POLITYKA
BEZPIECZEŃSTWA INFORMACJI

1. Cel

1. Celem niniejszego dokumentu jest wprowadzenie spójnych zasad zachowania bezpieczeństwa danych osobowych w Pogodnym Domu Seniora zwanym/ą dalej PDS.

2. Polityka bezpieczeństwa informacji jest dokumentem nadrzędnym dla innych procedur oraz regulaminów z zakresu ochrony danych osobowych przyjętych w PDS.

3. Zarządzanie bezpieczeństwem informacji jest pojęciem obejmującym zasady zarządzania systemem chroniącym dane oraz sposoby reagowania na zagrożenia. Zapewnienie odpowiedniej wiedzy zarządzających PDS oraz siecią informatyczną w zakresie pojawiających się nowych zagrożeń oraz metod ochrony jest kolejnym elementem zapewnienia bezpieczeństwa. Osoby obsługujące systemy przetwarzające dane osobowe są ogniwem zabezpieczeń, na którego skuteczność wpływa również zapewnienie rzetelnej informacji w zakresie sposobu bezpiecznego użytkowania oprogramowania i sprzętu.

4. Zastosowanie niniejszej Polityki Bezpieczeństwa Informacji powinno zapewnić zabezpieczenia adekwatne i proporcjonalne do wyników szacowania ryzyka występującego dla przetwarzanych i przechowywanych danych oraz w systemach informatycznych PDS.

5. Polityka Bezpieczeństwa Informacji jest jednocześnie dokumentem określającym zadania osób funkcyjnych, pracowników oraz pracowników i współpracowników podmiotów trzecich, które na mocy zawartych umów mają dostęp do informacji chronionych. Ma ona pomóc w zapewnieniu: poufności, integralności, dostępności oraz rozliczalności przetwarzanych danych osobowych i innych zidentyfikowanych aktywów informacyjnych.

2. Zakres stosowania

1. Politykę Bezpieczeństwa Informacji stosują osoby przetwarzające dane osobowe i inne dane chronione, niezależnie od formy zatrudnienia w PDS lub formy prawnej wiążącej PDS z tą osobą. W szczególności mogą być to osoby zatrudnione na umowę o pracę, stażyści, praktykanci, wolontariusze oraz osoby realizujące zadania na podstawie podpisanej z PDS umowy cywilnoprawnej, a także pracownicy i współpracownicy podmiotów trzecich, z którymi została zawarta umowa, na mocy której ww. osoby mają dostęp do informacji chronionych, w tym do danych osobowych.

2. Polityka Bezpieczeństwa Informacji obejmuje wszystkie dane osobowe oraz inne informacje podlegające ochronie, przetwarzanych w pomieszczeniach PDS niezależnie od formy ich przetwarzania. Polityka w zakresie danych osobowych odnosi się:

a) do danych przetwarzanych w zbiorach tradycyjnych, w szczególności kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych,

b) do danych przetwarzanych w systemach informatycznych.

3. Dla skutecznej realizacji Polityki Bezpieczeństwa Informacji, Administrator zapewnia:

a) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony,

b) okresowe szacowanie ryzyka zagrożeń dla zbiorów danych,

c) okresową ocenę skutków dla ochrony danych osobowych,

d) kontrolę, monitoring i nadzór nad przetwarzaniem danych osobowych,

e) monitorowanie zastosowanych środków ochrony,

f) możliwość realizacji wytycznych zawartych w Kodeksach, o których mowa w art. 40 RODO,

g) wdrożenie odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku;

h) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

i) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

j) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

3. Definicje przyjęte w analizie legalności przetwarzania danych osobowych

1. administrator danych (ADO)- Pogodny Dom Seniora;
2. dane osobowe - 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;
3. dostępność danych - rozumie się przez to właściwość zapewniającą, że dane są udostępniane dla upoważnionego podmiotu wtedy, gdy ich potrzebuje do przetwarzania;
4. integralność danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
5. naruszenie bezpieczeństwa informacji – wszelkie zdarzenia lub działania, w tym również niezamierzone, które mogą stanowić przyczynę utraty zasobów, obniżenia wymaganego poziomu poufności, integralności, dostępności informacji lub niezawodności systemów, a także odstępstwa od obowiązujących procedur postępowania, nawet jeżeli nie prowadzą do negatywnych skutków dla organizacji. Zdarzenia lub działania, które mogą prowadzić do naruszenia praw lub wolności osób fizycznych;
6. naruszenie ochrony danych osobowych - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
7. odbiorca danych – osoba fizyczna lub prawna, organ publiczny, jednostka 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 powszechnie obowiązującym, 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. Przy czym przez sformułowanie „strona trzecia" rozumie się osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które z upoważnienia Administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
8. osoba upoważniona do przetwarzania danych osobowych – osoba, która złożyła ADO oświadczenie
o zachowaniu w tajemnicy przetwarzanych danych i stosowanych sposobach zabezpieczenia tych danych, posiadająca imienne upoważnienie wydane przez ADO, określające imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych oraz identyfikator, jeżeli dane są przetwarzane w systemie informatycznym;
9. podmiot przetwarzający – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot,
który przetwarza dane osobowe w imieniu Administratora;
10. przetwarzanie - operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie,

rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

11. poufność danych - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

12. rozliczalność danych - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą
być przypisane w sposób jednoznaczny tylko temu podmiotowi,

13. RODO - 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);

14. usuwanie danych – trwałe zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

15. uwierzytelnianie – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

16. użytkownik/pracownik (w tym podmiotu trzeciego) - osoba przetwarzająca dane w systemie oraz poza nim (np. dokumentacji w formie tradycyjnej), niezależnie od formy zatrudnienia w PDS lub formy prawnej wiążącej z tą osobą. W szczególności mogą być to osoby zatrudnione na umowę o pracę, stażyści, praktykanci, osoby realizujące zadania na podstawie podpisanej umowy cywilnoprawnej;

17. zbiór danych – to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

18. zgoda na przetwarzanie danych osobowych - oświadczenie woli osoby, której dane są przetwarzane przez administratora danych, w której wyraża swoją aprobatę dla tego procesu;

4. Obowiązki osób przetwarzających dane osobowe

1. Każda osoba przetwarzająca dane osobowe na potrzeby PDS jest obowiązana zapoznać się z treścią Polityki Bezpieczeństwa oraz bezwzględnie stosować się do jej zapisów. Osoby przetwarzające dane osobowe czynią to na podstawie wydanego przez Administratora Danych - upoważnienia (załącznik nr 1 do niniejszej Polityki).

2. Pracownicy/użytkownicy są zobowiązani są do przestrzegania przepisów prawa powszechnie obowiązującego i regulacji wewnętrznych dotyczących ochrony danych osobowych. W tym celu zobowiązani są do:

a) pisemnego wnioskowania o zewidencjonowanie nowych zbiorów danych osobowych w wykazie,

b) bieżącej oceny funkcjonowania mechanizmów zabezpieczeń i ochrony,

c) występowania z wnioskami w sprawie wprowadzenia niezbędnych zmian w zakresie ochrony danych osobowych,

3. Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych osobowych, przewidują dalej idącą ich ochronę, niż to wynika z RODO, czy Ustawy, stosuje się przepisy tych ustaw.

4. Pracownicy/użytkownicy przetwarzający dane osobowe obowiązani są dołożyć należytej staranności w celu ochrony interesu osób, których dane są gromadzone i przetwarzane, a w szczególności należy przestrzegać, aby dane te były:

a) przetwarzane zgodnie z powszechnie obowiązującym prawem i regulacjami wewnętrznymi,

b) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,

c) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,

d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania,

e) oraz by wypełniany był obowiązek informacyjny, w przypadkach wskazanych w przepisach prawa powszechnie obowiązującego.

5. Naruszenie postanowień Polityki Bezpieczeństwa Informacji może skutkować zablokowaniem dostępu pracownika/użytkownika do informacji chronionych i systemów. W przypadku ciężkich naruszeń, takie działanie może prowadzić do wszczęcia postępowania dyscyplinarnego oraz do rozwiązania bądź wypowiedzenia umowy. W przypadku poniesienia strat w wyniku naruszenia, PDS może dochodzić roszczeń odszkodowawczych na drodze sądowej.

6. Każde naruszenie bezpieczeństwa informacji powinno być niezwłocznie zgłaszane Administratorowi Danych.

7. W razie wykrycia naruszenia ochrony informacji chronionych każdy pracownik ma obowiązek postępować zgodnie z procedurami zawartymi w Dokumentacji.

8. Osoby odpowiedzialne za zarządzanie kadrami w PDS informują niezwłocznie Administratora Danych o każdej zmianie w zakresie czynności pracowników, która wiąże się ze zmianą zakresu uprawnień do przetwarzania informacji chronionych.

9. Cofnięcie upoważnień do przetwarzania informacji chronionych powinno nastąpić niezwłocznie po zakończeniu wykonywania obowiązków pracownika/użytkownika.

10. Rozliczenie pracownika z aktywów związanych z przetwarzaniem informacji chronionych powinno odbywać się na podstawie procedur określonych przez Administratora Danych.

5. Obszary przetwarzania danych osobowych

1. W PDS dane osobowe przetwarzane są w ramach zbiorów danych osobowych, a obszary możliwego przetwarzania danych osobowych określa załącznik nr 2 do niniejszej Polityki Bezpieczeństwa Informacji.

2. Osoby upoważnione do przetwarzania danych osobowych mogą przetwarzać dane tylko wyznaczonych do tego miejscach z zachowaniem dedykowanego do tej czynności - sprzętu oraz wszelkich innych urządzeń.

3. Wynoszenie zbiorów danych osobowych poza obszar przetwarzania możliwy jest za wyłączną zgodą Administratora Danych.

6. Charakterystyka zbiorów danych osobowych

1. Wykaz prowadzonych w PDS zbiorów danych osobowych stanowi załącznik nr 3 do niniejszej Polityki Bezpieczeństwa Informacji.

2. Przetwarzanie danych osobowych, zgodnie z celem działalności, jest możliwe, jeżeli jest to niezbędne do wypełnienia usprawiedliwionych interesów Administratora, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Przetwarzanie jest również dozwolone, gdy osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych lub jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą. W szczególności można przetwarzać dane osobowe, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa, a także gdy jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.

3. Osoby przetwarzające zgromadzone dane są zobowiązane w szczególności do:

a) przetwarzania danych zgodnie z aktami prawa powszechnie obowiązującego lub aktami prawa wewnętrznego, w zakresie zgodnym z upoważnieniem podpisanym przez Administratora;

b) modyfikowania i usuwania danych, zgodnie z wnioskiem złożonym przez osobę, której dane dotyczą oraz ograniczenia przetwarzania danych.

7. Organizacja systemu ochrony danych osobowych

1. Administrator Danych Osobowych odpowiada za zakres i bezpieczeństwo przetwarzania danych osobowych w PDS.

2. Administrator jest odpowiedzialny za przestrzeganie przepisów RODO i musi być w stanie wykazać ich przestrzeganie (tzw. zasada rozliczalności RODO). Administrator zapewnia:

a) przetwarzanie danych osobowych zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość"),

b) zbieranie danych osobowych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami („ograniczenie celu").

c) adekwatność danych osobowych; dane osobowe powinny być stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych").

d) prawidłowość danych osobowych i w razie potrzeby ich uaktualnianie; podejmuje wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość").

e) przechowywanie danych osobowych w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania").

f) przetwarzanie w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

g) Administrator zapewnia i stosuje odpowiednie środki informatyczne, techniczne i organizacyjne (wykaz w/w środków stanowi załącznik nr 8 do niniejszej Polityki), zapewniając ochronę przetwarzanych danych osobowych odpowiednią do wyników analizy ryzyka, a w szczególności:

- podejmuje decyzje o celach i środkach przetwarzanie danych osobowych,
- podejmuje decyzje o technicznych i organizacyjnych zabezpieczeniach oraz wdraża zasady i procedury postępowania mające na celu zapewnienie adekwatnego poziomu bezpieczeństwa przetwarzanych danych,
- upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnym zakresie, odpowiadającym zakresowi jej obowiązków,
- podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych osobowych,
- prowadzi kontrolę przestrzegania procedur przetwarzania danych osobowych,
- zapewnia środki techniczne oraz organizacyjne w celu zapewnienia działań wymaganych przez przepisy prawa dotyczące ochrony danych osobowych,
- zapewnia realizację praw osób, których dane osobowe są przetwarzane (m. in. prawo wglądu, poprawiania danych i wniesienia sprzeciwu wobec przetwarzanych danych),
- reprezentuje PDS w postępowaniach przed organami publicznymi oraz w kontaktach z podmiotami trzecimi w sprawach związanych z pozyskiwaniem, przetwarzaniem, ochroną i powierzeniem danych osobowych,

▪ zapewnia udział osób o odpowiednich kompetencjach i wiedzy (pracowników Administratora i podmiotów zewnętrznych) przy realizacji audytów i weryfikacji systemu ochrony danych osobowych,

▪ zapewnia bezpieczne usunięcie danych osobowych w przypadku uzasadnionego żądania niezwłocznego usunięcia danych osobowych, bez zbędnej zwłoki.

3. Sposób udzielania upoważnień do przetwarzania danych osobowych:

a) do przetwarzania danych osobowych mogą być dopuszczone tylko osoby upoważnione przez Administratora, który w zależności od potrzeb jednostki może opracować procedurę nadawania upoważnień do przetwarzania danych osobowych uwzględniającą sposób nadawania uprawnień do systemów teleinformatycznych. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

▪ przed rozpoczęciem przetwarzania należy złożyć oświadczenie o zapoznaniu się z dokumentacją ochrony danych osobowych

▪ dane osobowe można przetwarzać wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych, zawartym w upoważnieniu i tylko w celu wykonywania obowiązków służbowych,

▪ przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia, a także po ustaniu stosunku pracy lub odwołania z pełnionej funkcji, przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres realizacji umowy, a także po zakończeniu jej realizacji,

▪ stosowanie określonych przez Administratora procedur oraz wytycznych mających na celu przetwarzanie danych zgodnie z obowiązującym prawem,

▪ zabezpieczenie danych osobowych przed udostępnieniem osobom nieupoważnionym,

▪ sposób nadawania adekwatnych uprawnień w systemach, jest wynikiem wydanego upoważnienia do przetwarzania danych osobowych, za realizację procedury nadawania uprawnień odpowiedzialny jest ADO, któremu należy zgłaszać zapotrzebowanie na zmianę zakresu upoważnień do przetwarzania danych osobowych oraz uprawnień do systemów,

▪ zakres dostępu do danych gromadzonych w systemie przypisany jest do niepowtarzalnych identyfikatorów użytkownika, niezbędnych do pracy w systemach oraz aplikacjach, do których Użytkownik otrzymał stosowne uprawnienia na podstawie podpisanego upoważnienia do przetwarzania danych,

▪ w aktach osobowych pracownika przechowuje się egzemplarz oryginalny upoważnienia do przetwarzania danych osobowych podpisany własnoręcznie przez pracownika, co jednocześnie jest potwierdzeniem, że pracownik przyjął treść upoważnienia do wiadomości,

▪ Rozwiązanie stosunku pracy lub odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych.

▪ W przypadku naruszenia przez pracownika/użytkownika przepisów lub zasad postępowania może podlegać on odpowiedzialności służbowej i karnej,

▪ Upoważnienia do przetwarzania danych osobowych udzielane są również wolontariuszom, praktykantom, stażystom, zakończenie stażu, praktyki, wolontariatu powoduje wygaśnięcie upoważnienia.

4. Zbieranie danych osobowych:

a) Dane osobowe przetwarzane w PDS mogą być pozyskiwane bezpośrednio od osób, których te dane dotyczą. W przypadku zbierania danych osobowych nie od osoby, której te dane dotyczą, należy zapewnić, że istnieje podstawa prawna przetwarzania danych,

b) Przetwarzanie i przechowywanie danych osobowych powinno odbywać się w postaci umożliwiającej identyfikację osób, których dotyczą.

c) Przetwarzanie i przechowywanie danych osobowych powinno odbywać się nie dłużej niż jest to niezbędne do realizacji celu przetwarzania.

d) Dane osobowe, które są zbierane powinny być merytorycznie poprawne.

e) Zakres danych osobowych, które są zbierane, powinien być adekwatny w stosunku do celu, w jakim dane zostały zebrane.

f) Zebrane dane po ich wykorzystaniu mogą być przechowywane w przypadku, gdy uprzednio zostaną poddane procesowi anonimizacji, czyli procesowi, który ma na celu uniemożliwienie identyfikacji osób, których dotyczą dane.

g) Zebrane dane po ich wykorzystaniu mogą być przechowywane w przypadku, gdy odpowiedni przepis prawa wymaga ich archiwizacji przez określony czas.

h) Przetwarzanie danych osobowych kandydata do pracy jest możliwe podczas procesu rekrutacji wyłącznie po uzyskaniu jego pisemnego oświadczenia zawierającego zgodę na przetwarzanie jego danych osobowych w celu przeprowadzenia procesu rekrutacyjnego lub przyszłych procesów rekrutacyjnych. W przypadku wymagań wynikających z zapisów odpowiednich przepisów prawa, po zakończeniu procesu rekrutacji dokumenty zawierające dane osobowe kandydatów do pracy są archiwizowane zgodnie z zapisami tych przepisów.

i) 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.

5. Obowiązek informacyjny:

a) Administrator zobowiązany jest na etapie gromadzenia danych (niezależnie od tego, czy zbiera je bezpośredniego od osób, których one dotyczą, czy też pozyskania ich od podmiotu trzeciego) powiadomić osoby, których dane gromadzi o przysługujących im prawach oraz przekazać informacje o zasadach i celu przetwarzania danych osobowych (wypełnienie „obowiązków informacyjnych" wskazanych w art. 12, 13, 14, 22 i 25 RODO),

b) Zgodnie z art. 13 ust. 1 i 2 RODO, do niezbędnych elementów informacyjnych zaliczyć należy podanie:

- nazwy i adresu Administratora oraz adresu poczty elektronicznej i numeru faksu i telefonu oraz gdy ma to zastosowanie, tożsamości i danych kontaktowych przedstawiciela Administratora,
- celu przetwarzania danych osobowych oraz podstawy prawnej przetwarzania,
- informacji o odbiorcach danych osobowych lub o kategoriach odbiorców,
- informacji o zamiarze transferu danych osobowych do państwa trzeciego, ze szczególnym uwzględnieniem:
  - przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej,
  - stwierdzenia lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony lub - w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO - wzmianki o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych,
- okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu;
- informacji o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
- jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO – informacji o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
- informacji o prawie wniesienia skargi do organu nadzorczego;
- informacji czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

▪ informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, 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.

▪ W przypadku zbierania danych osobowych z innego źródła niż od osoby, której dane dotyczą, zgodnie z art. 14 ust. 1 i 2 RODO, informacja powinna być poszerzona o:

- kategorie odnośnych danych osobowych;
- źródle pochodzenia danych osobowych, a jeżeli ma to zastosowanie, o pochodzeniu ich ze źródeł powszechnie dostępnych.

c) O ile jest to możliwe, informacje, o której mowa w pkt b każdorazowo należy przekazać indywidualnie osobie, której dane dotyczą przed podjęciem działań z jej danymi, a także dokumentować (najlepiej na piśmie podpisanym przez osobę, której dane dotyczą), że obowiązek informacyjny został wypełniony. Jeśli zamiast formy papierowej do gromadzenia danych wykorzystuje się system informatyczny to musi on zapewniać zapisanie w trwałej i wiarygodnej formie, że osoba podająca swoje dane za jego pomocą uzyskała informacje w zakresie określonym w przepisach prawa powszechnie obowiązującego. Klauzula powinna być zrozumiała dla osób, których dane mają być gromadzone i przetwarzane. Poświadczenie wykonania obowiązku informacyjnego może polegać na wypełnieniu odpowiednich formularzy (w tym w formie elektronicznej). Istotne jest, aby pola potwierdzające wyrażenie zgody na zbieranie i przetwarzanie danych w formularzu nie były domyślnie zaznaczane.

d) Informowanie powinno się dokonać bez prośby zainteresowanego. Powinno być ono wykonane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Należy uwzględniać także to, że informowana osoba musi mieć możliwość wniesienia sprzeciwu wobec przetwarzania jej danych i należy stworzyć jej warunki do wyrażenia tego sprzeciwu.

e) Wykonanie obowiązku informacyjnego jest zadaniem osoby przyjmującej dane osobowe, która o ile jest to możliwe, po otrzymaniu potwierdzenia jego wykonania (w przypadku gdy realizowany jest on w formie papierowej) przekazuje dowód wykonania obowiązku informacyjnego do Administratora Danych, lub osoby przez Administratora Danych do tego upoważnionej.

6. Informowanie o przetwarzanych danych osobowych:

a) Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych osobowych przetwarzanych i przechowywanych w PDS, a zwłaszcza prawo do uzyskania wyczerpującej informacji o przetwarzanych danych osobowych, które jej dotyczą.

b) Na wniosek osoby, której dane dotyczą, Administrator Danych jest zobowiązany do udzielania informacji zgodnie z pkt. a Informacja powinna być udzielona formie pisemnej oraz powszechnie zrozumiałej.

c) W razie wniesienia żądania oraz wykazania przez osobę, której dane osobowe dotyczą, że jej dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych osobowych, bez zbędnej zwłoki, dokonać uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne przepisy.

d) Osoba, której dane dotyczą, ma prawo wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach przetwarzania niezbędnego do wykonania określonych prawem zadań realizowanych dla dobra publicznego lub niezbędnego dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych

zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

7. Powierzanie przetwarzania danych osobowych:

a) Administrator:

▪ przekazuje dane do podmiotów trzecich zgodnie z przepisami prawa powszechnie obowiązującego, w szczególności do: Zakładu Ubezpieczeń Społecznych, Urzędu Skarbowego, Państwowej Inspekcji Pracy, sądów powszechnych, Policji i Prokuratury.

▪ powierza przetwarzanie danych osobowych innemu podmiotowi w drodze umowy zawartej
w na piśmie, która określa zasady przetwarzania i zabezpieczenia danych osobowych.

b) Umowa powierzenia danych osobowych do przetwarzania musi być zawarta w formie pisemnej w dwóch jednobrzmiących egzemplarzach dla obu stron.

c) W przypadku zawarcia umowy powierzenia przetwarzania danych osobowych z podmiotem trzecim, ADO jednocześnie zobowiązuje ten podmiot w formie pisemnej do zachowania poufności powierzanych do przetwarzania danych osobowych oraz sposobów ich zabezpieczeń. Zobowiązanie powinno pozostać w mocy również po zakończeniu przetwarzania.

d) Podmiot, któremu powierzono przetwarzanie danych osobowych, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

e) Podmiot, któremu powierzono przetwarzanie danych osobowych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie ryzyka dla danych objętych ochroną, a w szczególności powinien stosować techniczne i organizacyjne środki bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

8. Współadministrowanie danymi:

a) W przypadku wspólnego przetwarzanie danych w zbiorach przez podmioty, na mocy zawartej umowy lub porozumienia, ustalają one wspólnie cele i sposoby przetwarzania danych (są współadministratorami danych). W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z przepisów prawa powszechnie obowiązującego oraz aktów prawa wewnętrznego obowiązujących w obu podmiotach, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14 RODO, chyba że przypadające im obowiązki i ich zakres określa prawo powszechnie obowiązujące. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.

b) Uzgodnienia, o których mowa w pkt a, należycie odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a osobami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana osobom, których dane dotyczą.

c) Niezależnie od uzgodnień, o których mowa w pkt a, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z przepisów prawa powszechnego wobec każdego z Administratorów.

d) Informacja o współadministrowaniu zbiorem danych (wskazanie współadministratorów) odnotowywane jest w Rejestrze Czynności Przetwarzania.

9. Przekazanie danych do państwa trzeciego lub organizacji międzynarodowej:

a) Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja Europejska stwierdzi, że to państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.

b) W razie braku decyzji, o której mowa w pkt 1 Administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie,

gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowane prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej.

c) W razie braku decyzji stwierdzającej odpowiedni stopień ochrony określonej w pkt 1 oraz braku odpowiednich zabezpieczeń, o których mowa w pkt 2, w tym wiążących reguł korporacyjnych, jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej mogą nastąpić wyłącznie pod warunkiem, że:

▪ osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którymi – ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń – może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę,

▪ przekazanie jest niezbędne do wykonania umowy między osobą, której dane dotyczą, a administratorem lub do wprowadzenia w życie środków przed umownych podejmowanych na żądanie osoby, której dane dotyczą,

▪ przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, których dane dotyczą, między administratorem a inną osobą fizyczną lub prawną,

▪ przekazanie jest niezbędne ze względu na ważne względy interesu publicznego,

▪ przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń,

▪ przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody lub przekazanie następuje z rejestru, który zgodnie z prawem Unii lub prawem państwa członkowskiego ma służyć za źródło informacji dla ogółu obywateli i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes – ale wyłącznie w zakresie, w jakim w danym przypadku spełnione zostały warunki takiego dostępu określone w prawie Unii lub w prawie państwa członkowskiego.

▪ Szczegółowe zasady przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej określone zostały określone w RODO. O wyrażenie zgody na przekazanie danych występuje właściciel zbioru, wskazując cel i zakres przekazywanych danych. Administrator zobowiązany jest bezwzględnie przestrzegać postanowień RODO przy przekazywaniu danych do państwa trzeciego lub organizacji międzynarodowej.

8. Obowiązywanie dokumentu

Polityka Bezpieczeństwa wchodzi w życie z dniem 11.04.2023 r. i obowiązuje na wszystkich stanowiskach oraz obszarach gdzie dochodzi do przetwarzania informacji podlegających ochronie.

9. Wykaz załączników

1. załącznik nr 1 - wzór upoważnień,
2. załącznik nr 2 - wykaz obszarów przetwarzania danych osobowych,
3. załącznik nr 3 - wykaz zbiorów danych osobowych,
4. załącznik nr 4 - wniosek o realizację praw osób których dane dotyczą – WZÓR,
5. załącznik nr 5 - rejestr naruszeń ochrony danych osobowych,
6. załącznik nr 6 - rejestr umów powierzenia danych osobowych,
7. załącznik nr 7 - ewidencja wydanych upoważnień do przetwarzania danych osobowych,
8. załącznik nr 8 - wykaz środków fizycznych, technicznych oraz organizacyjnych stosowanych w celu zabezpieczenia danych oraz informacji.