisów prawa.

Dostępność – gwarancja dostępu do danych osobowych tylko przez osoby upoważnione.

DPIA – ocena skutków dla ochrony danych, wykonywana zgodnie z art. 35 RODO, gdy dany proces może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Hasło dostępu – ciąg znaków, unikalnych dla każdego użytkownika eksploatującego sprzęt komputerowy oraz korzystającego z zasobów informatycznych przetwarzanych i gromadzonych na serwerze lub w programie sieci informatycznej.

Incydent – każde zdarzenie lub seria zdarzeń, nie będące częścią normalnego działania systemu, mogące zakłócić przetwarzanie danych lub grozić bezpieczeństwu przetwarzania danych.

Instrukcja Zarządzania – Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany (przez osoby nieupoważnione).

Login (identyfikator) – ciąg znaków alfanumerycznych, unikalnych dla każdego użytkownika korzystającego z zasobów informatycznych przetwarzanych i gromadzonych na serwerze lub w programie sieci informatycznej.

Organ nadzorczy – Prezes Urzędu Ochrony Danych Osobowych.

Osoba upoważniona – osoba posiadająca upoważnienie wydane przez ADO lub osobę przez niego umocowaną i dopuszczona jako Użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu.

Osoba nieupoważniona – osoba nie posiadająca upoważnienia do przetworzenia danych osobowych nadanego przez Administratora Danych Osobowych.

Poufność – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym osobom.

Polityka bezpieczeństwa – Polityka bezpieczeństwa danych osobowych obowiązująca u ADO, ustanowiona w niniejszym dokumencie.

Przetwarzanie danych osobowych – jakiejkolwiek operacje wykonywane na danych osobowych takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie czy usuwanie, zwłaszcza te, które wykonuje się w systemach informatycznych.

Rejestr Kategorii Przetwarzania Danych – rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora na podstawie art. 30 ust. 2 RODO.

Rozliczalność – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu, konkretnemu podmiotowi.

Rozporządzenie (RODO) – Rozporządzenie Parlamentu Europejskiego i Rady 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).

Sieć informatyczna – struktura składająca się z serwerów, stacji roboczych, osprzętu sieciowego, połączonych ze sobą za pomocą mediów transmisji w celu wymiany danych lub współdzielenia różnych zasobów.

Stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego, umożliwiający Użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.

System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedura przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

System tradycyjny – zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji, wyposażenia i środków trwałych w celu przetwarzania danych osobowych w formie papierowej.

Teczka ODO – zbiór dokumentów, instrukcji, regulaminów, załączników opisujących sposób przetwarzania i ochrony danych, składający się na politykę ochrony danych osobowych, gromadzonych i nadzorowanych przez IOD.

Ustawa – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000).

Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Usuwanie danych osobowych – niszczenie danych osobowych lub taka ich modyfikacja, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczą.

Użytkownik – osoba obsługująca stanowisko komputerowe w zakresie udzielonych uprawnień.

Zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, mające na celu w szczególności zabezpieczenie danych przed ich udostępnianiem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, zmianą, utratą, uszkodzeniem lub zniszczeniem.

Zbiór danych osobowych – posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Zgoda osoby, której dane dotyczą – oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda taka nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

Zniszczenie – trwałe, fizyczne uszkodzenie nośników danych w stopniu uniemożliwiającym ich późniejsze odtworzenie przez osoby niepowołane przy zastosowaniu powszechnie dostępnych metod.

§ 3

ZASADY OCHRONY DANYCH

System zarządzania ochroną danych osobowych zgodny z wymaganiami niniejszej Polityki działa z poszanowaniem następujących zasad przetwarzania danych osobowych:

- 1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
- 2) rzetelnie i uczciwie (rzetelność);
- 3) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
- 4) w konkretnych celach i nie „na zapas” (minimalizacja);
- 5) nie więcej niż potrzeba (adekwatność);
- 6) z dbałością o prawidłowość danych (prawidłowość);
- 7) nie dłużej niż potrzeba (czasowość);
- 8) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

§ 4

1. W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Jest ona realizowana poprzez: zabezpieczenia fizyczne, zabezpieczenia logiczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu poniższych celów i zapewnić:

- 1) **rozliczalność** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
 - 2) **integralność** – rozumie się przez to właściwość zapewniającą, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
 - 3) **poufność** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
 - 4) **integralność systemu** – rozumiana jako nienaruszalność systemu, niemożność jakiegokolwiek manipulacji, zarówno zamierzonej jak i przypadkowej.
 - 5) **dostępność** – gwarantuje, że osoby, które są upoważnione i którym informacje są potrzebne, mają do nich dostęp w odpowiednim miejscu i czasie.
 - 6) **uwierzytelnienie** - uwiarygodnienie swojej tożsamości względem systemu teleinformatycznego;
 - 7) **autentyczność** - właściwość zapewniająca, że tożsamość podmiotu lub procesu jest taka, jak deklarowana;
3. Cele i strategie bezpieczeństwa:
- 1) zgodność z prawem;
 - 2) ochrona zasobów informacyjnych i innych aktywów;
 - 3) uzyskanie i utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa zasobów, rozumiane jako zapewnienie poufności, integralności i dostępności zasobów oraz zapewnienie rozliczalności podejmowanych działań;
 - 4) zapewnienie ciągłości działania procesów i właściwej reakcji na incydenty;
 - 5) zapewnienie odpowiedniego poziomu wiedzy dotyczącej ochrony danych osobowych wśród pracowników i współpracowników poprzez zapewnienie odpowiednich szkoleń.

§ 5

ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO DANYCH OSOBOWYCH

1. ADO zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez ADO.
2. ADO przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych.
3. Analiza, o której mowa w ustępie 2 niniejszego paragrafu polega na ocenie ryzyka (R) definiowanego jako iloczyn prawdopodobieństwa zaistnienia incydentu naruszenia ochrony danych osobowych (P) oraz skutków takiego naruszenia (S).
4. Przyjmuje się 5 stopniową skalę prawdopodobieństwa zaistnienia incydentu naruszenia ochrony danych osobowych:

Poziom	Opis	Częstotliwość występowania
1	Prawie niemożliwe	raz na 100 lat
2	Mało prawdopodobne	raz na 10 lat
3	Umiarkowanie możliwe	raz na 5 lat
4	Prawdopodobne	raz na rok
5	Prawie pewne	raz na miesiąc

5. Przyjmuje się 5 stopniową skalę skutków zaistnienia incydentu naruszenia ochrony danych osobowych:

Poziom	Skutek	Opis
1	Minimalny, pomijalny	Niski wpływ na naruszenie uprawnień osoby fizycznej
2	Mało znaczący, niski	Niewielki wpływ na naruszenie uprawnień osoby fizycznej
3	Znaczący, umiarkowany	Znaczący wpływ na naruszenie uprawnień osoby fizycznej
4	Poważny, wysoki	Poważny wpływ na naruszenie uprawnień osoby fizycznej
5	Katastrofalny, krytyczny	Krytyczny wpływ na naruszenie uprawnień osoby fizycznej

6. Przyjmuje się 5 stopniową skalę ryzyka naruszenia ochrony danych osobowych:

Wartość	Rodzaj ryzyka	Opis
25	Krytyczne	Konieczna natychmiastowa poprawa, należy rozważyć wstrzymanie procesu
10-20	Nieakceptowalne	Konieczne niezwłoczne podjęcie działań obniżających ryzyko
5-10	Akceptowalne warunkowo	W miarę możliwości należy podjąć działania zmniejszające ryzyko
2-4	Akceptowalne	Nie ma konieczności podejmowania działań zmniejszających ryzyko, ale należy je regularnie monitorować
1	Pomijalne	Nie ma konieczności podejmowania jakichkolwiek działań

7. Akceptowalny poziom ryzyka ustala się jako wartość nieprzekraczającą 10 punktów.
8. Analiza ryzyka jest dokumentowana dla poszczególnych czynności lub grup czynności przetwarzania, w szczególności dla procesów obejmujących dane o zdrowiu,

niepełnosprawności, przemocy domowej, sytuacji rodzinnej i majątkowej, dane dzieci oraz dane przetwarzane w systemach centralnych lub przez podmioty zewnętrzne.

9. Dla ryzyk ocenionych jako nieakceptowalne lub krytyczne Administrator wyznacza działania obniżające ryzyko, osobę odpowiedzialną i termin realizacji. Wykonanie działań podlega weryfikacji przez Administratora albo osobę przez niego wyznaczoną, przy udziale IOD.
10. Za bezpieczeństwo danych osobowych u ADO odpowiedzialni są wszyscy pracownicy. W szczególności odpowiadają oni za przestrzeganie zasad bezpieczeństwa wynikających z niniejszej Polityki oraz zgłaszanie incydentów i naruszeń, a także wykonywanie zaleceń IOD.
11. We wszystkich umowach, które mogą dotyczyć przetwarzania danych u ADO, należy uwzględnić zapisy zobowiązujące drugą stronę do przestrzegania art. 28 RODO oraz obowiązujących przepisów krajowych.
12. Inspektor ochrony danych prowadzi rejestr podmiotów zewnętrznych, z którymi realizacja umów/porozumień/zamówień lub aneksów do nich zobowiązuje lub umożliwia zleceniobiorcy/wykonawcy dostęp do informacji zawierających dane osobowe.
13. Za przestrzeganie zasad ochrony danych osobowych i za codzienną ochronę danych odpowiedzialni są upoważnieni użytkownicy.

§ 6

1. Realizację zamierzeń określonych w § 3 powinny zagwarantować następujące założenia:
 - 1) Wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania informacji oraz ich odpowiedzialność za ochronę danych.
 - 2) Przeszkolenie użytkowników w zakresie ochrony danych osobowych.
 - 3) Przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory).
 - 4) Podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń.
 - 5) Okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych.
 - 6) Opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii.
 - 7) Okresowe aktualizowanie Polityki.
 - 8) Identyfikacja zagrożeń i analiza ryzyka.

§ 7

1. Administrator dokonuje oceny, czy planowane lub realizowane operacje przetwarzania mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. W szczególności ocenie podlegają procesy obejmujące dane szczególnych kategorii, dane dzieci, dane dotyczące zdrowia, niepełnosprawności, przemocy domowej, sytuacji rodzinnej, bytowej i majątkowej, a także procesy prowadzone z wykorzystaniem systemów teleinformatycznych, systemów centralnych i integracji z rejestrami publicznymi.

2. Jeżeli z oceny wynika wysokie ryzyko, Administrator przeprowadza ocenę skutków dla ochrony danych zgodnie z art. 35 RODO, po konsultacji z IOD. Wynik DPIA dokumentuje się i przechowuje w Teczce ODO
3. W OPS w pierwszej kolejności kwalifikacji DPIA wymagają procesy: Niebieska Karta/przeciwdziałanie przemocy domowej, pomoc społeczna obejmująca dane o zdrowiu i niepełnosprawności, asystent rodziny, praca z dziećmi i rodziną, dostęp zdalny oraz integracje z systemami centralnymi.

II. OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH

§ 7

Podział zagrożeń:

- 1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
- 2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
- 3) zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

§ 8

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są informacje to głównie:

- 1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;
- 2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy;
- 3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru;
- 4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
- 5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
- 6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych;

- 7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
- 8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie;
- 9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń;
- 10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony informacji - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.;
- 11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.;
- 12) podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane;
- 13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur ochrony danych osobowych (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych, itp.).

§ 9

Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.

III. PRZEDSIĘWZIĘCIA ZABEZPIECZAJĄCE PRZED NARUSZENIEM OCHRONY DANYCH

§ 10

1. Każdy użytkownik – przed dopuszczeniem do przetwarzania danych osobowych podlega przeszkoleniu z przepisów w tym zakresie oraz wynikających z nich zadań i obowiązków.
2. Wszyscy użytkownicy podlegają okresowym szkoleniom.
3. Za organizację szkoleń odpowiedzialny jest Inspektor ochrony danych.

§ 11

1. Dla zapewnienia bezpieczeństwa danych zastosowano następujące **środki organizacyjne**:
 - 1) Dostęp do danych osobowych mogą mieć tylko i wyłącznie użytkownicy posiadający pisemne, imienne upoważnienia nadane przez Administratora Danych.
 - 2) Każdy z pracowników powinien zachować szczególną ostrożność przy przenoszeniu wszelkich nośników z danymi.
 - 3) Należy chronić dane przed wszelkim dostępem do nich osób nieuprawnionych.
 - 4) Pomieszczenia w których są przetwarzane dane osobowe muszą być zamykane na klucz.
 - 5) Dostęp do kluczy posiadają tylko upoważnieni pracownicy.

- 6) Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W wypadku gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie zezwolenia Administratora Danych lub IOD.
 - 7) Dostęp do pomieszczeń w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy.
 - 8) W przypadku pomieszczeń do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganych na wykonanie niezbędnych czynności.
 - 9) Szafy w których przechowywane są dane powinny być zamykane na klucz.
 - 10) Klucze do tych szaf posiadają tylko upoważnieni pracownicy.
 - 11) Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych a następnie powinny być zamykane.
 - 12) Dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych a następnie muszą być chowane do szaf.
2. Dla zapewnienia bezpieczeństwa danych i informacji zastosowano następujące **środki techniczne**:
- 1) Dostęp do komputerów na których są przetwarzane dane mają tylko upoważnieni pracownicy.
 - 2) Monitory komputerów na których przetwarzane są dane są tak ustawione aby osoby nieupoważnione nie miały wglądu w dane.
 - 3) Po zakończeniu pracy komputery przenośne (np. typu notebook) zawierające dane osobowe powinny być zabezpieczone w zamykanych na klucz szafach.
 - 4) W wypadku potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego dane osobowe, lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane.
 - 5) Nie należy udostępniać osobom nieupoważnionym tych komputerów.
 - 6) W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności.
 - 7) Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie) aby nie zostały na nich dane osobowe.
 - 8) W wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) należy taką płytę zniszczyć fizycznie.
 - 9) W przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków.
 - 10) Niezabezpieczonych danych osobowych nie należy przysyłać drogą elektroniczną.
 - 11) Dane osobowe przekazywane elektronicznie powinny być zabezpieczone adekwatnie do ryzyka, w szczególności przez szyfrowanie plików, użycie bezpiecznych kanałów komunikacji, ePUAP/e-Doręczeń lub innych rozwiązań zapewniających poufność i integralność.
 - 12) Dostęp zdalny pracowników, ASI lub dostawców zewnętrznych wymaga zgody Administratora lub osoby upoważnionej, powinien być czasowo ograniczony, zabezpieczony MFA, a czynności serwisowe powinny być dokumentowane.
 - 13) Sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz.

- 14) Błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie.

IV. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH

§ 12

DZIAŁANIA KORYGUJĄCE I ZAPOBIEGAWCZE

Działania korygujące podejmowane są w przypadku wykrycia niezgodności w działalności, bądź nieprawidłowego działania procesu. Przesłanką do podjęcia działań korygujących mogą być wyniki kontroli, audytów, zgłoszenia niezgodności, zdarzenia i incydenty związane z ochroną danych osobowych, zapisy, wyniki badania zadowolenia klientów.

Działania zapobiegawcze mają na celu zapobiec wystąpieniu potencjalnych niezgodności.

§ 13

ZGŁASZANIE NARUSZEŃ

1. ADO stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Prezesowi Urzędu Ochrony Danych Osobowych w terminie 72 godzin od ustalenia naruszenia. *Instrukcja postępowania w przypadku zdarzeń naruszających ochronę danych osobowych* stanowi załącznik nr 10.
2. Każde zgłoszenie wewnętrzne naruszenia albo podejrzenia naruszenia powinno nastąpić niezwłocznie, nie później niż w terminie 2 godzin od zauważenia zdarzenia, do ADO i IOD lub osoby wskazanej w procedurze.
3. Decyzja o zgłoszeniu naruszenia do PUODO, zawiadomieniu osób, których dane dotyczą, albo o braku takiego zgłoszenia wymaga udokumentowania w karcie oceny naruszenia wraz z uzasadnieniem.

V. DOSTĘP DO DANYCH OSOBOWYCH

§ 14

1. Przetwarzanie, w tym udostępnianie danych osobowych jest prawnie dopuszczalne, jeżeli jest niezbędne dla zrealizowania obowiązku wynikającego z przepisu prawa.
2. W przypadku udostępnienia danych osobowych w celach innych niż włączenie do rejestru, administrator danych udostępnia posiadane informacje osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
3. Dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. Podmiot występujący o udostępnienie informacji powinien wskazać podstawę prawną upoważniającą go do otrzymania tych danych albo uzasadnioną potrzebę żądania ich udostępnienia. Tylko w takiej sytuacji można dokonać oceny, czy w określonym przypadku

udostępnienie danych jest prawnie dopuszczalne i czy nie będzie ono stanowiło naruszenia zasad ochrony informacji.

5. Przetwarzanie, w tym udostępnianie danych osobowych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje w celu badań naukowych, dydaktycznych, historycznych oraz statystycznych.
6. Udostępnienie danych może nastąpić jedynie za zgodą Administratora Danych i powinno być odpowiednio udokumentowane.

§ 15

VI. PRAWA PODMIOTÓW DANYCH

1. Każdej osobie, której dane osobowe są przetwarzane przysługuje prawo do kontroli przetwarzania jej danych osobowych, a w szczególności prawo do:
 - 1) uzyskania wyczerpującej informacji, czy jej dane osobowe są przetwarzane oraz do otrzymania informacji o pełnej nazwie i adresie siedziby Administratora Danych;
 - 2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych osobowych;
 - 3) uzyskania informacji, od kiedy są przetwarzane jej dane osobowe, oraz podania w powszechnie zrozumiałej formie treści tych danych;
 - 4) uzyskania informacji o źródle, z którego pochodzą dane osobowe jej dotyczące;
 - 5) uzyskania informacji o sposobie udostępniania danych osobowych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym te dane osobowe są udostępniane;
 - 6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem przepisów prawa albo są już zbędne do realizacji celu, dla którego zostały zebrane.
2. Administrator realizuje prawa osób, których dane dotyczą, zgodnie z art. 12–22 RODO, z uwzględnieniem ograniczeń wynikających z przepisów prawa powszechnie obowiązującego, w szczególności obowiązków archiwizacyjnych, obowiązków prowadzenia postępowań administracyjnych oraz realizacji zadań publicznych OPS.
3. Osobie, której dane dotyczą, przysługuje w szczególności prawo dostępu do danych i otrzymania kopii danych, prawo sprostowania danych, prawo ograniczenia przetwarzania, prawo sprzeciwu w przypadkach, gdy podstawą przetwarzania jest art. 6 ust. 1 lit. e RODO, prawo usunięcia danych w przypadkach przewidzianych RODO oraz prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
4. Żądania osób rejestrowane są w Rejestrze żądań osób, których dane dotyczą. Odpowiedzi udziela się bez zbędnej zwłoki, nie później niż w terminie miesiąca od otrzymania żądania, z możliwością przedłużenia o kolejne dwa miesiące w przypadkach przewidzianych w art. 12 ust. 3 RODO.

§ 16

POROZUMIENIA I KONTAKTY ZE STRONAMI ZEWNĘTRZNYMI.

1. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.
2. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, wiążąc podmiot przetwarzający i administratora, określając przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.
3. Jeżeli realizacja umowy, porozumienia, zamówienia lub usługi wiąże się z przetwarzaniem danych osobowych w imieniu Administratora, zawarcie umowy powierzenia lub innego instrumentu prawnego zgodnego z art. 28 RODO jest obowiązkowe przed rozpoczęciem przetwarzania.
4. Administrator prowadzi i aktualizuje rejestr podmiotów przetwarzających, obejmujący co najmniej: nazwę procesora, zakres i cel powierzenia, kategorie danych i osób, informację o danych szczególnych kategorii, podprocesorów, lokalizację danych, transfer poza EOG, termin zgłaszania naruszeń i datę ostatniej weryfikacji procesora.

VII. REJESTR CZYNNOŚCI

§ 17

1. **Rejestr czynności przetwarzania danych osobowych (RCPDO)** stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli **zasady rozliczalności**.
2. RCP powinien zawierać przy każdej czynności co najmniej: cel przetwarzania, kategorie osób, kategorie danych zwykłych, kategorie danych szczególnych, dane z art. 10 RODO, źródło danych, podstawę prawną RODO, podstawę krajową, systemy i nośniki, odbiorców, procesorów, retencję/JRWA, środki techniczne i organizacyjne oraz informację, czy wymagana jest kwalifikacja DPIA.
3. Inspektor ochrony danych monitoruje prowadzenie Rejestru czynności przetwarzania danych osobowych. Wzór *Rejestru Czynności Przetwarzania Danych* stanowi **załącznik nr 1** do niniejszej Polityki.
4. RCPDO jest na bieżąco aktualizowany przez Inspektora ochrony danych, przy czym co najmniej raz do roku RCPDO jest sporządzany w formie dokumentu i załączany do Teczki ODO.
5. RCPDO zawiera analizę adekwatności środków bezpieczeństwa danych osobowych, o której mowa w § 5 niniejszej Polityki.

VIII. BEZPIECZEŃSTWO OSOBOWE

§ 18

ETAP NABORU PRACOWNIKA I WSPÓŁPRACOWNIKA

1. Do przetwarzania danych osobowych i do dostępu do innych informacji chronionych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych. Administrator danych może wydać pełnomocnictwo do nadawania upoważnień.
2. Wzór *Upoważnienia do przetwarzania danych osobowych wraz z oświadczeniem o zapoznaniu się z Polityką ochrony danych osobowych* stanowi **załącznik nr 8** do niniejszej Polityki. Upoważnienia rejestruje się w *Ewidencji osób upoważnionych do przetwarzania danych osobowych*, stanowiącej **załącznik nr 9** do niniejszej Polityki.
3. Zakres upoważnienia może również być określony w umowie o pracę lub współpracę.
4. Osoba upoważniona zobowiązana jest podpisać oświadczenie lub umowę, która określa odpowiedzialność w zakresie ochrony danych osobowych.
5. Osoby upoważnione do przeprowadzania działań związanych z naborem powinny zwrócić szczególną uwagę na zasady ochrony danych wymienione w § 3 niniejszej Polityki, a także aktualnie obowiązujące przepisy prawa w tym zakresie.

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH

1. Ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona przez Administratora danych. Wzór *Ewidencja osób upoważnionych do przetwarzania danych osobowych* stanowi **załącznik nr 9** do niniejszej Polityki.
2. Ewidencja zawiera:
 - 1) imię i nazwisko użytkownika;
 - 2) datę nadania i ustania upoważnienia;
 - 3) zakres upoważnienia;
 - 4) identyfikator dostępu do systemu informatycznego.
3. Ewidencja użytkowników może być prowadzona w systemie informatycznym.
4. Zmiany dotyczące użytkownika, takie jak:
 - 1) zmiana imienia lub nazwiska;
 - 2) zmiana zakresu upoważnienia,podlegają niezwłocznemu odnotowaniu w ewidencji.
5. Zmiany dotyczące użytkownika, takie jak:
 - 1) rozwiązanie umowy;
 - 2) utrata upoważnienia do przetwarzania danych osobowych;
 - 3) zmiana zakresu obowiązków służbowych skutkująca ustaniem upoważnienia,powodują wyrejestrowanie użytkownika przez ADO w trybie natychmiastowym z ewidencji, zablokowanie identyfikatora oraz unieważnienie hasła tego użytkownika.

6. Osoba odpowiedzialna za sprawy kadrowe, bezpośredni przełożony Użytkownika, odpowiadają za natychmiastowe zgłoszenie do ADO użytkowników, którzy utracili uprawnienia do dostępu do danych osobowych, celem zablokowania im dostępu do systemu informatycznego poprzez zablokowanie identyfikatora i wyrejestrowanie z ewidencji osób upoważnionych.
7. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.

§ 19

ZATRUDNIENIE / WSPÓŁPRACA

1. Pracownicy, współpracownicy, wykonawcy i podwykonawcy powinni być świadomi swoich obowiązków i odpowiedzialności prawnej oraz zagrożeń związanych z bezpieczeństwem informacji. W tym celu należy zapewnić wszystkim zatrudnionym właściwy poziom świadomości poprzez kształcenie i szkolenie z zakresu ochrony danych osobowych, ze szczególnym uwzględnieniem procedur bezpieczeństwa. Dokumentują to:
 - lista obecności ze szkoleń;
 - oświadczenia pracowników;
 - umowy o poufności;
 - posiadane zaświadczenia, dyplomy lub certyfikaty.
2. W przypadku naruszenia zasad ochrony danych osobowych jest uruchamiana odpowiednia procedura postępowania dyscyplinarnego, która powinna być poprzedzona potwierdzeniem naruszenia zasad ochrony danych osobowych i zgromadzeniem materiału dowodowego.
3. Postępowanie dyscyplinarne powinno uwzględniać: rodzaj i wagę naruszenia zasad ochrony danych osobowych, wpływ na procesy biznesowe, przypadek incydentalny czy jest to kolejne naruszenie oraz jakość odbytego przeszkolenia.
4. W przypadku pracy mobilnej i na odległość z wykorzystaniem urządzeń przenośnych zastosowano odpowiednie, dodatkowe środki bezpieczeństwa.
5. Przekazywanie sprzętu i urządzeń służących do przetwarzania danych odbywa się na podstawie protokołów przekazania sprzętu.

§ 20

ZAKOŃCZENIE ZATRUDNIENIA / WSPÓŁPRACY

1. Zakończenie zatrudnienia lub zmiana stanowiska pracy wewnątrz organizacji powinny odbywać się w sposób zorganizowany.
2. Odchodzenie z organizacji lub zmiana stanowiska pracy wiąże się ze zwrotem posiadanego przez pracownika sprzętu i odebraniem lub zmianą praw dostępu.
3. Zakończenie zatrudnienia, współpracy lub zmiana stanowiska wymaga: odebrania sprzętu i nośników, zablokowania kont, odebrania dostępów do systemów lokalnych i centralnych, odebrania dostępów pocztowych i zdalnych, rozliczenia dokumentacji papierowej oraz odnotowania daty odebrania uprawnień w ewidencji osób upoważnionych.

X. POSTANOWIENIA KOŃCOWE

§ 21

1. Do stosowania zasad określonych przez dokumenty Polityki zobowiązani są wszyscy pracownicy w rozumieniu przepisów Kodeksu Pracy i inne osoby mające dostęp do informacji podlegającej ochronie.
2. Z treścią niniejszego dokumentu powinni zapoznać się wszyscy pracownicy i inne osoby mające dostęp do informacji przetwarzanej u ADO, przed przystąpieniem do przetwarzania danych.
3. Niniejszy dokument może być przedstawiany podmiotom i jednostkom współpracującym z którymi współpraca może skutkować możliwością dostępu do informacji chronionych.
4. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne lub porządkowe.
5. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym IOD.
6. W przypadku naruszenia postanowień Polityki pracownik, który dopuścił się takiego naruszenia lub przyczynił do niego (umyślnie lub nieumyślnie), może zostać ukarany zgodnie z obowiązującym regulaminem pracy, obowiązującymi przepisami prawa z zakresu ochrony danych osobowych, a w skrajnych przypadkach pociągnięty do odpowiedzialności karnej.
7. Umyślne lub nieumyślne naruszenie postanowień Polityki lub niestosowanie się do poleceń służbowych w tym zakresie może być potraktowane jako naruszenie obowiązków pracowniczych.

§ 22

1. Polityka jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.
2. Użytkownicy są zobowiązani zapoznać się z treścią Polityki.
3. Użytkownik zobowiązany jest złożyć oświadczenie o tym, iż został zaznajomiony z przepisami i zasadami z zakresu ochrony danych osobowych, z niniejszą Polityką, a także zobowiązać się do ich przestrzegania.
4. Wzór *Upoważnienie do przetwarzania danych osobowych wraz z oświadczeniem o zapoznaniu się z Polityką ochrony danych osobowych* potwierdzającego zaznajomienie

użytkownika z przepisami w zakresie ochrony danych osobowych oraz Polityką ochrony danych osobowych obowiązującą u Administratora Danych, a także o zobowiązaniu się do jej przestrzegania, stanowi **załącznik nr 8** do niniejszej Polityki.

5. Oświadczenia przechowywane są w aktach osobowych.

§ 23

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie aktualnie obowiązujące przepisy prawa w zakresie ochrony danych osobowych, szczególnie RODO i ustawa o ochronie danych osobowych.
2. Użytkownicy zobowiązani są do bezwzględnego stosowania postanowień zawartych w niniejszej Polityce. W wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących u Administratora Danych, użytkownicy mają obowiązek stosowania unormowań dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.

XI. SPIS ZAŁĄCZNIKÓW

1. Wzór Rejestru Czynności Przetwarzania Danych.
2. Wzór Rejestru Kategorii Przetwarzania Danych.
3. Wzór Rejestru Naruszeń Ochrony Danych.
4. Wzór Wykazu podmiotów, którym powierzono przetwarzanie danych osobowych.
5. Instrukcja Zarządzania Systemem Informatycznym.
6. Klauzula informacyjna o przetwarzaniu danych.
7. Wzór Umowy powierzenia przetwarzania danych osobowych.
8. Upoważnienie do przetwarzania danych osobowych wraz z oświadczeniem o zapoznaniu się z Polityką ochrony danych osobowych.
9. Ewidencja osób upoważnionych do przetwarzania danych osobowych.
10. Instrukcja postępowania w przypadku zdarzeń naruszających ochronę danych osobowych.

KIEROWNIK
Ośrodka Pomocy Społecznej
w Niemcach
mgr Barbara Ścisiel

ZAŁĄCZNIK NR 1 - Wzór Rejestru Czynności Przetwarzania Danych

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
LP.	Nazwa czynności przetwarzania	Cel przetwarzania	Kategorie osób	Kategorie danych	Podstawa prawna	Planowany termin usunięcia kategorii danych (jeżeli jest to możliwe)	Nazwa administratora i dane kontaktowe (jeżeli dotyczy)	Nazwa podmiotu przetwarzającego i dane kontaktowe (jeżeli dotyczy)	Kategorie odbiorców (innych niż podmiot przetwarzający) (jeżeli jest to możliwe)	Ogólny opis technicznych środków bezpieczeństwa zgodnie z art. 32 ust. 1 (jeżeli jest to możliwe)	Prawdopodobieństwo zaistnienia incydentu naruszenia ochrony danych osobowych	Skutki zaistnienia incydentu naruszenia danych osobowych	Ryzyko naruszenia uprawnień osób fizycznych	DPIA (jeżeli tak, lokalizacja raportu)	Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Jeżeli transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Art. 30 ust. 1 pkt e	Art. 30 ust. 1 pkt e
		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									

ZAŁĄCZNIK NR 2 - Wzór Rejestru Kategorii Przetwarzania Danych

Rejestr kategorii czynności przetwarzania (art. 30 ust. 2 RODO) dotyczy przetwarzania dokonywanego w imieniu innego administratora (rola podmiotu przetwarzającego). Ośrodek Pomocy Społecznej w Niemcach działa co do zasady jako administrator — na dzień rejestr pozostaje niewypełniony (nie dotyczy). Rejestr zostanie wypełniony, jeżeli OPS przyjmie dane do przetwarzania w powierzeniu.

	1	2	3	4	5	6	7	8	9	10	11
LP.	Kategorie przetwarzania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	Administrator			Inspektor ochrony danych administratora (jeżeli powołano)	Czas trwania przetwarzania	Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na	Podprzetwarzający	
			Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe współadministratora (jeżeli dotyczy)	Nazwa i dane kontaktowe przedstawiciela administratora (jeżeli wyznaczono)					Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy)	Kategorie podpowierzonych przetwarzanych
	Art. 30 ust. 2 lit. b	Art. 30 ust. 2 lit. d, art. 32 ust. 1	Art. 30 ust. 2 lit. a					Art. 30 ust. 2 lit. c	Art. 30 ust. 2 lit. c		

11

ZAŁĄCZNIK NR 4 - Wzór Wykazu podmiotów, którym powierzono przetwarzanie danych osobowych

Wykaz podmiotów, z którymi zawarto umowy powierzenia przetwarzania danych

L p.	Nazwa podmiotu, któremu powierzono dane	Nr umowy powierzenia	Czas trwania powierzenia	Cel i charakter powierzenia	Rodzaj danych osobowych (zwykle/wrażliwe)	Kategorie osób, których dane dotyczą
---------	---	-------------------------	--------------------------------	--------------------------------	--	--

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

SPIS TREŚCI

- I. Cel instrukcji.
- II. Definicje.
- III. Poziom bezpieczeństwa.
- IV. Metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem.
- V. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkownika systemu.
- VI. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.
- VII. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz przed wirusami komputerowymi.
- VIII. Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiami danych osobowych.
- IX. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.
- X. Naprawa komputerów z danymi osobowymi.
- XI. Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego.
- XII. Postanowienia końcowe.

I. CEL INSTRUKCJI

1. Instrukcja Zarządzania systemem informatycznym, zwana dalej Instrukcją, określa sposób zarządzania systemem informatycznym wykorzystywanym do przetwarzania danych osobowych przez Administratora Danych Osobowych w celu zabezpieczenia danych przed zagrożeniami, w szczególności przed ich udostępnianiem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Instrukcja opisuje nadawanie uprawnień użytkownikom, określa sposoby pracy w systemie informatycznym oraz czynności wpływające na zapewnienie bezpieczeństwa systemu informatycznego.
3. Instrukcja ma zastosowanie w szczególności do następujących systemów, usług i zasobów wykorzystywanych w OPS:
 - a. systemy dziedzinowe pomocy społecznej i świadczeń;
 - b. systemy centralne i rejestry publiczne, oraz inne systemy wykorzystywane przy realizacji zadań ustawowych;
 - c. systemy kadrowo-płacowe i finansowo-księgowe;
 - d. poczta elektroniczna, system obiegu korespondencji, ePUAP, e-Doręczenia, jeżeli są wykorzystywane;
 - e. serwery, stacje robocze, komputery przenośne, urządzenia mobilne, nośniki danych, system kopii zapasowych, system antywirusowy/EDR, zaporą sieciową oraz systemy zdalnego dostępu.

II. DEFINICJE

Niniejsza Instrukcja posługuje się terminami zdefiniowanymi w Polityce Bezpieczeństwa.

III. POZIOM BEZPIECZEŃSTWA

1. Mając na uwadze kategorie danych osobowych przetwarzanych w OPS, w tym dane szczególnych kategorii oraz dane przetwarzane w systemach połączonych z siecią publiczną lub systemami centralnymi administracji publicznej, Administrator stosuje środki techniczne i organizacyjne adekwatne do ryzyka naruszenia praw lub wolności osób fizycznych, zgodnie z art. 24, art. 25 i art. 32 RODO oraz wymaganiami Krajowych Ram Interoperacyjności.
2. Każdy z użytkowników systemu przed przystąpieniem do przetwarzania danych zobowiązany jest do zapoznania się z:
 - a. Ustawą;
 - b. Polityką Bezpieczeństwa;
 - c. Niniejszą Instrukcją.

3. Każdy z użytkowników systemu posiada upoważnienie do przetwarzania danych osobowych.
4. ADO przyznaje użytkownikom uprawnienia w zakresie dostępu do systemu informatycznego.

IV.

METODY I ŚRODKI UWIERZYTELNIANIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZRZĄDZANIEM I UŻYTKOWANIEM SYSTEMU

1. Rejestracja użytkownika polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.
2. Wyrejestrowanie następuje przez zablokowanie konta użytkownika lub usunięcie danych użytkownika z bazy użytkowników systemu.
3. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych zostaje niezwłocznie wyrejestrowany z systemu informatycznego, a hasło unieważnione.
4. Identyfikator składa się z co najmniej 2 znaków.
5. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
6. W systemie stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.
7. Bezpośredni dostęp do systemu informatycznego może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
8. Hasło użytkownika należy wprowadzać w sposób uniemożliwiający innym osobom jego poznanie.
9. Hasło powinno składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry.
10. Hasło nie może być tożsame z identyfikatorem użytkownika, jego imieniem, nazwiskiem lub numerem PESEL, numerem telefonu użytkownika, imionami osób z najbliższej rodziny, numerem rejestracyjnym samochodu użytkownika, jak również nie może stanowić przewidywanych sekwencji z klawiatury.
11. Nie należy korzystać z opcji zapamiętywania hasła w systemie.
12. W przypadku złamania poufności hasła, użytkownik zobowiązany jest zmienić hasło i poinformować o tym fakcie ADO.
13. Dostęp do kont administracyjnych, poczty elektronicznej, VPN, systemów zdalnego dostępu oraz systemów przetwarzających dane szczególnych kategorii powinien być zabezpieczony uwierzytelnianiem wieloskładnikowym, jeżeli system technicznie to umożliwia.
14. Konta administracyjne oraz konta o podwyższonych uprawnieniach są kontami imiennymi. Korzystanie z kont współdzielonych jest dopuszczalne wyłącznie wtedy, gdy ograniczenia techniczne systemu uniemożliwiają stosowanie kont imiennych. W takim przypadku należy prowadzić ewidencję osób znających dane dostępowe oraz dokumentować użycie konta.

15. Uprawnienia użytkowników i administratorów podlegają przeglądowi nie rzadziej niż raz na 6 miesięcy oraz każdorazowo po zmianie stanowiska, zakończeniu zatrudnienia lub współpracy albo zmianie zakresu obowiązków.
16. Zabrania się udostępniania loginów i haseł innym osobom, zapisywania ich w miejscach widocznych lub przechowywania w sposób umożliwiający dostęp osobom nieupoważnionym.

V.

PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU

1. Rozpoczęcie pracy na stacji roboczej następuje po włączeniu komputera, a następnie wprowadzeniu identyfikatora indywidualnego oraz hasła znanego jedynie użytkownikowi.
2. W pomieszczeniu, w którym przetwarzane są dane osobowe, osoby nieupoważnione do przetwarzania danych mogą znajdować się jedynie za zgodą i w obecności użytkownika lub ADO.
3. Przed osobami nieupoważnionymi należy chronić ekrany komputerów, wydruki leżące na biurkach oraz w otwartych szafach.
4. Monitory komputerów wyposażone są w wygaszacze ekrany, włączające się w odpowiednim czasie do przerywania pracy. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu odpowiedniego hasła.
5. W przypadku opuszczenia stanowiska pracy użytkownik ma obowiązek wylogować się z systemu, dezaktywizować lub zablokować stację roboczą.
6. Niedozwolone jest wykonywanie kopii zbiorów danych. Mogą być one kopiowane przez ADO lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych.
7. Jednostkowe dane osobowe mogą być przekazywane drogą elektroniczną wyłącznie w zakresie niezbędnym do realizacji zadania i przy zastosowaniu zabezpieczeń adekwatnych do ryzyka, w szczególności przez szyfrowanie plików, przekazanie hasła innym kanałem komunikacji, użycie ePUAP, e-Doręczeń lub innego bezpiecznego kanału zapewniającego poufność i integralność danych.
8. Niedozwolone jest wynoszenie na jakichkolwiek nośnikach całych zbiorów danych, także w postaci zaszyfrowanej.
9. Zakazana jest samodzielna modernizacja oprogramowania, wgrywanie przez użytkownika własnych programów lub aplikacji bez zgody ADO.
10. Zakończenie pracy na stacji roboczej następuje po wprowadzeniu danych, a następnie prawidłowym zamknięciu aplikacji oraz wylogowaniu się użytkownika i wyłączeniu komputera.
11. Przed opuszczeniem miejsca pracy użytkownik ma obowiązek:
 - a. zniszczyć w niszczarce lub schować do zamykanych szaf wszelkie wydruki zawierające dane osobowe;
 - b. schować do zamykanych szaf akta zawierające dane osobowe;
 - c. umieścić klucze do szaf w ustalonym miejscu;
 - d. zamknąć okna;

- e. powziąć inne środki zapewniające maksymalny poziom zabezpieczenia przed nieuprawnionym ujawnieniem danych osobowych.
12. Ostatni użytkownik opuszczając miejsce pracy ma obowiązek zamknięcia drzwi wyjściowych na klucz i włączenia systemu alarmowego.
13. Podczas przetwarzania danych osobowych na komputerach przenośnych użytkownik powinien zachować szczególną ostrożność, a ponadto:
- a. podczas transportu, przechowywania i użytkowania komputera przenośnego konieczne jest zachowanie szczególnej ostrożności;
 - b. dane osobowe zlokalizowane na dyskach komputerów przenośnych podlegają ochronie kryptograficznej;
 - c. pozostawienie komputera przenośnego bez nadzoru w samochodzie, przechowalni bagażu itp. jest niedozwolone;
 - d. korzystający z komputera przenośnego zobowiązany jest do takiego użytkowania, aby uniemożliwić wgląd w wyświetlane na monitorze dane przez osoby nieupoważnione;
 - e. udostępnianie komputera przenośnego osobom nieupoważnionym jest zabronione.

VI.

SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

- 1. Dane osobowe w postaci elektronicznej zapisywane na nośnikach (płyty CD, pendrive) mogą być wnoszone poza siedzibę ich przechowywania tylko w uzasadnionych przypadkach za zgodą ADO.
- 2. Nie należy przechowywać zbędnych nośników informacji zawierających dane osobowe.
- 3. Po upływie okresu ich użyteczności lub przechowywania, dane osobowe są kasowane lub niszczone tak, aby nie było możliwe ich odczytanie, zrekonstruowanie lub odzyskanie danych.
- 4. Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika.
- 5. W przypadku kopii zapasowych sporządzanych przez użytkownika, odpowiedzialny za zniszczenie jest użytkownik.
- 6. Informatyczne nośniki zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, niszczy się w sposób mechaniczny uniemożliwiający ich odczytywanie.
- 7. Informatyczne nośniki zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych.
- 8. Informatyczne nośniki zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.

9. Zakazane jest przetwarzanie danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą elektroniczną bez uprzedniego zaszyfrowania.
10. Przed posługiwaniem się nośnikiem danych pochodzącym od innego podmiotu, użytkownik zobowiązany jest do sprawdzenia go programem antywirusowym na swojej stacji roboczej.
11. Nośniki przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych osobowych.
12. Podmiot, któremu powierzono przetwarzanie danych osobowych, podejmuje wszelkie niezbędne i wymagane przez Ustawę i Rozporządzenie działania.
13. Dla systemów przetwarzających dane osobowe wykonuje się kopie zapasowe zgodnie z harmonogramem zatwierdzonym przez Administratora lub osobę przez niego upoważnioną.
14. Harmonogram kopii zapasowych określa co najmniej: nazwę systemu, zakres kopii, częstotliwość wykonywania kopii, miejsce przechowywania, okres retencji, sposób zabezpieczenia kopii, osobę odpowiedzialną oraz sposób kontroli poprawności wykonania kopii.
15. Kopie zapasowe zawierające dane osobowe powinny być zabezpieczone przed dostępem osób nieupoważnionych, w szczególności przez kontrolę dostępu, szyfrowanie lub inne środki adekwatne do ryzyka.
16. Test odtworzenia danych z kopii zapasowej przeprowadza się nie rzadziej niż raz w roku oraz po istotnych zmianach systemu informatycznego. Wynik testu dokumentuje się protokołem.
17. Kopie zapasowe usuwa się po upływie okresu retencji w sposób uniemożliwiający odtworzenie danych, chyba że przepisy prawa lub potrzeba zabezpieczenia dowodów wymagają ich dłuższego przechowywania.

VII.

SPOSÓB ZABEZPIECZENIEA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO ORAZ PRZED WIRUSAMI KOMPUTEROWYMI

1. Każda stacja robocza posiada zainstalowane oprogramowanie antywirusowe.
2. Aktualizacja programów antywirusowych następuje nie rzadziej niż raz w tygodniu.
3. Zabrania się używania nośników niewiadomego pochodzenia bez uprzedniego sprawdzenia ich programem antywirusowym przez użytkownika, który zamierza z danego nośnika skorzystać.
4. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia bez uprzedniego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który zamierza pobrać plik.
5. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pocztę otrzymał.

6. Zabrania się wyłączania, blokowania, odinstalowywania programów zabezpieczających stację roboczą przed oprogramowaniem złośliwym lub nieautoryzowanym dostępem (skaner antywirusowy, firewall).
7. Aktualizacja oprogramowania zabezpieczającego, w tym systemu antywirusowego/EDR oraz jego sygnatur, następuje automatycznie, o ile system technicznie to umożliwia. W przypadku braku możliwości automatycznej aktualizacji aktualizacje wykonuje się niezwłocznie po ich udostępnieniu, nie rzadziej niż raz w tygodniu.
8. ADO przeprowadza cykliczne kontrole antywirusowe na wszystkich stacjach roboczych.
9. ADO lub ASI zapewnia monitorowanie stanu ochrony antywirusowej/EDR, w szczególności sprawdzanie, czy ochrona jest aktywna, aktualna i obejmuje stacje robocze oraz serwery przetwarzające dane osobowe.
10. Użytkownicy systemu są odpowiedzialni za ochronę stanowisk pracy przed osobami postronnymi, nieuprawnionymi do korzystania z systemu informatycznego, w którym przetwarza się dane osobowe.
11. Systemy operacyjne, oprogramowanie użytkowe, przeglądarki internetowe, komponenty systemowe oraz systemy dziedziczne powinny być aktualizowane w sposób zapewniający ograniczenie ryzyka wykorzystania znanych podatności. Aktualizacje bezpieczeństwa wdraża się niezwłocznie po ich przetestowaniu, z uwzględnieniem ciągłości działania OPS.
12. ASI lub osoba odpowiedzialna za IT monitoruje dostępność aktualizacji bezpieczeństwa oraz podatności dotyczących wykorzystywanych systemów i podejmuje działania zmierzające do ich usunięcia albo ograniczenia ryzyka.

VIII. DOSTĘP ZDALNY I CZYNNOŚCI SERWISOWE

1. Dostęp zdalny do systemów lub stacji roboczych OPS może odbywać się wyłącznie za zgodą Administratora lub osoby przez niego upoważnionej.
2. Dostęp zdalny powinien być ograniczony czasowo i zakresowo do czynności niezbędnych do wykonania zadania serwisowego lub administracyjnego.
3. Dostęp zdalny powinien być zabezpieczony uwierzytelnianiem wieloskładnikowym, jeżeli wykorzystywane rozwiązanie technicznie to umożliwia.
4. Czynności wykonywane zdalnie przez dostawców zewnętrznych powinny być dokumentowane, w szczególności przez wskazanie daty, osoby wykonującej czynności, zakresu prac, systemu, którego dotyczyły, oraz osoby ze strony OPS zatwierdzającej dostęp.
5. Dostawca zewnętrzny uzyskujący dostęp do danych osobowych lub systemów OPS powinien posiadać właściwą podstawę dostępu, w szczególności umowę powierzenia przetwarzania danych, upoważnienie albo zobowiązanie do poufności - zależnie od charakteru czynności.

IX.

KONTROLA NA WPROWADZANIEM, DALSZYM PRZETWARZANIEM I UDOSTĘPNIANIEM DANYCH OSOBOWYCH

1. Dane osobowe z systemów informatycznych mogą być udostępniane wyłącznie osobom uprawnionym.
2. W systemie informatycznym służącym do przetwarzania danych osobowych odnotowane są informacje o odbiorcach danych, a jeżeli jest to niemożliwe – ADO dokonuje adnotacji w zestawieniu przekazywanych danych osobowych.
3. Dane osobowe powierzone zostają do przetwarzania na podstawie umowy. Podmiot przetwarzający podejmuje wszelkie niezbędne i wymagane przez przepisy prawa powszechnie obowiązującego działania w celu ochrony danych osobowych.

X.

PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

1. Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji, służących do przetwarzania danych osobowych przeprowadzane są w miarę możliwości w pomieszczeniach stanowiących obszar przetwarzania danych osobowych u ADO.
2. Przegląd systemu dokonuje IOD wraz z upoważnionym specjalistą ds. Informatyki.
3. Zmiana konfiguracji sprzętu komputerowego lub zmiana jego lokalizacji może nastąpić tylko za zgodą i wiedzą ADO.
4. Przeglądy techniczne są dokonywane nie rzadziej niż raz w roku.
5. W zakresie, w jakim przetwarzanie danych osobowych powierzono zewnętrznemu podmiotowi, udostępniającemu ADP na podstawie umowy swoje serwery, obowiązek dokonywania przeglądów i konserwacji serwerów spoczywa na tym podmiocie.

XI.

NAPRAWA KOMPUTERÓW Z DANYMI OSOBOWYMI

1. Naprawa sprzętu komputerowego oraz nośników informacji, służących do przetwarzania danych osobowych przeprowadzana jest w miarę możliwości w pomieszczeniach stanowiących obszar przetwarzania danych osobowych u ADO.
2. Naprawa wykonywana jest przez upoważnionego specjalistę z zakresu informatyki w obecności ADO lub innego upoważnionego użytkownika systemu.
3. Przed naprawą sprzętu komputerowego poza obszarem przetwarzania danych osobowych, z twardego dysku usuwa się wszelkie aplikacje przetwarzające i zawierające dane osobowe. ADO tworzy kopię bazy i przechowuje ją w bezpiecznym miejscu.
4. Po dokonaniu naprawy sprzętu komputerowego i zwrocie do ADO, baza danych jest ponownie instalowana, a kopia bazy zostaje zniszczona.
5. Przekazanie sprzętu lub nośnika do naprawy poza OPS wymaga sporządzenia protokołu przekazania, zawierającego co najmniej: datę przekazania, oznaczenie sprzętu/nośnika, osobę przekazującą, podmiot przyjmujący, informację o usunięciu danych albo zastosowanym zabezpieczeniu oraz datę zwrotu.

6. Jeżeli usunięcie danych przed naprawą nie jest możliwe, naprawa powinna odbywać się pod nadzorem osoby upoważnionej albo na podstawie umowy powierzenia/zobowiązania do poufności, z zastosowaniem środków ograniczających dostęp do danych.

XII.

POSTĘPOWANIE W PRZYPADKU STWIERDZENIA NARUSZENIA BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO

1. Użytkownik zobowiązany jest niezwłocznie, nie później niż w terminie 2 godzin od zauważenia zdarzenia, zawiadomić Administratora Sieci/ASI, ADO lub IOD o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu informatycznego, a w szczególności o:
- a. naruszeniu hasła dostępu i identyfikatora;
 - b. częściowym lub całkowitym braku danych;
 - c. niewłaściwym dostępem do danych (w szerszym lub węższym zakresie, aniżeli przydzielone uprawnienia);
 - d. braku dostępu do właściwej aplikacji;
 - e. wykryciu wirusa komputerowego;
 - f. wykryciu śladów włamania do systemu informatycznego;
 - g. podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe;
 - h. wykryciu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf;
 - i. zauważonych awariach systemu informatycznego;
 - j. zauważonych przypadkach naruszenia niniejszej instrukcji oraz Polityki Bezpieczeństwa;
 - k. nieprzestrzeganiu zasad używania oprogramowania antywirusowego;
 - l. niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych osobowych w sposób niezgodny z procedurami ochrony danych osobowych
2. Do czasu przybycia na miejsce Administratora Sieci użytkownik jest zobowiązany do:
- a. podjęcia czynności niezbędnych do powstrzymania niepożądanych skutków zaistniałego zdarzenia;
 - b. o ile jest to uzasadnione – wstrzymanie bieżącej pracy na komputerze w celu zabezpieczenia miejsca zdarzenia;
 - c. zaniechanie czynności, mogących utrudnić udokumentowanie i analizę zdarzenia;
 - d. zastosowanie się do instrukcji i regulaminów obowiązujących i ADO.
3. Administrator Sieci/ASI niezwłocznie powiadamia ADO oraz IOD o naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu. ADO, przy udziale IOD i ASI, przeprowadza postępowanie wyjaśniające, ustala okoliczności zdarzenia, zabezpiecza dowody, podejmuje działania ograniczające skutki naruszenia oraz dokonuje oceny, czy zdarzenie stanowi naruszenie ochrony danych osobowych wymagające działań zgodnie z procedurą naruszeń.

4. ADO podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych, szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego.

XIII. POSTANOWIENIA KOŃCOWE

1. Niniejsza instrukcja została sporządzona w celu dochowania obowiązków przewidzianych przepisami prawa powszechnie obowiązującego.
2. W sprawach nieuregulowanych niniejszą instrukcją należy stosować przepisy prawa powszechnie obowiązującego, jak również instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.

Naruszenie obowiązków wynikających z niniejszej instrukcji oraz przepisów o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych podlegające sankcjom wynikającym z przepisów prawa.

ZAŁĄCZNIK NR 6 - Klauzula informacyjna o przetwarzaniu danych INFORMACJA O PRZETWARZANIU DANYCH OSBOWYCH

Niniejszym informujemy Pana/Panią, że przetwarzamy Pana/Pani dane osobowe. Szczegóły tego dotyczące znajdują się poniżej:

I. Administrator danych osobowych

Administratorem Pani/Pana danych osobowych jest:

Ośrodek Pomocy Społecznej w Niemcach

ul. Lubelska 119

21-025 Niemce

tel.:

e-mail:

ePUAP:

adres do e-Doręczeń:

☐ II. Inspektor Ochrony Danych

Administrator wyznaczył Inspektora Ochrony Danych, z którym można skontaktować się we wszystkich sprawach dotyczących ochrony danych osobowych oraz realizacji praw osoby, której dane dotyczą:

e-mail:

lub pisemnie na adres siedziby Administratora.

III. Cele i podstawy przetwarzania danych

Pani/Pana dane osobowe będą przetwarzane w celu realizacji zadań Ośrodka Pomocy Społecznej wynikających z przepisów prawa, w szczególności w zakresie:

1. pomocy społecznej;
2. świadczeń rodzinnych;
- ☐ 3. funduszu alimentacyjnego;
4. wspierania rodziny i systemu pieczy zastępczej;
5. przeciwdziałania przemocy domowej;
6. prowadzenia postępowań administracyjnych;
7. obsługi korespondencji;
8. realizacji obowiązków archiwalnych;
9. realizacji innych zadań powierzonych OPS przepisami prawa.

Podstawą przetwarzania danych osobowych jest:

1. art. 6 ust. 1 lit. c RODO - gdy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze;

2. **art. 6 ust. 1 lit. e RODO** - gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;
3. **art. 9 ust. 2 RODO** - gdy przetwarzane są szczególne kategorie danych osobowych, w szczególności dane dotyczące zdrowia, niepełnosprawności, sytuacji rodzinnej, przemocy domowej lub potrzeb socjalnych;
4. **art. 10 RODO** - gdy przetwarzane są dane dotyczące wyroków skazujących, czynów zabronionych lub powiązanych środków bezpieczeństwa, jeżeli przetwarzanie takich danych wynika z przepisów prawa.

Szczegółowe podstawy prawne przetwarzania wynikają w szczególności z:

1. ustawy o pomocy społecznej;
2. ustawy o świadczeniach rodzinnych;
3. ustawy o pomocy osobom uprawnionym do alimentów;
4. ustawy o wspieraniu rodziny i systemie pieczy zastępczej;
5. ustawy o przeciwdziałaniu przemocy domowej;
6. Kodeksu postępowania administracyjnego;
7. ustawy o narodowym zasobie archiwalnym i archiwach;
8. innych przepisów właściwych dla realizowanego zadania.

IV. Kategorie danych, które przetwarzamy

Administrator przetwarza dane osobowe wyłącznie w zakresie niezbędnym do realizacji określonego celu.

W zależności od rodzaju sprawy mogą być przetwarzane w szczególności:

1. dane identyfikacyjne, takie jak imię, nazwisko, PESEL, data urodzenia;
2. dane adresowe i kontaktowe;
3. dane rodzinne;
4. dane dotyczące sytuacji życiowej, socjalnej, majątkowej i dochodowej;
5. dane dotyczące zatrudnienia lub źródeł utrzymania;
6. dane dotyczące zdrowia i niepełnosprawności;
7. dane dotyczące przemocy domowej;
8. dane dotyczące orzeczeń, decyzji, postępowań administracyjnych lub sądowych;
9. dane dotyczące rachunku bankowego;
10. dane zawarte w dokumentach przedstawionych w toku prowadzonej sprawy;
11. inne dane wymagane przepisami prawa.

Administrator nie stosuje wobec Pani/Pana zautomatyzowanego podejmowania decyzji, w tym profilowania, w rozumieniu art. 22 RODO.

V. Odbiorcy danych

Pani/Pana dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym na podstawie przepisów prawa oraz podmiotom, z którymi Administrator zawarł odpowiednie umowy.

Odbiorcami danych mogą być w szczególności:

1. organy administracji publicznej;
2. wojewoda;
3. minister właściwy do spraw zabezpieczenia społecznego;
4. Zakład Ubezpieczeń Społecznych;
5. urzędy skarbowe;
- ☐ 6. powiatowe urzędy pracy;
7. sądy;
8. prokuratura;
9. Policja;
10. kuratorzy sądowi;
11. komornicy;
12. jednostki organizacyjne pomocy społecznej;
13. banki - w zakresie realizacji wypłat;
- ☐ 14. podmioty świadczące obsługę informatyczną, serwisową, prawną, pocztową, archiwizacyjną lub niszczenia dokumentacji - wyłącznie na podstawie właściwej umowy lub przepisów prawa.

VI. Przekazywanie danych do państw trzecich lub organizacji międzynarodowych

Administrator nie przekazuje Pani/Pana danych osobowych do państw trzecich ani organizacji międzynarodowych, chyba że w konkretnym procesie zostanie to wyraźnie wskazane wraz z podstawą prawną i zabezpieczeniami wymaganymi przez RODO.

VII. Okres przechowywania danych

Pani/Pana dane osobowe będą przechowywane przez okres niezbędny do realizacji celu, dla którego zostały zebrane, a następnie przez okres wynikający z przepisów prawa, w szczególności z przepisów archiwalnych, instrukcji kancelaryjnej, jednolitego rzeczowego wykazu akt oraz przepisów właściwych dla danej sprawy.

VIII. Prawa osób, których dane dotyczą

Osobie, której dane dotyczą, przysługuje:

1. prawo dostępu do swoich danych oraz otrzymania ich kopii;
2. prawo do sprostowania danych;
3. prawo do ograniczenia przetwarzania danych;
4. prawo do usunięcia danych - w przypadkach przewidzianych przepisami RODO;
5. prawo do sprzeciwu - w przypadkach, gdy podstawą przetwarzania jest art. 6 ust. 1 lit. e RODO;
6. prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Realizacja niektórych praw, w szczególności prawa do usunięcia danych, może być ograniczona, jeżeli dalsze przetwarzanie jest niezbędne do wykonania obowiązku prawnego, realizacji zadania publicznego, prowadzenia postępowania administracyjnego lub wykonania obowiązków archiwalnych.

Obecny katalog praw jest niepełny — nie wskazuje prawa sprzeciwu i nie precyzuje organu nadzorczego jako Prezesa UODO.

IX. Źródła pochodzenia danych

Jeżeli dane osobowe nie zostały pozyskane bezpośrednio od osoby, której dotyczą, Administrator może pozyskiwać je z rejestrów publicznych, systemów teleinformatycznych administracji publicznej oraz od podmiotów uprawnionych na podstawie przepisów prawa.

Dane mogą pochodzić w szczególności od:

1. członków rodziny;
2. innych osób uczestniczących w postępowaniu;
3. Zakładu Ubezpieczeń Społecznych;
4. urzędu skarbowego;
5. powiatowego urzędu pracy;
6. rejestru PESEL;
7. KRUS;
8. komornika;
9. sądu;
10. Policji;
11. kuratora;
12. innych jednostek organizacyjnych pomocy społecznej;
13. systemów teleinformatycznych wykorzystywanych przy realizacji zadań publicznych.

X. Dobrowolność lub obowiązek podania danych

Podanie danych osobowych jest obowiązkowe, jeżeli wynika z przepisów prawa i jest niezbędne do realizacji sprawy prowadzonej przez OPS.

Niepodanie danych wymaganych przepisami prawa może skutkować brakiem możliwości rozpatrzenia sprawy, przyznania świadczenia, udzielenia pomocy lub realizacji innego zadania publicznego.

W przypadkach, w których przetwarzanie odbywa się na podstawie zgody, podanie danych jest dobrowolne, a zgoda może zostać wycofana w dowolnym momencie, bez wpływu na zgodność z prawem przetwarzania dokonanego przed jej wycofaniem.

ZAŁĄCZNIK NR 7 – Wzór umowy powierzenia przetwarzania danych osobowych

**UMOWA POWIERZENIA
PRZETWARZANIA DANYCH OSOBOWYCH**

zawarta dnia w (zwana dalej „Umową”) pomiędzy:

Ośrodkiem Pomocy Społecznej w Niemcach, ul. Lubelska 119, 21-025 Niemce, reprezentowanym przez, zwanym dalej „Administratorem” lub „Administratorem danych”,

oraz

.....
....., z siedzibą w NIP/KRS:
....., reprezentowanym przez
....., zwanym dalej „Podmiotem przetwarzającym” lub „Procesorem”.

Administrator i Podmiot przetwarzający zwani są dalej łącznie „Stronami”.

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (zwanego dalej „RODO” albo „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, RODO oraz innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki techniczne i organizacyjne zapewniające stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych.
4. Podmiot przetwarzający przetwarza dane osobowe wyłącznie w imieniu Administratora, na jego udokumentowane polecenie oraz wyłącznie w zakresie i celu określonym w niniejszej Umowie, umowie głównej lub załączniku określającym zakres powierzenia.
5. Podmiot przetwarzający nie jest uprawniony do samodzielnego określania celów ani sposobów przetwarzania powierzonych danych osobowych. W przypadku naruszenia tego zakazu Podmiot przetwarzający może zostać uznany za administratora w odniesieniu do tego przetwarzania zgodnie z art. 28 ust. 10 RODO.

§ 2

Zakres, charakter i cel przetwarzania danych

1. Administrator powierza Podmiotowi przetwarzającemu dane osobowe w zakresie niezbędnym do wykonania umowy głównej nr z dnia, której przedmiotem jest

2. Charakter przetwarzania obejmuje w szczególności następujące operacje: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesyłanie, usuwanie lub niszczenie danych - wyłącznie w zakresie niezbędnym do realizacji celu określonego w ust. 3.

3. Celem przetwarzania danych jest:

4. Kategorie osób, których dane dotyczą:, w szczególności mogą to być: klienci OPS, członkowie rodzin klientów OPS, pracownicy Administratora, współpracownicy Administratora, osoby kontaktowe, kontrahenci lub osoby wskazane w dokumentacji prowadzonej przez OPS - zależnie od przedmiotu umowy głównej.

5. Kategorie powierzonych danych osobowych:, w szczególności mogą to być: dane identyfikacyjne, adresowe, kontaktowe, numer PESEL, dane rodzinne, majątkowe, dochodowe, dane dotyczące świadczeń, dane dotyczące rachunku bankowego oraz dane zawarte w dokumentacji prowadzonej przez OPS.

6. Jeżeli jest to niezbędne do realizacji umowy głównej, powierzenie może obejmować szczególne kategorie danych osobowych, w szczególności dane dotyczące zdrowia, niepełnosprawności, sytuacji rodzinnej, sytuacji socjalnej, przemocy domowej lub innych okoliczności wynikających z dokumentacji prowadzonej przez OPS.

7. Jeżeli jest to niezbędne do realizacji umowy głównej, powierzenie może obejmować dane, o których mowa w art. 10 RODO, wyłącznie w zakresie wynikającym z przepisów prawa i dokumentacji prowadzonej przez Administratora.

8. Szczegółowy zakres powierzenia może zostać określony w Załączniku nr 1 do niniejszej Umowy.

§ 3

Sposób wykonania umowy w zakresie przetwarzania danych osobowych

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 RODO.

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 lit. b RODO, przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej Umowy, zarówno w trakcie zatrudnienia lub współpracy z Podmiotem przetwarzającym, jak i po ich ustaniu.

5. Po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych Podmiot przetwarzający, według decyzji Administratora, zwraca Administratorowi wszelkie powierzone dane osobowe albo usuwa je w sposób uniemożliwiający ich odtworzenie oraz usuwa wszelkie istniejące kopie, chyba że prawo Unii Europejskiej lub prawo krajowe nakazuje dalsze przechowywanie danych osobowych. Wykonanie usunięcia albo zwrotu danych powinno zostać potwierdzone pisemnie lub dokumentowo.

6. 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 RODO.

7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych lub podejrzeniu takiego naruszenia zgłasza je Administratorowi bez zbędnej zwłoki, nie później niż w terminie 24 godzin od jego stwierdzenia. Zgłoszenie powinno zawierać co najmniej: opis charakteru naruszenia, datę i godzinę stwierdzenia, kategorie i przybliżoną liczbę osób, których dane dotyczą, zakres danych objętych naruszeniem, możliwe konsekwencje naruszenia, zastosowane lub proponowane środki zaradcze oraz dane osoby kontaktowej po stronie Podmiotu przetwarzającego.

8. Podmiot przetwarzający stosuje środki techniczne i organizacyjne adekwatne do ryzyka, w szczególności: kontrolę dostępu, nadawanie uprawnień wyłącznie osobom upoważnionym, zobowiązanie osób do poufności, zabezpieczenie systemów i nośników, ochronę przed złośliwym oprogramowaniem, wykonywanie kopii zapasowych, szyfrowanie danych lub nośników, jeżeli jest adekwatne do ryzyka, oraz dokumentowanie czynności związanych z przetwarzaniem danych.

9. Podmiot przetwarzający zobowiązuje się niezwłocznie poinformować Administratora, jeżeli jego zdaniem wydane mu polecenie narusza RODO lub inne przepisy dotyczące ochrony danych osobowych.

§ 4 Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 lit. h RODO 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, z minimum 3-dniowym uprzedzeniem. W przypadku podejrzenia naruszenia ochrony danych osobowych, istotnego naruszenia Umowy lub zagrożenia dla praw i wolności osób fizycznych, kontrola może zostać przeprowadzona bez zachowania powyższego terminu uprzedzenia.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych, nie dłuższym niż 7 dni, chyba że Strony uzgodnią inny termin ze względu na charakter uchybień.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO.
5. Kontrola może mieć formę audytu na miejscu, audytu zdalnego, ankiety bezpieczeństwa, przeglądu dokumentów, żądania wyjaśnień lub przedstawienia certyfikatów, raportów i innych dowodów potwierdzających spełnianie wymagań niniejszej Umowy.

§ 5 Podpowierzenie

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, chyba że Strony uzgodniły ogólną zgodę na korzystanie z podwykonawców.
2. Przekazanie powierzonych danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić wyłącznie na udokumentowane polecenie Administratora albo gdy obowiązek taki nakłada na Podmiot przetwarzający prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo nie zabrania udzielenia takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca powinien spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.
5. Podmiot przetwarzający prowadzi aktualną listę podwykonawców, którym podpowierzono przetwarzanie danych osobowych, i udostępnia ją Administratorowi na każde żądanie.
6. W przypadku ogólnej zgody Administratora na korzystanie z podwykonawców Podmiot przetwarzający informuje Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia podwykonawców, dając Administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.
7. Podmiot przetwarzający zapewnia, aby na podwykonawcę zostały nałożone co najmniej takie same obowiązki ochrony danych, jakie wynikają z niniejszej Umowy.

§ 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 jakiegokolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania tych danych osobowych, w szczególności prowadzonych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

3. Podmiot przetwarzający odpowiada za działania i zaniechania osób, którym powierzył przetwarzanie danych osobowych, jak za własne działania i zaniechania, z zastrzeżeniem ☐ bezwzględnie obowiązujących przepisów prawa.

§ 7

Czas obowiązywania umowy

1. Niniejsza Umowa obowiązuje od dnia jej zawarcia przez okres obowiązywania umowy głównej, o której mowa w § 2 ust. 1, albo do czasu zakończenia przetwarzania danych osobowych przez Podmiot przetwarzający, w zależności od tego, które zdarzenie nastąpi później.

2. Każda ze Stron może wypowiedzieć niniejszą Umowę na zasadach określonych w umowie głównej, chyba że dalsze obowiązywanie Umowy jest niezbędne do zgodnego z prawem zakończenia przetwarzania danych osobowych.

§ 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, RODO lub udokumentowanymi poleceniami Administratora;

c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez wymaganej zgody Administratora danych;

d) naruszył obowiązek poufności lub obowiązek zgłaszania naruszeń ochrony danych osobowych;

e) nie zapewnia środków technicznych i organizacyjnych adekwatnych do ryzyka przetwarzania danych osobowych.

§ 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.
3. Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, aby środki łączności wykorzystywane do odbioru, przekazywania oraz przechowywania danych poufnych gwarantowały zabezpieczenie danych poufnych, w tym w szczególności danych osobowych powierzonych do przetwarzania, przed dostępem osób trzecich nieupoważnionych do zapoznania się z ich treścią.
4. Obowiązek zachowania poufności obowiązuje przez cały czas trwania Umowy oraz po jej zakończeniu, bez względu na przyczynę jej rozwiązania lub wygaśnięcia.
5. Obowiązek poufności obejmuje również informacje dotyczące organizacji i zabezpieczeń systemów informatycznych Administratora, sposobów dostępu, konfiguracji, haseł, kopii zapasowych, incydentów bezpieczeństwa oraz innych informacji, których ujawnienie mogłoby zagrozić bezpieczeństwu danych osobowych.

§ 10

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego, RODO oraz inne właściwe przepisy prawa powszechnie obowiązującego.
3. Sędem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy miejscowo dla siedziby Administratora danych, chyba że Strony postanowią inaczej w umowie głównej.

..... Administrator danych	 Podmiot przetwarzający
data i podpis	data i podpis

Załącznik nr 1 do Umowy powierzenia

Szczegółowy zakres powierzenia danych osobowych

Lp.	Element	Opis / do uzupełnienia
1.	Umowa główna	nr z dnia
2.	Przedmiot usługi	

3.	Cel przetwarzania	
4.	Kategorie osób	
5.	Kategorie danych zwykłych	
6.	Dane szczególnych kategorii	TAK / NIE; jeżeli TAK, wskazać jakie:
7.	Dane z art. 10 RODO	TAK / NIE; jeżeli TAK, wskazać zakres:
8.	Systemy lub obszary przetwarzania	
9.	Miejsce przetwarzania danych	siedziba Administratora / siedziba Procesora / inne:
10.	Podwykonawcy	NIE / TAK, wykaz:
11.	Transfer poza EOG	NIE / TAK, podstawa i zabezpieczenia:
12.	Termin zgłaszania naruszeń	nie później niż 24 godziny od stwierdzenia naruszenia
13.	Sposób zakończenia powierzenia	zwrot danych / usunięcie danych / protokół zniszczenia

ZAŁĄCZNIK NR 8 – Wzór Upoważnienie do przetwarzania danych osobowych wraz z oświadczeniem o zapoznaniu się z Polityką ochrony danych osobowych.

Niemce, dnia 25 maja 2018 r.

**UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH**

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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, s. 1) – dalej RODO – nadaję upoważnienie Pani/Panu:

.....
(imię i nazwisko)

.....
(stanowisko)

do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku, tj. uzyskuje Pani/Pan upoważnienie do przetwarzania danych osobowych w zakresie określonym przez Politykę ochrony danych osobowych. Osoba upoważniona przetwarza dane wyłącznie w zakresie niezbędnym do realizacji powierzonych zadań i jest zobowiązana do zachowania w tajemnicy danych osobowych, informacji o zabezpieczeniach oraz informacji uzyskanych przy wykonywaniu zadań pomocy społecznej, także po ustaniu zatrudnienia lub współpracy.

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami prawa powszechnie obowiązującego, a także z Polityką ochrony danych osobowych i załączonej do niej Instrukcji Zarządzania Systemem Informatycznym.

Jednocześnie upoważniam Panią/Pana do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień, ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w Polityce ochrony danych osobowych Pracodawcy.

.....
podpis osoby uprawnionej do nadania upoważnienia

Upoważnienie odwołano w dniu

.....
podpis osoby uprawnionej do odwołania upoważnienia

Niniejszym oświadczam, że zapoznałem/zapoznałam się z treścią Polityki ochrony danych osobowych, ustawą o ochronie danych osobowych oraz RODO. Zobowiązuję się zachować w tajemnicy wszelkie informacje, które uzyskałem/uzyskałam w związku z przetwarzaniem danych osobowych, w tym informacje o zabezpieczeniach takiego przetwarzania oraz dane osobowe szczególnych kategorii na mocy art. 9 ust. 3 RODO.

.....
podpis osoby upoważnionej do przetwarzania

ZAŁĄCZNIK NR 9 - Ewidencja osób upoważnionych do przetwarzania danych osobowych

L.p.	Imię i nazwisko upoważnionej osoby	Data udzielenia upoważnienia	Data ustania upoważnienia	Zakres upoważnienia - kategorie danych lub rodzaj czynności lub operacji	Wylączenia kategorii danych lub czynności, które wynikają z upoważnienia	Identyfikator nadany do przetwarzania w systemie informaty- cznym
1.						
2.						
3.						

INSTRUKCJA POSTĘPOWANIA W PRZYPADKU ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

1. Cel i zakres instrukcji

- 1.1. Instrukcja określa zasady postępowania w przypadku zdarzeń, incydentów bezpieczeństwa oraz naruszeń ochrony danych osobowych przetwarzanych przez Ośrodek Pomocy Społecznej w Niemcach, zarówno w systemach informatycznych, jak i w dokumentacji papierowej.
- 1.2. Instrukcja ma zastosowanie do wszystkich pracowników, współpracowników, osób upoważnionych do przetwarzania danych osobowych, Administratora Systemów Informatycznych, dostawców usług oraz innych osób, które mogą uzyskać dostęp do danych osobowych przetwarzanych przez ADO.

2. Definicje

- 2.1. ADO - Administrator Danych Osobowych, tj. Ośrodek Pomocy Społecznej w Niemcach reprezentowany przez Kierownika OPS.
- 2.2. IOD - Inspektor Ochrony Danych wyznaczony przez ADO.
- 2.3. ASI - Administrator Systemów Informatycznych albo osoba odpowiedzialna za techniczne utrzymanie systemów informatycznych OPS.
- 2.4. Incydent bezpieczeństwa - każde zdarzenie lub podejrzenie zdarzenia mogącego wpływać na poufność, integralność, dostępność lub rozliczalność danych osobowych.
- 2.5. Naruszenie ochrony danych osobowych - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

3. Zgłoszenie zdarzenia lub podejrzenia naruszenia

- 3.1. Każda osoba przetwarzająca dane osobowe, w przypadku stwierdzenia lub podejrzenia naruszenia zabezpieczenia danych osobowych, jest zobowiązana niezwłocznie powiadomić o tym ADO, IOD lub ASI.
- 3.2. Zgłoszenie wewnętrzne powinno nastąpić niezwłocznie, nie później niż w terminie 2 godzin od zauważenia zdarzenia, jeżeli okoliczności organizacyjne na to pozwalają.
- 3.3. Zgłoszenie powinno zawierać, o ile jest to możliwe: datę i godzinę zauważenia zdarzenia, opis zdarzenia, system lub dokumentację, której zdarzenie dotyczy, osoby uczestniczące, kategorie danych oraz podjęte dotychczas działania zabezpieczające.
- 3.4. Brak pełnych informacji o zdarzeniu nie zwalnia z obowiązku niezwłocznego zgłoszenia podejrzenia naruszenia.

4. Czynności po otrzymaniu zgłoszenia

- 4.1. ADO, po otrzymaniu zgłoszenia, podejmuje działania wyjaśniające przy udziale IOD, ASI lub innej osoby upoważnionej, jeżeli jest to uzasadnione charakterem zdarzenia.
- 4.2. W ramach czynności wyjaśniających należy w szczególności:
 - sprawdzić stan urządzeń i systemów wykorzystywanych do przetwarzania danych osobowych;
 - sprawdzić sposób działania programów, usług sieciowych i zabezpieczeń, w tym ochrony antywirusowej/EDR;
 - sprawdzić jakość i dostępność komunikacji sieciowej oraz usług teleinformatycznych;
 - ustalić zakres danych, których dotyczy zdarzenie;
 - ustalić kategorie i przybliżoną liczbę osób, których dane dotyczą;
 - zabezpieczyć dowody, w szczególności logi, wiadomości e-mail, zrzuty ekranu, dokumentację, nośniki, protokoły i notatki służbowe;
 - ocenić, czy zdarzenie stanowi naruszenie ochrony danych osobowych w rozumieniu RODO.

5. Działania ograniczające skutki zdarzenia

5.1. W przypadku stwierdzenia naruszenia zabezpieczenia danych ADO lub osoba przez niego upoważniona podejmuje działania mające na celu uniemożliwienie dalszego naruszenia, ograniczenie jego skutków i przywrócenie prawidłowego stanu działania systemu lub procesu.

5.2. Działania te mogą obejmować w szczególności: odłączenie wadliwych urządzeń, zablokowanie kont użytkowników, zmianę haseł, ograniczenie dostępu do systemu lub zbioru danych, zabezpieczenie dokumentacji, cofnięcie uprawnień, odtworzenie danych z kopii zapasowej, powiadomienie procesora lub dostawcy usługi oraz zabezpieczenie miejsca zdarzenia.

5.3. Do czasu zakończenia czynności wyjaśniających zabrania się podejmowania działań, które mogłyby utrudnić ustalenie okoliczności zdarzenia, w szczególności samodzielnego kasowania logów, korespondencji, plików lub dokumentacji związanej ze zdarzeniem.

6. Ocena ryzyka naruszenia

6.1. ADO, przy udziale IOD, dokonuje oceny, czy naruszenie może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych.

6.2. Przy ocenie ryzyka należy uwzględnić w szczególności: rodzaj naruszenia, kategorie i zakres danych, łatwość identyfikacji osób, liczbę osób, których dane dotyczą, możliwe skutki dla osób, zastosowane zabezpieczenia, charakter osób, których dane dotyczą, w tym czy są to dzieci, osoby zależne, osoby korzystające z pomocy społecznej lub osoby doświadczające przemocy domowej.

6.3. Szczególnej ostrożności wymagają naruszenia obejmujące dane szczególnych kategorii, dane o zdrowiu, niepełnosprawności, przemocy domowej, sytuacji rodzinnej, sytuacji majątkowej, dane dzieci oraz dane dotyczące wyroków skazujących lub czynów zabronionych.

6.4. Wynik oceny ryzyka dokumentuje się w Karcie oceny naruszenia ochrony danych osobowych, stanowiącej załącznik do niniejszej Instrukcji.

7. Zgłoszenie naruszenia Prezesowi UODO

7.1. W przypadku naruszenia ochrony danych osobowych ADO zgłasza naruszenie Prezesowi Urzędu Ochrony Danych Osobowych bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że jest mało prawdopodobne, aby naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

7.2. Jeżeli zgłoszenie następuje po upływie 72 godzin, ADO dołącza do zgłoszenia wyjaśnienie przyczyn opóźnienia.

7.3. Decyzję o zgłoszeniu naruszenia albo o braku zgłoszenia dokumentuje się wraz z uzasadnieniem w Karcie oceny naruszenia i Rejestrze naruszeń ochrony danych osobowych.

7.4. Zgłoszenie naruszenia powinno zawierać informacje wymagane przez art. 33 RODO, w szczególności:

- charakter naruszenia ochrony danych osobowych;
- kategorie i przybliżoną liczbę osób, których dane dotyczą;
- kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- imię i nazwisko oraz dane kontaktowe IOD lub innego punktu kontaktowego;
- możliwe konsekwencje naruszenia;
- środki zastosowane lub proponowane w celu zaradzenia naruszeniu oraz zminimalizowania jego negatywnych skutków.

8. Zawiadomienie osób, których dane dotyczą

8.1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO zawiadamia osoby, których dane dotyczą, bez zbędnej zwłoki, zgodnie z art. 34 RODO.

8.2. Zawiadomienie powinno być sformułowane jasnym i prostym językiem oraz zawierać co najmniej opis charakteru naruszenia, dane kontaktowe IOD lub innego punktu kontaktowego,

możliwe konsekwencje naruszenia oraz środki zastosowane lub proponowane przez ADO w celu zaradzenia naruszeniu.

8.3. Decyzja o zawiadomieniu albo o braku zawiadomienia osób, których dane dotyczą, wymaga udokumentowania wraz z uzasadnieniem.

9. Rejestr naruszeń i dokumentowanie

9.1. ADO prowadzi Rejestr naruszeń ochrony danych osobowych.

9.2. ADO dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia, jego skutki, wynik oceny ryzyka, decyzję o zgłoszeniu lub braku zgłoszenia do Prezesa UODO, decyzję o zawiadomieniu osób oraz podjęte działania zaradcze i zapobiegawcze.

9.3. Rejestr naruszeń i karty oceny naruszeń przechowuje się w Teczce Ochrony Danych Osobowych albo w innym miejscu wskazanym przez ADO, z zapewnieniem poufności i integralności dokumentacji.

10. Działania korygujące i zapobiegawcze

10.1. Po zakończeniu obsługi zdarzenia ADO, przy udziale IOD i ASI, analizuje przyczyny naruszenia oraz podejmuje działania zapobiegające podobnym naruszeniom w przyszłości.

10.2. Działania zapobiegawcze mogą obejmować w szczególności zmianę procedur, dodatkowe szkolenie pracowników, zmianę uprawnień, aktualizację zabezpieczeń technicznych, aktualizację umów powierzenia, test kopii zapasowych, audyt dostawcy lub przegląd organizacji pracy.

10.3. Dla każdego działania zapobiegawczego wyznacza się osobę odpowiedzialną oraz termin realizacji. Wykonanie działań powinno zostać zweryfikowane i odnotowane w dokumentacji naruszenia.

11. Pełnomocnictwo i brak konfliktu interesów

11.1. ADO może udzielić pełnomocnictwa innej osobie, również zatrudnionej u ADO, w zakresie przeprowadzenia czynności związanych z obsługą naruszenia lub podejrzenia naruszenia, pod warunkiem braku konfliktu interesów.

11.2. Osoba, której działania lub zaniechania mogły przyczynić się do naruszenia, nie powinna samodzielnie prowadzić czynności wyjaśniających dotyczących tego naruszenia.

12. Postanowienia końcowe

12.1. W sprawach nieuregulowanych niniejszą Instrukcją stosuje się RODO, ustawę o ochronie danych osobowych, Politykę Ochrony Danych Osobowych oraz inne procedury obowiązujące u ADO.

12.2. Naruszenie obowiązków wynikających z niniejszej Instrukcji może być uznane za naruszenie obowiązków pracowniczych lub obowiązków wynikających ze współpracy z ADO.

KARTA OCENY NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Wzór formularza do stosowania przy ocenie i dokumentowaniu naruszeń ochrony danych osobowych.

Lp.	Pole	Opis / do uzupełnienia
1	Numer sprawy	
2	Data i godzina wykrycia zdarzenia	
3	Data i godzina stwierdzenia naruszenia	
4	Osoba zgłaszająca	
5	Opis zdarzenia	
6	System, proces lub dokumentacja, której dotyczy zdarzenie	
7	Kategorie osób, których dane dotyczą	
8	Kategorie danych osobowych	
9	Czy naruszenie obejmuje dane szczególnych kategorii lub dane z art. 10 RODO	TAK / NIE; jeżeli TAK - wskazać zakres
10	Przybliżona liczba osób, których dane dotyczą	
11	Możliwe konsekwencje naruszenia	
12	Podjęte środki zaradcze	
13	Ocena ryzyka dla praw lub wolności osób fizycznych	niskie / średnie / wysokie
14	Decyzja o zgłoszeniu do Prezesa UODO	TAK / NIE
15	Uzasadnienie decyzji o zgłoszeniu albo braku zgłoszenia	
16	Data zgłoszenia do Prezesa UODO	
17	Decyzja o zawiadomieniu osób, których dane dotyczą	TAK / NIE
18	Uzasadnienie decyzji o zawiadomieniu albo braku zawiadomienia	
19	Opinia IOD	
20	Decyzja ADO	
21	Działania zapobiegawcze	
22	Osoba odpowiedzialna i termin realizacji działań	
23	Data zamknięcia sprawy	

Przedstawione powyżej wzory nie stanowią katalogu zamkniętego dokumentacji składającej się na Politykę ochrony danych osobowych. Każda dodatkowa, nowa procedura, instrukcja czy wytyczna ADO dotycząca obszaru ochrony danych osobowych stanowi integralną część niniejszej Polityki, a ich dodanie nie wymaga jej zmiany.

Wypełnione wzory załączników przechowywane są w Teczce Ochrony Danych Osobowych.

