Załącznik nr 1 do Zarządzenia nr 5/2021 z dnia 29.01.2021 r. Dyrektora Powiatowego Centrum Pomocy Rodzinie w Tucholi

POLITYKA OCHRONY DANYCH OSOBOWYCH W Powiatowym Centrum Pomocy Rodzinie w Tucholi

ZATWIERDZAM

DYREKTOR
POWIATOWEGO CENTRUM
POMOCY RODZINIE
mgr Anna Toby

29.01.2021 r.

.....

(data i podpis Administratora Danych)

ROZDZIAŁ 1. POSTANOWIENIA OGÓLNE

§ 1

Zakres

1. **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) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.
2. Stanowi ona zbiór wymogów, zasad i regulacji ochrony danych osobowych u **Administratora danych osobowych**, którym jest Powiatowe Centrum Pomocy Rodzinie w Tucholi, reprezentowane przez Kierownika Powiatowego Centrum Pomocy Rodzinie w Tucholi (dalej jako ADO).
3. Zasady, działania, kompetencje i zakresy odpowiedzialności opisane w niniejszej Polityce Ochrony Danych Osobowych (PODO lub Polityka), obowiązują wszystkich pracowników i współpracowników ADO.
4. 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.
5. 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.
6. 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.
7. 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 jakiejkolwiek innej.
    4) nieprzestrzeganie postanowień zawartych w Polityce może skutkować sankcjami w pełnym zakresie dopuszczonym przez stosunek pracy oraz obowiązujące przepisy prawa.

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

§ 2

Definicje

1) **Administrator danych** - „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; **Administratorem jest Powiatowe Centrum Pomocy Rodzinie w Tucholi, reprezentowane przez Kierownika Powiatowego Centrum Pomocy Rodzinie w Tucholi** (dalej jako **ADO**).
2) **Administrator Systemu Informatycznego (ASI)** – rozumie się przez to osobę odpowiedzialną za nadzór nad systemami informatycznymi wykorzystywanymi u Administratora Danych. Obowiązki ASI opisuje **załącznik nr 3** do niniejszej Polityki.
3) **bezpieczeństwo informacji** – zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
4) **dane osobowe** - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
5) **dane szczególne** oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;
6) **eksport danych** oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej;
7) **hasło** – rozumie się przez to ciąg znaków alfanumerycznych, znany jedynie użytkownikowi;
8) **identyfikator** – rozumie się przez to, ciąg znaków literowych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
9) **incydent ochrony danych osobowych** – zdarzenie albo seria niepożądanych lub niespodziewanych zdarzeń ochrony danych osobowych stwarzających znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrożenia ochrony danych osobowych;
10) **Inspektor ochrony danych (IOD)** – osoba sprawująca nadzór nad przestrzeganiem zasad ochrony danych osobowych wyznaczona przez ADO; zakres obowiązków IOD określa **załącznik nr 1**, a regulamin funkcjonowania IOD **załącznik nr 2** do niniejszej Polityki.
11) **naruszenie ochrony danych osobowych** - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

12) **obszar przetwarzania danych** – rozumie się przez to budynki i pomieszczenia określone przez administratora danych, tworzące obszar, w którym przetwarzane są dane osobowe i inne informacje prawem chronione; obszar przetwarzania danych opisany jest w **załączniku nr 4** do niniejszej Polityki;
13) **odbiorca danych** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
14) **osoba, podmiot danych** - oznacza osobę, której dane dotyczą;
15) **podmiot przetwarzający** - oznacza organizację lub osobę, której ADO powierzył przetwarzanie danych osobowych (np. usługodawca IT);
16) **polityka** oznacza niniejszą politykę ochrony danych osobowych;
17) **postępowanie z ryzykiem** – proces planowania i wdrażania działań wpływających na ryzyko;
18) **poufność danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
19) **profilowanie** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
20) **raport** – rozumie się przez to przygotowanie przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
21) **RCPDO lub rejestr** oznacza rejestr czynności przetwarzania danych osobowych;
22) **RODO** oznacza rozporządzenie 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).
23) **ryzyko** – niepewność osiągnięcia zamierzonych celów;
24) **serwisant** – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego;
25) **system informatyczny administratora danych** – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych;
26) **szacowanie ryzyka** – proces identyfikowania, analizowania i oceniania ryzyka;
27) **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.
28) **teletransmisja** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
29) **uwierzytelnienie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

30) **użytkownik** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło;
31) **zgoda** osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

§ 3
Zasady ochrony danych

System zarządzania ochroną danych osobowych zgodny z wymaganiami niniejszej Polityki działa z poszanowaniem następujących zasad:
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 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** – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek 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

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. *Procedura zarządzania ryzykiem* stanowi **załącznik nr 10** do niniejszej Polityki.
3. 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.
4. 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.
5. ADO prowadzi rejestr podmiotów zewnętrznych, z którymi realizacja umów lub aneksów do nich zobowiązuje lub umożliwia zleceniobiorcy/wykonawcy dostęp do informacji zawierających dane osobowe.
6. Za przestrzeganie zasad ochrony danych osobowych i za codzienną ochronę danych odpowiedzialni są upoważnieni użytkownicy.

§ 6

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.

ROZDZIAŁ 2. 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 (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, niewykonanie 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.

ROZDZIAŁ 3. DZIAŁANIA 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,
   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 wymaganym 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) nie należy udostępniać osobom nieupoważnionym tych komputerów,
   5) w przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności,
   6) nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie) aby nie zostały na nich dane osobowe,
   7) w wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) należy taką płytę zniszczyć fizycznie,
   8) w przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków,
   9) niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną,
   10) sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz,
   11) 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.

ROZDZIAŁ 4. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH

§ 12

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, analiza reklamacji klientów.

Działania zapobiegawcze mają na celu zapobiec wystąpieniu potencjalnych niezgodności.

§ 13

ADO stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia – Procedura postępowania w przypadku naruszenia danych osobowych stanowi **załącznik nr 12** do niniejszej Polityki.

ROZDZIAŁ 5. 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 stanowić 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 lub IOD i powinno być odpowiednio udokumentowane.

§ 15

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.
7) Polityka realizacji praw osób, których dane dotyczą, sposoby informowania i komunikacji oraz tryb wykonywania praw przez osobę, której dane dotyczą opisane są *w* **załączniku nr 13** do niniejszej Polityki.

§ 16

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. W przypadku zawierania umów z firmami zewnętrznymi mającymi wpływ na funkcjonowanie kluczowych elementów systemu zarządzania bezpieczeństwem informacji zalecane jest zawarcie umowy powierzenia.

ROZDZIAŁ 6. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH

§ 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. W Rejestrze, dla każdej czynności przetwarzania danych, którą ADO uznał za odrębną odnotowuje co najmniej: imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, cel przetwarzania, opis kategorii osób i opis kategorii danych, opis kategorii odbiorców danych (w tym przetwarzających), informację o przekazaniu poza EU/EOG; planowany termin usunięcia danych, ogólny opis technicznych i organizacyjnych środków ochrony danych.
3. Inspektor ochrony danych monitoruje prowadzenie Rejestru czynności przetwarzania danych osobowych. Wzór Rejestru czynności przetwarzania danych stanowi **załącznik nr 5** do niniejszej Polityki.

ROZDZIAŁ 7. BEZPIECZEŃSTWO OSOBOWE

§ 18
Etap naboru pracownika

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 stanowi **załącznik nr 7** do niniejszej Polityki. Upoważnienia rejestruje się w ewidencji upoważnień, stanowiącej **załącznik nr 8** do niniejszej Polityki.
3. Zakres upoważnienia może również być określony w umowie.
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.

§ 19
Ewidencja osób upoważnionych do przetwarzania danych

1. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych nadzoruje Inspektor ochrony danych. Wzór ewidencji stanowi **załącznik nr 10** do niniejszej Polityki.
2. Ewidencja zawiera:
   1) imię i nazwisko użytkownika,
   2) datę nadania i ustania upoważnienia
   3) zakres upoważnienia
   4) identyfikator użytkownika
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 Administratora w trybie natychmiastowym z ewidencji, zablokowanie identyfikatora oraz unieważnienie hasła tego użytkownika.
6. Osoba odpowiedzialna za sprawy kadrowe odpowiadają za natychmiastowe zgłoszenie do Administratora osób, 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.

§ 20
Zatrudnienie

1. Pracownicy i inne osoby współpracujące 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,
   - posiadane zaświadczenia, dyplomy lub certyfikaty.
2. W przypadku naruszenia zasad ochrony danych osobowych jest uruchomiana odpowiednia procedura postępowania dyscyplinarnego, która powinna być poprzedzona potwierdzeniem naruszenia zasad ochrony danych osobowych i zgromadzeniem materiału dowodowego.
3. Przekazywanie sprzętu i urządzeń służących do przetwarzania danych odbywa się na podstawie protokołów przekazania sprzętu.

§ 21
Zakończenie zatrudnienia

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.

§ 22
Zasady przyznawania dostępu

1. Przyznawanie zakresu uprawnień powinno być w ścisłym związku z zakresem obowiązków danego pracownika.
2. Zarządzanie dostępem na etapie nadawania, zmiany i cofania praw dostępu pracowników w obszarze przetwarzania danych oraz do systemów teleinformatycznych powinno się odbywać przez Administratora.
3. W zarządzaniu dostępem obowiązuje zasada, że dostęp użytkownika powinien opierać się na spełnieniu zasady rozliczalności oraz zasady niezaprzeczalności. W przypadku systemów informatycznych obowiązują następujące wymagania:
   1) wymóg jednoznacznej identyfikacji pracownika - tj. w systemach informatycznych każdy użytkownik pracuje wyłącznie na swoim indywidualnym koncie, nie są stosowane konta

anonimowe lub współdzielone poza wyjątkami, gdzie z przyczyn technicznych nie ma innej możliwości,

2) wymóg uwierzytelnienia pracownika przy korzystaniu z systemu informatycznego,
3) autoryzacji przyznania praw dostępu do systemów informatycznych.

ROZDZIAŁ 8. BEZPIECZENSTWO TELEINFORMATYCZNE

§ 23
Autoryzacja i dopuszczalne wykorzystanie zasobów

1. Przy ochronie zasobów kluczowe jest stosowanie podstawowej zasady bezpieczeństwa, że nie jest dozwolone wykorzystywanie zasobów w sposób inny niż jawnie dozwolony.
2. Do wykonywania obowiązków służbowych związanych z przetwarzaniem informacji dozwolone jest używanie systemów, urządzeń i oprogramowania dopuszczonych do użytku zgodnie z wymogami Polityki
3. Pracownicy są uprawnieni do korzystania z zasobów teleinformatycznych niezbędnych do wykonywania ich obowiązków.
4. Zakazane jest użytkowanie na terenie obszaru przetwarzania danych lub przy wykonywaniu obowiązków służbowych poza obszarem przetwarzania danych innych niż dopuszczone urządzeń, systemów i oprogramowania bez zgody Administratora Systemu Informatycznego (ASI).
5. Zakazane jest bez zgody ASI:
   a) użytkowanie urządzeń skutkujących połączeniem systemów Administratora danych z sieciami teleinformatycznymi innych podmiotów, w tym publicznymi sieciami teleinformatycznymi,
   b) użytkowanie urządzeń lub oprogramowania mających na celu zakłócenie działania innych systemów, urządzeń lub oprogramowania,
   c) użytkowanie urządzeń lub oprogramowania mogących naruszyć bezpieczeństwo innych systemów lub urządzeń,
   e) wprowadzanie zmian konfiguracji urządzeń, systemów lub oprogramowania.
6. Zakazane jest bez zgody IOD wykorzystywanie urządzeń do niejawnego przekazywania lub rejestracji danych dotyczących informacji chronionych, w tym głosu i obrazu, tj.: magnetofonów, dyktafonów, aparatów fotograficznych, kamer, telefonów komórkowych z opcją rejestrowania dźwięku i obrazu, rejestratorów ruchu sieciowego, rejestratorów pracy klawiatur itp.
7. Wykorzystanie należących do Administratora danych urządzeń, systemów i oprogramowania oraz innych zasobów do prywatnych celów pracowników jest dozwolone jedynie na uzasadniony wniosek pracownika i za zgodą IOD i ASI.
9. Zasoby Administratora danych powinny być przechowywane w taki sposób, aby zapobiec możliwości ich kradzieży lub uszkodzenia przez osoby postronne oraz przypadkowe uszkodzenia przez osoby lub czynniki środowiskowe.
10. Wynoszenie zasobów i informacji poza obszar przetwarzania danych możliwe jest za zgodą IOD lub ADO.

11. Zakazane jest przesyłanie informacji podlegających ochronie na prywatne adresy poczty elektronicznej oraz prowadzenie korespondencji służbowej z wykorzystaniem prywatnego adresu e-mail użytkownika.
12. Zakazane jest używanie prywatnych nośników zewnętrznych (np. typu pendrive) i tworzenie nieautoryzowanych kopii z baz danych.
13. Pracownicy zobowiązani są stosować zasadę czystego biurka, drukarki i ekranu - wszystkie dokumenty i materiały powinny być po zakończeniu pracy chowane w przeznaczonych do tego szafkach, szufladach itp. W przypadku braku dostatecznej ilości dostępnego miejsca dokumenty i materiały powinny być pozostawiane na biurku uporządkowane.
14. Pracownicy są zobowiązani do ochrony zasobów będących własnością innych podmiotów, a powierzonych lub oddanych do dyspozycji Administratorowi danych lub udostępnionych pracownikom na czas wykonywania przez nich czynności służbowych w takim samym stopniu jak w przypadku zasobów będących własnością Administratora danych.
15. Procedury i instrukcje dotyczące bezpieczeństwa teleinformatycznego opracowuje ASI i przechowuje w Teczce ODO.

§ 24
Metody i środki uwierzytelnienia

1. **Identyfikator**
   1) identyfikator nadaje Administrator Sytemu Informatycznego.
   2) identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
2. **Hasło użytkownika**
   1) hasło powinno składać się z unikalnego zestawu znaków. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.
   2) użytkownicy powinni stosować hasła, które:
      a) są łatwe do zapamiętania, a trudne do odgadnięcia,
      b) nie są oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących właściciela konta (np. imię, nazwisko, numer telefonu, data urodzenia itp.),
      c) zawierają przynajmniej jedną dużą literę, jedną małą literę, jedną cyfrę i znak specjalny.
   3) hasła powinny być często zmieniane, na przykład co 30 dni; IOD lub ASI może, w uzasadnionych sytuacjach polecić dokonanie zmiany hasła przez użytkownika np. po każdym incydencie lub podejrzeniu naruszenia bezpieczeństwa.
   4) należy unikać ponownego lub cyklicznego używania starych haseł.
   5) zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.
   6) pracownicy są odpowiedzialni za zachowanie w poufności swoich haseł.
   7) użytkownik nie powinien przechowywać haseł w widocznych miejscach, nie powinien umieszczać haseł w żadnych automatycznych procesach logowania (skryptach, makrach lub pod klawiszami funkcyjnymi).

8) użytkownik wprowadza swoje hasło w sposób uniemożliwiający innym osobom jego poznanie.
9) w sytuacji, gdy zachodzi podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik natychmiast dokonuje zmiany hasła.
10) hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
11) Administrator Systemu Informatycznego przeprowadza okresowe sprawdzanie, usuwanie lub blokowanie zbędnych identyfikatorów użytkowników oraz kont w systemach za które są odpowiedzialni.

3. **Hasło administratora systemu informatycznego**
Hasła użytkowników uprzywilejowanych (tzn. użytkowników posiadających uprawnienia na poziomie administratorów systemów informatycznych) są zabezpieczone u Administratora danych na wypadek sytuacji awaryjnych, szczególnie w przypadku nieobecności ASI.

ROZDZIAŁ 9. POSTANOWIENIA KOŃCOWE

§ 25

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. Wyznaczony pracownik PCPR we współpracy z IOD i ASI dokonuje analizy zapisów wewnętrznych procedur regulujących zasady funkcjonowania jednostki pod względem bezpieczeństwa przetwarzania danych osobowych.
4. Analizę, o której mowa w ust. 3, przeprowadza się nie rzadziej niż raz na 6 miesięcy oraz za każdym razem, gdy stwierdzono incydent w zakresie przetwarzania danych osobowych.
5. 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.
6. 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.
7. 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.
8. Umyślne lub nieumyślne naruszenie postanowień Polityki lub niestosowanie się do poleceń służbowych w tym zakresie może być potraktowane jako naruszenie obowiązków pracowniczych.

§ 26

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 oświadczenia potwierdzającego zaznajomienie użytkownika z przepisami w zakresie ochrony informacji oraz z dokumentacją obowiązującą u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania, stanowi **załącznik nr 6** do niniejszej Polityki.
5. Oświadczenia przechowywane są w aktach osobowych.

§ 27

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie aktualnie obowiązujące przepisy prawa w zakresie ochrony danych osobowych, szczególnie RODO.
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.

ROZDZIAŁ 10. SPIS ZAŁĄCZNIKÓW

Załącznik nr 1. Zakres zadań IOD
Załącznik nr 2. Regulamin funkcjonowania IOD
Załącznik nr 3. Zakres zadań Administratora Systemu Informatycznego
Załącznik nr 4. Obszar przetwarzania danych
Załącznik nr 5. Rejestr czynności przetwarzania danych (prowadzi się w formie elektronicznej)
Załącznik nr 6. Oświadczenie o znajomości i przestrzeganiu przepisów i zasad ochrony danych oraz zachowaniu tajemnicy danych osobowych
Załącznik nr 7. Upoważnienie do przetwarzania danych osobowych
Załącznik nr 8. Ewidencja osób upoważnionych do przetwarzania danych (prowadzi się w formie elektronicznej)
Załącznik nr 9. Procedura zarządzania ryzykiem
Załącznik nr 10. Procedura postępowania w przypadku naruszenia danych osobowych
Załącznik nr 11. Polityka realizacji praw osób, których dane dotyczą
Załącznik nr 12. Polityka korzystania z usług podmiotów przetwarzających

Wypełnione załączniki (z wyjątkiem tych prowadzonych w formie elektronicznej) przechowywane są w Teczce Ochrony Danych Osobowych.

Załącznik nr 1. Zakres zadań IOD

ZAKRES ZADAŃ INSPEKTORA OCHRONY DANYCH

Zgodnie z przepisami RODO inspektor ochrony danych ma następujące zadania:

1. Informowanie administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia - RODO, oraz przepisów ustawy z 10 maja 2018 r. o ochronie danych i doradzanie im w tej sprawie.
2. Monitorowanie zgodności z RODO, tj. min. :
   a) zbieranie informacji w celu identyfikacji procesów przetwarzania;
   b) analizowanie i sprawdzanie zgodności przetwarzania;
   c) informowanie, doradzanie i rekomendowanie określonych działań administratorowi;
   d) monitorowanie prowadzenia rejestru czynności przetwarzania danych osobowych.
3. Ocena skutków dla ochrony danych:
   a) rekomendacja zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą;
   b) analiza prawidłowości przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z wymogami ochrony danych (czy należy kontynuować przetwarzanie czy też nie oraz jakie zabezpieczenia należy zastosować).
4. Współpraca z organem nadzorczym, w tym pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Wszystkie z powyżej wskazanych zadań IOD jest obowiązany wypełniać z „uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania" (art. 39 ust. 2 RODO).

Załącznik nr 2. Regulamin funkcjonowania IOD.

1. Wyznaczenie i zadania inspektora ochrony danych

1.1. Administrator na podstawie art. 37 ust. 1 lit. a Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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 - RODO), oraz na podstawie art. 9 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, wyznaczył Inspektora ochrony danych (dalej również IOD).

1.2. Do zadań IOD należy, w szczególności, monitorowanie przestrzegania przepisów o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.

1.3. Zakres zadań inspektora ochrony danych określa załącznik nr 2 do niniejszej Polityki

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

1.5. IOD wypełnia swoje zadania z uwzględnieniem wytycznych dotyczących inspektorów ochrony danych przyjętych przez Grupę Roboczą Art. 29 ds. Ochrony Danych (Europejską Radę Ochrony Danych).

1.6. IOD wypełnia swoje zadania z należytą starannością.

1.7. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.

2. Pozycja inspektora ochrony danych w jednostce (status)

1.1. Administrator zapewnia, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.

1.2. Administrator wspiera IOD w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania

1.3. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy rozporządzenia - RODO.

1.4. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.

1.5. Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.

3. Dane kontaktowe inspektora ochrony danych

Dane kontaktowe do IOD to: adres e-mail. inspektor.rodo@wp.pl nr tel.: 500438300 i zostały zamieszczone na stronie internetowej administratora pod adresem www.pcprtuchola.pl oraz w siedzibie administratora przy ul. Kościuszki 16, 89-500 Tuchola .

4. Odwołanie lub zmiana Inspektora ochrony danych

1.1. IOD nie jest odwoływany ani karany przez administratora za należyte wypełnianie swoich zadań. IOD nie może zostać odwołany ani karany za udzielenie określonego zalecenia dotyczącego bezpieczeństwa danych osobowych, z którym nie zgadza się Administrator.

1.2. Zgodnie z regułami, przepisami karnymi i prawa pracy, jak w przypadku każdego innego pracownika czy zleceniobiorcy, IOD może zostać odwołany w uzasadnionych sytuacjach z przyczyn innych niż wykonywanie obowiązków IOD (np. kradzież, ciężkie naruszenie obowiązków).

1.3. Administrator zawiadamia Prezesa Urzędu o każdej zmianie danych IOD oraz o odwołaniu inspektora, w terminie 14 dni od dnia zaistnienia zmiany lub odwołania.

Załącznik nr 3. Zakres zadań Administratora Systemu Informatycznego

Administratora systemów informatycznych (ASI) w Powiatowym Centrum Pomocy Rodzinie w Tucholi obowiązuje następujący zakres zadań:

1) monitorowanie oraz zapewnianie ciągłości działania systemów informatycznych,
2) utrzymywanie, konfigurowanie i monitorowanie wydajności systemów informatycznych,
3) instalacja i konfiguracja sprzętu i aplikacji,
4) administracja oprogramowania systemowego w celu zachowania bezpieczeństwa i integralności systemów informatycznych oraz zabezpieczenia danych a w szczególności danych osobowych przed bezprawnym dostępem osób trzecich,
5) konserwacja oprogramowania i systemów informatycznych,
6) współpraca z licencjodawcami i innymi dostawcami oprogramowania,
7) zarządzanie kopiami zapasowymi, w tym danych osobowych zgodnie z otrzymanym upoważnieniem.

Załącznik nr 4. Obszar przetwarzania danych.

Lp	Nazwa obszaru (wykaz pomieszczeń)	Lokalizacja adres	Osoba, osoby użytkujące pomieszczenie	uwagi
1.	Pokój 2.11	Ul. Kościuszki 16, 89-500 Tuchola	Paulina Grzonkowska Janina Jagła Marcin Scheffs	
2.	Pokój 2.12	Ul. Kościuszki 16, 89-500 Tuchola	Joanna Klewicz Przemysław Zysnarski	
3.	Pokój 2.13	Ul. Kościuszki 16, 89-500 Tuchola	Joanna Gumińska	
4.	Pokój 2.23	Ul. Kościuszki 16, 89-500 Tuchola	Julia Wiśniewska Magdalena Zakryś	
5.	Pokój 2.24	Ul. Kościuszki 16, 89-500 Tuchola	Kinga Czapiewska Katarzyna Kotowska Anna Szwinkowska	
6.	Pokój 2.25	Ul. Kościuszki 16, 89-500 Tuchola	Magdalena Gierszewska Kamila Synak	
7.	Pokój 2.26	Ul. Kościuszki 16, 89-	Hanna Zielinska	

		500 Tuchola		
8.	Pokój 2.28	Ul. Kościuszki 16, 89-500 Tuchola	Natalia Kamecka Alina Kowalska-Wamka	
9.	Pokój 2.29	Ul. Kościuszki 16, 89-500 Tuchola	Bernadeta Kądziela-Niemczewska	
10.	Pokój 2.30	Ul. Kościuszki 16, 89-500 Tuchola	Adrian Czapiewski Ewa Weltrowska	
11.	Pokój 2.32	Ul. Kościuszki 16, 89-500 Tuchola	Anna Toby	

Załącznik nr 6. Oświadczenie o znajomości i przestrzeganiu przepisów i zasad ochrony danych oraz zachowaniu tajemnicy danych osobowych

....., dnia.....

.....

(imię i nawiązko, stanowisko)

Oświadczenie

Ja, niżej podpisany/a, zapoznałem/łam się i zrozumiałem/am zasady, reguły i postanowienia powszechnie obowiązujących przepisów o ochronie danych osobowych (rozporządzenie 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 i ustawy z 10 maja 2018 r. o ochronie danych osobowych) oraz Polityką Ochrony Danych Osobowych obowiązującej w Powiatowym Centrum Pomocy Rodzinie w Tucholi oraz zobowiązuję się do ich przestrzegania.

Ponadto w związku z udzielonym w dniu ..... upoważnieniem do przetwarzania danych osobowych, zobowiązuję się do zachowania w tajemnicy wszelkich informacji o danych osobowych uzyskanych w trakcie dokonywania operacji związanych z przetwarzaniem danych osobowych oraz informacji o ich zabezpieczeniu. Powyższej tajemnicy zobowiązuję się dochować również po zakończeniu zatrudnienia.

.....

(podpis pracownika)

Załącznik nr 6. Upoważnienie do przetwarzania danych osobowych

....., dnia .....

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej **RODO** – nadaję upoważnienie Pani/Panu:

.....
(imię i nazwisko)

.....
(stanowisko)

do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku.

Upoważnienie obejmuje uprawnienie do przetwarzania danych:
.....

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, innych aktami prawnymi a także z wewnętrzną Polityką ochrony danych osobowych.

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 .....

Okres ważności
od:
do:

.....
podpis osoby uprawnionej do nadania upoważnienia

Data wygaśnięcia* .....
Odwołano, dnia .....

.....
podpis osoby uprawnionej do odwołania upoważnienia

* Data rozwiązania stosunku pracy

Załącznik nr 9. Procedura zarządzania ryzykiem

Sposób oceny prawdopodobieństwa wystąpienia ryzyka:

Prawdopodobieństwo wystąpienia ryzyka	Ilość punktów	Przesłanki
wysokie	3	Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się wielokrotnie w ciągu roku.
średnie	2	Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się kilkakrotnie w ciągu roku.
niskie	1	Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się raz lub nie zdarzy się w ciągu roku.

Sposób oceny skutku ryzyka:

Skutek wystąpienia ryzyka	Ilość punktów	Przesłanki
wysokie	3	Poważne zagrożenie realizacji czynności Długotrwały i trudny proces przywracania stanu poprzedniego
średnie	2	Spadek efektywności działania i obniżenie jakości wykonywania zadań. Trudny proces przywracania stanu poprzedniego.
niskie	1	Zakłócenie lub opóźnienie w wykonywaniu zadań. Skutki łatwe do usunięcia.

Progi akceptowalności ryzyka	
1-2 ryzyko nieznaczne	akceptowalne
3-5 ryzyko umiarkowane	akceptowalne
6-9 ryzyko wysokie	nieakceptowalne

1.	2.	3.	4.	5.	6.
Lp	Rodzaj ryzyka	Prawdopodobieństwo wystąpienia ryzyka (od 1 do 3)	Skutek ryzyka w skali (od 1 do 3)	Wysokość ryzyka (iloczyn kolumn 5x6)	Środki techniczne i organizacyjne w celu zmniejszenia ryzyka
1.	Nieuprawniony dostęp do pomieszczenia, w którym są przetwarzane dane osobowe	2	1	2	- szkolenia dla pracowników - monitoring budynku - przechowywanie kluczy w zamkniętej kasetce
2.	Ujawnienie haseł dostępu do stanowiska komputerowego, na którym przetwarzane są dane osobowe	1	3	3	- okresowa zmiana haseł dostępu - rejestrowanie czynności prowadzonych na komputerze
3.	Utrata nośnika zawierającego dane osobowe	1	1	1	- okresowe archiwizowanie danych - zakup nowych nośników
4.	Nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym	1	1	1	- szkolenia dla pracowników
5.	Atak wirusa, włamanie do systemu komputerowego	3	1	3	- szkolenia dla pracowników - zabezpieczenie komputerów (program antywirusowy, firewall) - używanie tylko zaufanych programów pochodzących
6.	Klęska żywiołowa, wypadek, pożar, zalanie lub inne zdarzenie, w wyniku których utracono poufność danych osobowych	1	3	3	- okresowe próbne alarmy - wdrożenie odpowiednich procedur na wypadek

					zdarzeń losowych - okresowa archiwizacja danych
7.	Błędy i pomyłki użytkowników	3	1	3	- szkolenia pracowników - kontrola zarządcza - okresowy audyt
8.	Awaria sprzętu (w tym utrata dostaw prądu)	2	2	4	- okresowe przeglądy techniczne - stopniowa wymiana sprzętu - archiwizacja danych na nośnikach zewnętrznych - używanie UPS
9.	Odtworzenie z powtórnie wykorzystanych lub wyrzuconych nośników	1	3	3	- trwałe usuwanie nośników danych przez wyspecjalizowane firmy
10.	Nieautoryzowane użycie urządzeń	1	3	3	- szkolenia pracowników - wymuszanie zmiany haseł dostępu - nadawanie unikalnych loginów i haseł użytkownikom
11.	Nielegalne przetwarzanie danych osobowych	1	3	3	- szkolenia pracowników - okresowy audyt przetwarzania danych (w tym dokumentów dane zawierających)

Załącznik nr 10. Procedura postępowania w przypadku naruszenia danych osobowych

Postępowanie w przypadku naruszenia danych osobowych

§ 1

1. Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.
2. Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

1) nieautoryzowany dostęp do danych;
2) nieautoryzowane modyfikacje lub zniszczenie danych;
3) udostępnienie danych nieautoryzowanym podmiotom;
4) nielegalne ujawnienie danych;
5) pozyskiwanie danych z nielegalnych źródeł.

§ 2

1. Każdy pracownik, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązany niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu. Przełożony zgłasza fakt Inspektorowi ochrony danych.
2. Typowe sytuacje, gdy użytkownik powinien powiadomić Inspektora ochrony danych:

1) ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
2) dokumentacja jest niszczona bez użycia niszczarki;
3) fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
4) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, 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.;
5) niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych;

6) ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe;
7) wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia;
8) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;
9) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
10) telefoniczne próby wyłudzenia danych osobowych;
11) kradzież komputerów lub twardych dysków z danymi osobowymi;
12) utrata kontroli nad kopią danych osobowych;
13) maile zachęcające do ujawnienia identyfikatora i/lub hasła;
14) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
15) istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki";
16) hasła do systemów przechowywane są w pobliżu komputera.

§ 3

Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia .

§ 4

W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora ochrony danych lub innej osoby upoważnionej przez Administratora danych.

§ 5

Administrator Systemu Informatycznego jest zobowiązany do informowania Inspektora ochrony danych o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

§ 6

Inspektor ochrony danych podejmuje następujące kroki:

1) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy,
2) odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
3) nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).

§ 7

Inspektor ochrony danych dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając raport - wzór nr 1.

§ 8

Inspektor ochrony danych zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych) – wzór nr 2 - rejestr incydentów i działań korygujących i zapobiegawczych

§ 9

Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

§ 10

1. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi Ochrony Danych Osobowych, chyba że jest mało prawdopodobne,

by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia - wzór nr 3.

2. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:

1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
2) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
4) opisywać środki zastosowane lub proponowane przez Administratora w celu zapobiegania naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach - środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

3. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania art. 33 RODO.

§ 11

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w § 10 ust. 2 lit. b), c) i d).
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:

1) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

2) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1; c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Wzór nr 1

RAPORT Z NARUSZENIA OCHRONY DANYCH

1. Data ..... Godzina .....

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe):

.....

3. Lokalizacja zdarzenia (nr pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

.....

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

.....

5. Podjęte działania:

.....

6. Wstępna ocena przyczyn wystąpienia naruszenia:

.....

7. Postępowanie wyjaśniające i naprawcze:

.....

....

(podpis pracownika) (data i podpis inspektora ochrony danych)

Wzór nr 2

REJESTR INCYDENTÓW BEZPIECZEŃSTWA

Zadanie / problem / incydent (*podać opis incydentu*)	Źródło zgłoszenia (*podać źródło zgłoszenia np. zawiadomienie, kontrola, itd.*)	Data rozpoczęcia	Data zakończenia	Odpowiedzialny za realizację (*podać dane osoby lub funkcje osoby odpowiedzialnej*)	Przyczyna niezgodności (*podać przyczynę powstania incydentu*)	Działanie korygujące / zapobiegawcze (*opisać działania jakie podjęto w celu przywrócenia bezpieczeństwa*)	Ocena skuteczności (*opisać jakie skutki przyniosło działanie korygujące*)

Wzór nr 3

Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

Opis procedury zgłaszania naruszenia
https://uodo.gov.pl/pl/134/233

Organem właściwym do zgłaszania naruszeń ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO).

1. Zgłoszenia naruszenia dokonuje się elektronicznie za pomocą odpowiedniego formularza, który należy wypełnić a następnie...

2. ...załączyć do pisma ogólnego dostępnego na platformie **biznes.gov.pl** bądź wysłać przez elektroniczną skrzynkę podawczą **ePUAP: /UODO/SkrytkaESP**

Załącznik nr 11. Polityka realizacji praw osób, których dane dotyczą

1. Podstawy przetwarzania danych osobowych przez Administratora

1.1. Przetwarzanie **danych osobowych zwykłych** przez Administratora jest zgodne z prawem wyłącznie wtedy, gdy (art. 6 ust. 1 RODO):

a) osoba, której dane dotyczą, wyraziła zgodę na ich przetwarzanie (art. 6 ust. 1 lit a RODO),
b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą lub jest konieczne do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (art. 6 ust. 1 lit b RODO),
c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit c RODO),
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej (art. 6 ust. 1 lit d RODO),
e) przetwarzanie jest niezbędne do wykonywania zadania realizowanego w interesie publicznym (art. 6 ust. 1 lit e RODO),
f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub prawa i wolności osoby, której dane dotyczą (art. 6 ust. 1 lit f RODO). Na przesłankę prawnie uzasadnionego interesu realizowanego przez administratora lub osobę trzecią nie mogą się powołać organy publiczne w ramach wykonywania swoich zadań.

1.2 Przetwarzanie **szczególnych kategorii danych (wrażliwych)** jest co do zasady zabronione. Jednak art. 9 ust. 2 RODO przewiduje zamknięty katalog przesłanek, a spełnienie choć jednej uprawnia Administratora do przetwarzania tego rodzaju danych osobowych.
W przypadku Administratora będą to najczęściej:

a) udzielenie przez osobę, której dane dotyczą, lub przez jej opiekuna prawnego (w przypadku niepełnoletnich), wyraźnej zgody na przetwarzanie danych w konkretnym celu lub celach (art. 9 ust. 2 lit a RODO),
b) niezbędność przetwarzania danych do wypełnienia obowiązków i wykonywania poszczególnych praw przez administratora lub osobę, której dane dotyczą w dziedzinie prawa pracy, zabezpieczenia socjalnego i społecznego (art. 9 ust. 2 lit b RODO);
c) niezbędność przetwarzania danych do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej, o ile osoba, której dane dotyczą jest niezdolna do wyrażenia zgody (art. 9 ust. 2 lit c RODO);
d) przetwarzanie danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą (art. 9 ust. 2 lit e RODO);
e) niezbędność przetwarzania danych ze względów związanych z ważnym interesem publicznym, o ile przepisy nie naruszają istoty prawa do ochrony danych (art. 9 ust. 2 lit g RODO);
f) niezbędność przetwarzania danych do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy (art. 9 ust. 2 lit. h RODO);

g) niezbędność przetwarzania danych do celów archiwalnych w interesie publicznym, do celów badań naukowych, historycznych lub statystycznych (art. 9 ust. 2 lit j RODO).

1.4. Każda z przesłanek legalności przetwarzania danych z pkt 1.1 i 1.2 ma charakter samodzielny. Spełnienie przynajmniej jednej z nich uprawnia Administratora do ich przetwarzania.

1.5. Podstawą prawną przetwarzania danych osobowych podmiotów danych przez Administratora jest przede wszystkim **wypełnienie obowiązku prawnego** określanego przepisami polskich ustaw pozostających w związku z realizacją zadań z zakresu pomocy społecznej (art. 6 ust. 1 lit.c RODO). Przede wszystkim są to:

a) Ustawy z dnia 9 czerwca 2011 r. o wspieraniu rodziny i systemie pieczy zastępczej;

b) Ustawy z dnia 12 marca 2004 r. o pomocy społecznej;

c) Ustawy z dnia 28 listopada 2003 r. o świadczeniach rodzinnych;

d) Ustawy z dnia 11 listopada 2016 r. o pomocy państwa w wychowaniu dzieci;

e) Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu przemocy w rodzinie;

f) Ustawa z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych;

g) Ustawa z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności w perspektywie finansowej 2014-2020;

h) Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy;

i) Ustawa z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych;

1.6. Co do zasady Administrator w związku z wypełnianiem obowiązków prawnych nie musi uzyskiwać zgody podmiotu danych na przetwarzanie danych osobowych. O zgodę na przetwarzanie danych osobowych należy prosić jedynie wtedy, gdy nie istnieją inne przesłanki przetwarzania danych.

2. Obowiązek informacyjny z art. 13 i 14 RODO

2.1. Administrator przekazuje podmiotom danych informacje, o których mowa w art. 13 i 14 RODO w zwięzłej, przejrzystej, zrozumiałej oraz łatwo dostępnej formie, a także jasnym i prostym językiem, w tym w formie graficznej.

2.2. Obowiązek informacyjny może być zrealizowany poprzez podjęcie co najmniej 2 ze wskazanych poniżej działań podjętych jednocześnie przez Administratora:

a) umieszczenie klauzul informacyjnych w dokumentach przekazywanych podmiotowi danych; lub

b) umieszczenie klauzul informacyjnych na stronie internetowej Administratora lub w systemie informatycznym dostępnym dla podmiotu danych; lub

c) umieszczenie informacji na tablicach informacyjnych w przestrzeniach ogólnodostępnych, najczęściej wykorzystywanych przez podmiotów danych.

2.3. Obowiązki informacyjne z art. 13 ust 1-3 RODO nie mają zastosowania, gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami.

2.4. Obowiązki informacyjne z art. 14 ust. 1 - 5 RODO nie mają zastosowania, gdy - i w zakresie, w jakim:

a) osoba, której dane dotyczą, dysponuje już tymi informacjami;

b) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku;
c) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega Administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą;
d) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

2.5. Wyłączenia z obowiązków informacyjnych dla podmiotów wykonujących zadania publiczne:

Obowiązek informacyjny z RODO	**Wyłączenia z obowiązku informacyjnego**
Art. 13 ust. 3 RODO Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2.	**Nowa ustawa z 10 maja o ochronie danych osobowych** Art. 3. 1. Administrator wykonujący zadanie publiczne nie przekazuje informacji, o których mowa w art. 13 ust. 3 rozporządzenia 2016/679, jeżeli zmiana celu przetwarzania służy realizacji zadania publicznego i niewykonanie obowiązku, o którym mowa w art. 13 ust. 3 rozporządzenia 2016/679, jest niezbędne dla realizacji celów, o których mowa w art. 23 ust. 1 tego rozporządzenia, oraz przekazanie tych informacji: 1) uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego lub 2) naruszy ochronę informacji niejawnych. 2. W przypadku, o którym mowa w ust. 1, administrator zapewnia odpowiednie środki służące ochronie interesu lub podstawowych praw i wolności osoby, której dane dotyczą. 3. Administrator jest obowiązany poinformować osobę, której dane dotyczą, na jej wniosek, bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od dnia otrzymania wniosku, o podstawie nieprzekazania informacji, o których mowa w art. 13 ust. 3 rozporządzenia 2016/679.
Art. 14 ust. 5 RODO 1. Ust. 1– 4 nie mają zastosowania,	**Nowa ustawa z 10 maja o ochronie danych osobowych**

gdy – i w zakresie, w jakim: a) osoba, której dane dotyczą, dysponuje już tymi informacjami; b) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1, lub o ile obowiązek, o którym mowa w ust. 1 niniejszego artykułu, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie; c) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub d) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.	Art. 4. 1. W zakresie nieuregulowanym w art. 14 ust. 5 rozporządzenia 2016/679 administrator wykonujący zadanie publiczne nie przekazuje informacji, o których mowa w art. 14 ust. 1, 2 i 4 rozporządzenia 2016/679, jeżeli służy to realizacji zadania publicznego i niewykonanie obowiązku, o którym mowa w art. 14 ust. 1, 2 i 4 rozporządzenia 2016/679, jest niezbędne dla realizacji celów, o których mowa w art. 23 ust. 1 tego rozporządzenia, oraz przekazanie tych informacji: 1) uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego lub 2) naruszy ochronę informacji niejawnych. 2. W przypadku, o którym mowa w ust. 1, administrator zapewnia odpowiednie środki służące ochronie interesu lub podstawowych praw i wolności osoby, której dane dotyczą. 3. Administrator jest obowiązany poinformować osobę, której dane dotyczą, na jej wniosek, bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od dnia otrzymania wniosku, o podstawie nieprzekazania informacji, o których mowa w art. 14 ust. 1, 2 i 4 rozporządzenia 2016/679.
Art. 15 ust. 1-3 RODO 1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji: a) cele przetwarzania; b) kategorie odnośnych danych osobowych; c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w	**Nowa ustawa z 10 maja o ochronie danych osobowych** Art. 5. 1. Administrator wykonujący zadanie publiczne nie przekazuje informacji, o których mowa w art. 15 ust. 1–3 rozporządzenia 2016/679, jeżeli służy to realizacji zadania publicznego i niewykonanie obowiązków, o których mowa w art. 15 ust. 1–3 rozporządzenia 2016/679, jest niezbędne dla realizacji celów, o których mowa w art. 23 ust. 1 tego rozporządzenia, oraz wykonanie tych obowiązków: 1) uniemożliwi lub znacząco utrudni

szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych; d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu; e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania; f) informacje o prawie wniesienia skargi do organu nadzorczego; g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle; h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. 2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46, związanych z przekazaniem. 3. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.	prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego lub 2) naruszy ochronę informacji niejawnych. 2. W przypadku gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1 i 3 rozporządzenia 2016/679, wymaga niewspółmiernie dużego wysiłku związanego z wyszukaniem danych osobowych, administrator wykonujący zadanie publiczne wzywa osobę, której dane dotyczą, do udzielenia informacji pozwalających na wyszukanie tych danych. Przepis art. 64 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2017 r. poz. 1257 oraz z 2018 r. poz. 149 i 650) stosuje się odpowiednio. 3. W przypadkach, o których mowa w ust. 1 i 2, administrator zapewnia odpowiednie środki służące ochronie interesu lub podstawowych praw i wolności osoby, której dane dotyczą. 4. Administrator jest obowiązany poinformować osobę, której dane dotyczą, na jej wniosek, bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od dnia otrzymania wniosku, o podstawie niewykonania obowiązków, o których mowa w art. 15 ust. 1–3 rozporządzenia 2016/679.

2.6 W przypadku, w którym Administrator wchodzi w posiadanie danych osobowych podmiotu danych w sposób inny niż od osoby, której dane dotyczą, ale w związku z realizacją

zadań publicznych, Administrator nie musi realizować wobec podmiotu danych obowiązku informacyjnego. Podstawą wyłączenia tego obowiązku jest art. 14 ust. 5 lit. c RODO, tj. pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą.

3. Prawo podmiotu danych do dostępu do swoich danych (art. 15 RODO)

3.1. Podmiot danych jest uprawniony do uzyskania od Administratora potwierdzenia, czy przetwarzane są dane osobowe jego dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich
3.2. Administrator dostarcza podmiotowi danych (na wniosek) kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli podmiot danych zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się w powszechnie stosowanej formie elektronicznej.
3.3 Podmiot danych ma również prawo żądać od Administratora informacji z art. 13 i 14 RODO.

4. Prawo podmiotu danych do sprostowania i uzupełnienia danych osobowych (art. 16 RODO)

4.1. Podmiot danych ma prawo zażądać w każdym momencie niezwłocznego sprostowania danych osobowych go dotyczących, które przetwarza Administrator. Ma również prawo żądania uzupełnienia niekompletnych danych osobowych na jego temat przetwarzanych przez Administratora, w tym poprzez przedstawienie dodatkowego oświadczenia.
4.2. Wraz z wykonaniem żądania podmiotu danych dotyczącego sprostowania lub uzupełnienia danych osobowych, wprowadzający dokonuje oceny istotności i charakteru sprostowań i uzupełnień.

5. Prawo podmiotu danych do bycia zapomnianym (art. 17 RODO)

5.1. Prawo podmiotu danych do bycia zapomnianym nie znajduje zastosowania wobec danych osobowych przetwarzanych na podstawie art. 6 ust. 1 lit c RODO, w tym w szczególności wobec danych przetwarzanych w ramach wykonania zadania realizowanego w interesie publicznym na podstawie art. 6 ust. 1 lit e RODO.
5.2. Administrator odmawia zrealizowania prawa podmiotu danych do bycia zapomnianym w odniesieniu do danych osobowych zawartych w dokumentacji Administratora przez cały wymagany przepisami prawa okres archiwizacji dokumentacji.
5.3. W przypadku gdy przetwarzanie danych osobowych podmiotu danych odbywa się na podstawie zgody może zrealizować prawo do bycia zapomnianym w zakresie celu, w którym dane osobowe są przetwarzane na podstawie tej zgody, pod warunkiem że zachodzi przynajmniej jedna z przesłanek wskazanych w art. 17 ust. 1 RODO. Czyli jeśli:

a) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie;

b) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust.1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;
c) dane osobowe były przetwarzane niezgodnie z prawem;
d) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii;
e) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

6. Prawo podmiotu danych do żądania ograniczenia przetwarzania danych (art. 18 RODO)

Pomimo żądania przez podmiot danych ograniczenia przetwarzania zgodnie z przesłanką określoną w art. 18 ust. 1 lit a RODO (tj - osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych) - w odniesieniu do danych osobowych podmiotów danych przetwarzanych na podstawie art. 6 ust. 1 lit c oraz e RODO, Administrator może przetwarzać te dane w dotychczasowym zakresie, bowiem ograniczenie przetwarzania danych dokonywanego w wyżej wymienionych celach mogłoby istotnie utrudnić realizację tych celów.

7. Prawo podmiotu danych do przenoszenia danych (art. 20 RODO)

7.1. Prawo podmiotu danych do przenoszenia danych nie znajduje zastosowania wobec danych osobowych przetwarzanych przez Administratora na podstawie art. 6 ust. 1 lit. c, e RODO.
7.2. W przypadku otrzymania żądania podmiotu danych związanego z wykonywaniem prawa do przenoszenia danych w odniesieniu do danych osobowych zgromadzonych w dokumentacji Administratora, Administrator ma obowiązek poinformować podmiot danych o braku możliwości wykonywania tego prawa oraz poinformować o trybie w jakim może on uzyskać dostęp do swoich danych.

8. Prawo interesanta do sprzeciwu wobec przetwarzania danych osobowych (art. 21 RODO)

Prawo podmiotu danych do sprzeciwu wobec przetwarzania danych osobowych nie znajduje zastosowania wobec danych osobowych przetwarzanych przez Administratora na podstawie art. 6 ust. 1 lit. c RODO.

9. Przetwarzanie danych na podstawie zgody podmiotu danych

9.1 Jeżeli przetwarzanie danych odbywa się na podstawie zgody Administrator musi być w stanie wykazać, że osoba, której dane dotyczą (lub w przypadku osób niepełnoletnich – jej opiekun prawny), wyraziła zgodę na przetwarzanie swoich danych osobowych.

9.2 Jeżeli oświadczenie zgody jest zawarte w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

9.3 Zgoda może być w dowolnym momencie wycofana. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. O możliwości wycofania zgody należy poinformować podmiot danych zanim wyrazi zgodę, a wycofanie zgody musi być równie łatwe jak jej wyrażenie.

9.4 Każda zgoda na przetwarzanie danych powinna charakteryzować się następującymi cechami:

1) dobrowolność – zgoda może być ważna tylko jeżeli osoba, której dane dotyczą, ma możliwość dokonania rzeczywistego wyboru, przy czym nie zachodzi ryzyko wprowadzenia w błąd, zastraszenia, przymusu lub znaczących negatywnych konsekwencji, jeśli nie wyrazi zgody; jeżeli konsekwencje wyrażenia zgody nie dają się pogodzić ze swobodą wyboru, zgoda nie jest dobrowolna;
2) konkretność – aby zgoda była ważna, musi być konkretna; innymi słowy, niedopuszczalna jest ogólna zgoda bez określenia dokładnego celu przetwarzania;
3) świadomość – zgoda na przetwarzanie danych osobowych nie może mieć charakteru abstrakcyjnego (np. wyrażam zgodę na przetwarzanie danych osobowych w celach marketingowych.), lecz winna odnosić się do skonkretyzowanego stanu faktycznego, obejmując tylko określone dane oraz sprecyzowany sposób i cel ich przetwarzania; aby wyrażenie zgody było świadome, osoba, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych;
4) jednoznaczność – zgoda musi mieć charakter wyraźny, a jej wszystkie aspekty muszą być jasne dla podpisującego w momencie jej wyrażania.

9.5. Zgoda nie powinna stanowić podstawy prawnej w sytuacji, w której istnieje wyraźny brak równowagi między podmiotem danych, a administratorem, np. pracownik – pracodawca.

9.6. Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania przez podmiot danych nie może oznaczać zgody.

9.7. Sposoby wyrażenia zgody:

1) pisemne (w tym elektroniczne) lub ustne oświadczenie woli;
2) wyraźne działanie potwierdzające (zgoda „konkludentna"):

a) zapisanie się do serwisu rozsyłającego wiadomości (listy mailingowej czy newslettera),
b) inne oświadczenie bądź zachowanie, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych.

Załącznik nr 12. Polityka korzystania z usług podmiotów przetwarzających

1. Powierzenie przetwarzania danych osobowych polega na przekazaniu danych podmiotowi trzeciemu, który przetwarza dane w imieniu i na rzecz Administratora.
2. Administrator przy wyborze podmiotu trzeciego, o którym mowa w ust. 1, kieruje się przede wszystkim kryterium bezpieczeństwa danych – czy ww. podmiot daje wystarczające gwarancje wdrożenia odpowiednich środków adekwatnych do ryzyka naruszenia danych osobowych, a także realizacji praw jednostki oraz innych obowiązków ochrony spoczywających na Administratorze.
3. Wskazane w ust. 1 powierzenie przetwarzania danych osobowych może się odbywać wyłącznie w trybie przewidzianym w art. 28 RODO poprzez zawarcie na piśmie lub w formie elektronicznej umowy powierzenia przetwarzania danych osobowych.
4. W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych określa się przede wszystkim zobowiązania podmiotu przetwarzającego do:
a) przetwarzania danych wyłącznie na udokumentowane polecenie administratora;
b) zapewnienia, by osoby upoważnione do przetwarzania danych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
c) podejmowania środków zabezpieczenia danych wymaganych przez RODO i pomagania administratorowi wywiązać się z tych obowiązków;
d) przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego, w tym między innymi za zgodą Administratora;
e) pomagania Administratorowi wywiązać się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania jej praw określonych w RODO;
f) usunięcia danych lub do zwrotu danych Administratorowi danych po zakończeniu przetwarzania, zgodnie z decyzją administratora;
g) udostępniania Administratorowi wszelkich informacji niezbędnych do wykazania spełnienia jego obowiązków oraz do umożliwiania Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzania audytów;
h) uzyskania uprzedniej pisemnej zgody Administratora na powierzenie konkretnych operacji przetwarzania danych w drodze pisemnej umowy pod powierzenia, zgodnie z art. 28 ust. 2 i 4 RODO, tylko w celu wykonania umowy powierzenia;
i) nieprzekazywania danych do państwa trzeciego lub organizacji międzynarodowej,
j) prowadzenia rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora, zgodnie z art. 30 RODO.
6. Administrator prowadzi **ewidencję umów powierzania przetwarzania danych osobowych**, która stanowi wzór nr 1.

Wzór nr 1. Ewidencja umów powierzania przetwarzania danych osobowych

L.p.	Nazwa podmiotu, któremu powierzono dane	Data zawarcia umowy	Data zakończenia umowy	Zakres umowy
1.				
2.				
3.				
4.				
5.				
6.				
7.				