ZARZĄDZENIE NR 69/2024

WÓJTA GMINY GOWOROWO

z dnia 26 lipca 2024 r.

w sprawie zmiany zarządzenia Nr 42/2018 Wójta Gminy Goworowo z dnia 29 czerwca 2018 r. w sprawie wprowadzenia Polityki Ochrony Danych oraz Instytucji Zarządzania Systemem Informatycznym

Na podstawie art. 24 ust. 1 i 2 Rozporządzenia parlamentu europejskiego i rady (ue) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/we (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L.2016.119.1 z późn. zm.) zarządzam, co następuje:

§ 1. W zarządzeniu Nr 42/2018 Wójta Gminy Goworowo z dnia 29 czerwca 2018 r. w sprawie wprowadzenia Polityki Ochrony Danych oraz Instytucji Zarządzania Systemem Informatycznym wprowadza się następujące zmiany:

1) w tytule zarządzenia wyrazy „ Polityki Ochrony Danych" zastępuje się wyrazami „Polityki Zarządzania Obszarem Ochrony Danych";

2) § 1 otrzymuje brzmienie:

„§1. Wprowadza się w Urzędzie Gminy Goworowo dokument o nazwie Polityka Zarządzania Obszarem Ochrony Danych, którego treść stanowi załącznik nr 1 do zarządzenia.";

3) załącznik Nr 1 do zarządzenia otrzymuje brzmienie jak w załączniku do niniejszego zarządzenia.

§ 2. Wykonanie zarządzenia powierza się Sekretarzowi Gminy Goworowo.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Goworowo

Piotr Kosiorek

POLITYKA ZARZĄDZANIA OBSZAREM OCHRONY DANYCH

Zatwierdzam

Spis treści

1. Cel dokumentu

Głównym celem dokumentu jest uszczegółowienie procesu zarządzania obszarem ochrony danych osobowych oraz ustanowienie konkretnych reguł, obowiązków i zasad związanych z przetwarzaniem i ochroną danych osobowych.

2. Zakres dokumentu

2.1. Dokument swoim zakresem obejmuje:

1) główne zasady przetwarzania danych osobowych;
2) prawa osób, których dane dotyczą;
3) rejestrowanie czynności przetwarzania;
4) powierzanie danych osobowych;
5) udostępnianie danych osobowych;
6) zarządzanie zabezpieczeniami
7) zasady bezpieczeństwa.

2.2. Wymagania niniejszego dokumentu obowiązują wszystkich pracowników, współpracowników lub osoby upoważnione przez administratora, bez względu na formę przetwarzania danych osobowych jak również bez względu na miejsce przetwarzania danych osobowych.

3. Podstawy prawne

3.1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

3.2. Ustawa z dnia 10 maja 2018r. o ochronie danych osobowych.

4. Role i odpowiedzialności

4.1. W dokumencie określono następujące role i odpowiedzialności:

1) **Administrator** – odpowiada za określenie celów i sposobów przetwarzania oraz wdrożenie wszelkich reguł, zasad i zabezpieczeń w obszarze ochrony danych. W ramach obowiązujących przepisów prawa

2) **Inspektor Ochrony Danych** – odpowiada za wspieranie administratora, jego pracowników oraz stosowanie się do wewnętrznych regulacji bezpieczeństwa o których mowa jest w niniejszej instrukcji oraz powiązanych dokumentach zintegrowanego systemu zarządzania bezpieczeństwem.

3) **Osoba upoważniona do przetwarzania danych osobowych** – odpowiada za zastosowanie wszelkich reguł, zasad i zabezpieczeń, o których mowa jest w przepisach prawa dot. przetwarzania danych oraz w niniejszej polityce i pozostałych dokumentach regulujących obszar bezpieczeństwa

4.2. W przypadku wątpliwości co do ról bądź odpowiedzialności w obszarze ochrony danych osobowych należy skontaktować się z Inspektorem Ochrony Danych w celu uzyskania wyczerpujących odpowiedzi na nurtujące pytania lub zagadnienia.

5. Główne zasady przetwarzania danych osobowych

Zgodnie z wymaganiami przepisów „RODO" **istnieje 7 głównych zasad** związanych z przetwarzaniem i ochroną danych osobowych, **które wskazują, że dane osobowe muszą być:**

1) *przetwarzane zgodnie z prawem, w sposób przejrzysty i rzetelny;*
2) *przetwarzane w konkretnym celu, w którym zostały pozyskane;*
3) *przetwarzane w minimalnym zakresie niezbędnym do osiągnięcia;*
4) *prawidłowe i w razie potrzeb aktualizowane;*
5) *przetwarzane przez określony czas;*
6) *przetwarzane w sposób zapewniający ich bezpieczeństwo;*
7) *przetwarzane w sposób wykazujący stosowanie powyższych zasad.*

5.1. Zasada przetwarzania danych osobowych zgodnie z prawem

5.1.1. Zrozumienie zasady zgodności, rzetelności i przejrzystości przetwarzani danych osobowych, stanowi zazwyczaj największy problem w przetwarzaniu, dlatego też poniżej przedstawiono szczegółowe mapowanie wymagań w raz z opisem, które powinno ułatwić zrozumienie i stosowanie omawianej zasady przetwarzania danych osobowych.

5.1.2. **Zgodność z niniejszą zasadą przetwarzania jest zapewniona, gdy spełnione są łącznie dwa wymagania:**

1) **posiada się prawidłową** (minimum jedną) **przesłankę legalności** przetwarzania danych osobowych;
2) wszelka **komunikacja z osobami fizycznymi prowadzona jest w oparciu o zwięzłą, przejrzystą, zrozumiałą i łatwo dostępną formę, realizowaną jasnym i prostym językiem**.

5.1.3. Dla każdej kategorii danych osobowych istnieją inne przesłanki legalności określone w *art. 6 ust. 1* lub w *art. 9 ust. 2* lub w *art. 10 RODO*.

5.1.4. **Przetwarzanie danych zwykłych jest zgodne z prawem gdy:**

1) **posiadana jest zgoda osoby, której dane dotyczą** – należy jednak pamiętać, że:
   a) **o ile jest to możliwe zgodę należy być wstanie wykazać** bez względu na fakt czy została ona pozyskana na piśmie, w rozmowie mailowej, rozmowie telefonicznej rozmowie bezpośredniej;
   b) **zgodę wyraża się w konkretnym celu**, a w przypadku gdy tych celów jest więcej należy je wyszczególnić, tak aby było wiadomo, na co wyraziła zgodę osoba fizyczna. Dla każdego celu należy zapewnić w formularzach osobną kratkę (checbox'a) do zaznaczenia. Nie dopuszczalne jest aby zgoda była domyślnie zaznaczona, musi ją własnoręcznie zaznaczyć osoba fizyczna wyrażająca zgodę;

c) **osoba fizyczna może w każdej chwili wycofać** swoją zgodę i wtedy należy zaprzestać dalszego przetwarzania danych osobowych. Przetwarzanie, które było realizowane przed wycofaniem zgody było zgodne z prawem,

d) jeżeli istnieje inna przesłanka legalności niż zgoda, to nie powinno się jej zbierać aby nie wprowadzać w błąd osoby fizycznej.

2) **jest to niezbędne do zawarcia umowy** – należy pamiętać, że niniejsze przesłanka dotyczy przygotowania umowy, której stroną jest osoba fizyczna, a także dalszego jej realizowania. Przesłanka nie ma zastosowania w przypadku gdy prócz danych strony umowy podaje się również dane np. pracowników.

3) **jest to niezbędne do zrealizowania obowiązku ciążącego na podmiocie** – należy pamiętać, że obowiązek nałożony na podmiot musi wynikać z przepisów prawa. Przez przepisy prawa należy rozumieć: konstytucję, umowy międzynarodowe, ustawy, rozporządzenia, akty prawa miejscowego;

4) **jest to niezbędne do ochrony żywotnych interesów osoby fizycznej lub innej osoby fizycznej**. Żywotny interes innej osoby fizycznej powinien zasadniczo być podstawą przetwarzania danych osobowych wyłącznie w przypadkach, gdy ewidentnie przetwarzania tego nie da się oprzeć na innej podstawie prawnej. Niektóre rodzaje przetwarzania mogą służyć zarówno ważnemu interesowi publicznemu, jak i żywotnym interesom osoby, której dane dotyczą, na przykład gdy przetwarzanie jest niezbędne do celów humanitarnych, w tym monitorowania epidemii i ich rozprzestrzeniania się. Ta przesłanka prawna praktycznie nie występuje w polskich przepisach.

5) **jest to niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej**. Podstawę przetwarzania powinno stanowić prawo Unii lub prawo państwa członkowskiego. Rozporządzenie nie nakłada wymogu, aby dla każdego indywidualnego przetwarzania istniało szczegółowe uregulowanie prawne. Wystarczyć może to, że dane uregulowanie prawne stanowi podstawę różnych operacji przetwarzania wynikających z obowiązku prawnego, któremu podlega administrator, lub że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej. Prawo Unii lub prawo państwa członkowskiego powinno określać także cel przetwarzania. Ponadto prawo to może doprecyzowywać ogólne warunki określone w niniejszym rozporządzeniu dotyczące zgodności przetwarzania z prawem, określać sposoby wskazywania administratora, rodzaj danych osobowych podlegających przetwarzaniu, osoby, których dane dotyczą, podmioty, którym można ujawniać dane osobowe, ograniczenia celu, okres przechowywania oraz inne środki zapewniające zgodność z prawem i rzetelność przetwarzania;

6) **jest to niezbędne do realizacji uzasadnionych interesów administratora** – należy pamiętać, że prawnie uzasadniony interes musi zostać podany osobie, której dane dotyczą. Osoby mogą w każdej chwili wyrazić sprzeciw wobec takiej przesłanki legalności. **Podstawa nie ma zastosowania dla podmiotów publicznych.**

5.1.5. **Dla Administratora najczęstszymi przesłankami legalności przetwarzania danych osobowych są punkty 1,2,3,5**, czyli zgoda udzielona przez osobę której dane dotyczą, niezbędność zawierania umów, przesłanka wynikająca z przepisów prawa lub przesłanka wykonania zadania w interesie publicznym lub też sprawowania władzy publicznej.

5.1.6. **Przetwarzanie danych szczególnej kategorii jest zgodne z prawem gdy:**

1) **osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych** w jednym lub kilku konkretnych celach - należy pamiętać, że:

   a) zgodę należy być wstanie wykazać bez względu na fakt czy została ona pozyskana na piśmie, w rozmowie mailowej, rozmowie telefonicznej rozmowie bezpośredniej,

   b) zgodę wyraża się w konkretnym celu, a w przypadku gdy tych celów jest więcej należy je wyszczególnić, tak aby było wiadomo, na co wyraziła zgodę osoba fizyczna. Dla każdego celu należy zapewnić w formularzach osobną kratkę (checbox'a) do zaznaczenia. Nie dopuszczalne jest aby zgoda była domyślnie zaznaczona, musi ją własnoręcznie zaznaczyć osoba fizyczna wyrażająca zgodę,

   c) osoba fizyczna może w każdej chwili wycofać swoją zgodę i wtedy należy zaprzestać dalszego przetwarzania danych osobowych. Przetwarzanie, które było realizowane przed wycofaniem zgody było zgodne z prawem,

   d) jeżeli istnieje inna przesłanka legalności niż zgoda, to nie powinno się jej zbierać aby nie wprowadzać w błąd osoby fizycznej.

2) **jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie:** prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego;

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

4) **dokonuje się go w ramach uprawnionej działalności** prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach: politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą – należy pamiętać, że ta podstawa prawna nie ma zastosowania w ramach przetwarzania którego dokonuje Administrator;

5) **dotyczy to danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą**;

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

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

8) **jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy**, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego;

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

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

5.1.7. **Przetwarzanie danych dotyczących wyroków skazujących i naruszeń prawa wolno dokonywać wyłącznie pod nadzorem władz publicznych** lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą.

5.1.8. **Spełnienie drugiego wymagania dotyczącego komunikacji z osobami fizycznymi jest możliwe gdy:**

1) **wszelka komunikacja prowadzona jest w sposób zwięzły, przejrzysty, zrozumiały**. Oznacza to, że komunikacja zarówno słowna, elektroniczna jak i tradycyjna musi być prowadzona nieskomplikowanym językiem (zrozumiałym również dla dzieci, a w szczególności dla dzieci, gdy to ich dotyczy komunikat);

2) **komunikacja przyjmuje łatwo dostępną formę**. Oznacza to, że podmiot powinien przewidywać jaka forma komunikacji będzie odpowiednia dla odbiorcy np.: ludzie w wieku emerytalnym w Polsce będą mieli problem z komunikacją elektroniczną ale z tradycyjną pocztą już nie.

3) **Komunikacja jest realizowana niezwłocznie na tyle na ile jest to możliwe,** a w przypadku problemów nie dłużej niż w przeciągu miesiąca od chwili pozyskania danych.

5.1.9. Komunikacja, o której mowa jest powyżej dotyczy:

1) **spełnienia wobec osoby fizycznej obowiązku informacyjnego**, o którym mowa jest w art. 13 i art. 14 RODO. Każda treść klauzul informacyjnych musi:
   a) być zamieszczona na stronie internetowej o ile ma to zastosowanie;
   b) być wytworzona zgodnie z wymaganiami przepisów prawa;
   c) być stosowana podczas pozyskiwania danych;
   d) być zweryfikowana przez IOD.
2) **udzielenia w terminie 30 dni odpowiedzi w związku z chęcią skorzystania przez osobę fizyczną z praw jej przysługujących**, a dotyczących danych osobowych, o których mowa w art. 15 – 23 RODO. Procesy realizacji praw osób, których dane dotyczą przedstawiono w dalszej części dokumentu.

5.1.10. **Niedopuszczalne jest pozyskiwanie danych osobowych bez spełnienia obowiązku informacyjnego** tj. bez przekazania osobie, której dane dotyczą informacji, o których mowa jest w art. 13 i art. 14 RODO.

5.1.11. Administrator w celu zapewnienia prawidłowości treści klauzul informacyjnych wymaga aby ich treść zawsze była zweryfikowana przez IOD.

5.1.12. Zatwierdzone klauzule informacyjne zamieszczane są na stronie internetowej (o ile jest to możliwe), a komórki merytoryczne odpowiedzialne za realizację zadań w ramach, których pozyskiwane są dane osobowe zobowiązane są do posiadania zalaminowanych, zatwierdzonych treści klauzul.

5.1.13. Odpowiedzi związane z realizacją praw osób fizycznych wynikające z ich uprawnień oraz regulacji zawartych w art. 15-22 RODO muszą być konsultowane z IOD przed ich przekazaniem osobie wnioskującej.

5.2. Zasada przetwarzania danych osobowych w konkretnym celu

5.2.1. Zasada ta jasno i precyzyjnie wskazuje, że **pozyskując dane osobowe, można je przetwarzać tylko i wyłącznie w ramach konkretnego celu**, dla którego zostały zebrane.

5.2.2. **Cel przetwarzanych danych musi być jasno i precyzyjnie określony** przed rozpoczęciem pozyskiwania danych.

5.2.3. O celu przetwarzania danych musi być zawsze poinformowana osoba fizyczna, której dane są przetwarzane. **Wskazaną informację przekazuje się w treści klauzuli informacyjnej.**

5.3. Zasada przetwarzania danych osobowych w minimalnym zakresie

5.3.1. **Zasada nakazuje przetwarzać tylko i wyłącznie taki zakres danych** osobowych, **który jest wymagany do osiągnięcia** wcześniej zdefiniowanego **celu** przetwarzania.

5.3.2. Jeżeli przepisy prawa określają konkretny zestaw danych osobowych niezbędny do zrealizowania zadania, to przetwarzanie dodatkowych danych osobowych nie uwzględnionych w przepisach prawa wymaga aby została spełniona dodatkowa przesłanka legalności przetwarzania danych osobowych.

5.3.3. Przetwarzanie danych osobowych poza zakresem określonym przepisami prawa przy jednoczesnym niespełnieniu powyższego punktu oznacza łamanie przepisów prawa.

5.4. Zasada przetwarzania prawidłowych danych

5.4.1. **Zasada nakazuje przetwarzać tylko i wyłącznie prawidłowe dane osobowe**, co oznacza że należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

5.4.2. **Każda osoba**, której dane są przetwarzane **ma prawo do aktualizacji danych jej dotyczących**.

5.5. Zasada przetwarzania danych osobowych przez ograniczony czas

5.5.1. **Zasada nakazuje aby wszelkie dane osobowe były przetwarzane przez określony, konkretny czas.**

5.5.2. W praktyce podmioty realizują zasadę ograniczonego czasu poprzez stosowanie się do Jednolitego Rzeczowego Wykazu Akt lub wyznaczają czas przetwarzania, który zamieszczany jest w klauzuli informacyjnej i rejestrze czynności lub kategorii.

5.5.3. W przypadku gdy w wykazie nie ma określonego czasu przetwarzania danych osobowych, przed przystąpieniem do przetwarzania danych osobowych, administrator ma obowiązek samodzielnie określić okres przetwarzania danych.

5.6. Zasada przetwarzania zapewniajaca bezpieczeństwo

5.6.1. **Zasada nakazuje administratorowi, jego pracownikom oraz podmiotom przetwarzającym zapewnianie odpowiedniego poziomu bezpieczeństwa przetwarzanym informacjom**.

5.6.2. Odpowiedni poziom bezpieczeństwa jest zapewniony gdy atrybuty informacji tj. dostępność, integralność, poufność i rozliczalność są zapewnione w procesie przetwarzania danych osobowych poprzez stosowane zabezpieczenia.

5.6.3. Stosowane zabezpieczania muszą być dobierane na podstawie przeprowadzanej analizy ryzyka w oparciu o jak najlepsze praktyki bezpieczeństwa.

5.6.4. Administrator zapewnia aby dane osobowe były prawidłowo zabezpieczone poprzez opracowanie i wdrożenie różnych zasad bezpieczeństwa przetwarzania danych osobowych.

6. Zarządzanie ryzykiem

6.1. **Zarządzanie ryzykiem jako proces mający na celu**:

1) zidentyfikować możliwe do wystąpienia ryzyka;
2) określić ich istotność dla organizacji;
3) określić sposób postępowania z nimi,

jest nieodłącznym elementem podejmowania decyzji, który stosowany jest przez Administratora w celu strategicznego podejmowania decyzji.

6.2. **Proces zarządzania ryzykiem bezpośrednio odnosi się do obszaru ochrony danych osobowych.**

6.3. **Decyzją najwyższego kierownictwa, proces zarządzania ryzykiem i szansami musi być uwzględniany** w:

1) świadczonych usługach;
2) planowanych projektach;
3) realizowanych projektach;
4) procesach funkcjonujących w organizacji;
5) realizowanych zadaniach własnych i zleconych.

6.4. Ryzykiem należy zarządzać już na etapie planowanie, tak aby w późniejszych fazach nie pojawiały się niepotrzebne wydatki i modyfikacje.

6.5. **Za uwzględnianie ryzyka** w w/w działaniach **odpowiedzialni są Kierownicy Komórek Organizacyjnych oraz osoby wskazane przez Administratora** przy współpracy z IOD.

6.6. **Ryzyka uwzględnia się poprzez**:

1) przypisanie w każdej komórce organizacyjnej realizowanych procesów;
2) przypisanie do każdego procesu wykorzystywanych aktywów i zasobów;
3) określenie zagrożeń dla wykorzystywanych aktywów i zasobów
4) określenie i przypisanie wartości prawdopodobieństwa wystąpienia zagrożenia;
5) określenie i przypisanie wartości skutku materializacji zagrożenia;
6) ostateczne określenie poziomu ryzyka;
7) określenie sposobu dalszego postępowania z ryzykiem.

6.7. **Proces** zarządzania ryzykiem jest dokumentowany i przeprowadzany minimum raz do roku w celu potwierdzenia zagrożeń oddziaływujących na obszar ochrony danych.

7. Zarządzanie zabezpieczeniami

7.1. **W ramach planowanych, implementowanych i wdrażanych działań, we wszelkich projektach, usługach, procesach, zadaniach muszą być bezwzględnie stosowane zabezpieczenia,** których celem jest zapewnienie odpowiedniego poziomu bezpieczeństwa przetwarzanym informacjom (w tym danym osobowym).

7.2. **Odpowiedni poziom bezpieczeństwa zapewnia się gdy atrybuty informacji tj.**

1) **dostępność;**
2) **integralność;**
3) **poufność;**
4) **rozliczalność;**

są na wysokim, akceptowalnym poziomie.

7.3. Zapewnienie odpowiedniego poziomu bezpieczeństwa wynika z:

1) regulacji prawnych;
2) regulacji wewnętrznych;
3) potrzeb interesariuszy.

7.4. **Dobór zabezpieczeń wynika m.in. z:**

1) **analizy i oceny ryzyka;**
2) **dobrych praktyk bezpieczeństwa;**
3) **rekomendacji Inspektora Ochrony Danych.**

7.5. **Od dnia obowiązywania niniejszej polityki stosuje się bezwzględnie 2 kluczowe zasady związane z ustalaniem zabezpieczeń:**

1) **zabezpieczenia muszą być uwzględniane we wszystkich działań już w fazie projektowania, aby podejmowane działania były od początku bezpieczne;**
2) **zabezpieczenia muszą być uwzględniane we wszystkich działaniach w sposób domyślny, a ich zmiana jest możliwa wyłącznie na wyraźne żądanie użytkownika**

7.6. Na podstawie opinii IOD, administrator pozostawia zaplanowane lub aktualnie stosowane zabezpieczenia lub wdraża dodatkowe środki zabezpieczające przetwarzanie informacji w realizowanych działach.

7.7. **IOD prowadzi deklarację stosowanych zabezpieczeń**, którą wykorzystuje zarówno do procesów zarządzania ryzykiem jak również rejestrów czynności i kategorii czynności przetwarzanych danych osobowych.

8. Prawa osób, których dane dotyczą

6.1. W przepisach **RODO przewidziano kilka szczególnych praw** dotyczących przetwarzania danych osobowych, **które to przyznano osobom fizycznym**, do których zalicza się m.in.:

1) **prawo dostępu do danych** – na podstawie, którego osoba fizyczna, ma prawo wglądu do danych jej dotyczących, a także ma prawo otrzymać ich kopię;

2) **prawo do sprostowania danych** - na podstawie, którego osoba fizyczna, ma prawo żądać od administratora aktualizacji danych lub ich poprawy;

3) **prawo do usunięcia danych** - na podstawie, którego osoba fizyczna, ma prawo żądać od administratora usunięcia jej danych – o ile są nadmiarowe i nie wymagane przez przepisy prawa;

4) **prawo do ograniczenia przetwarzania** - na podstawie, którego osoba fizyczna, ma prawo żądać od administratora ograniczenia dalszego przetwarzania danych;

5) **prawo do przenoszenia danych** - na podstawie, którego osoba fizyczna, ma prawo żądać od administratora przekazania posiadanych danych do innego podmiotu o ile są one w formie elektronicznej oraz są przetwarzane na podstawie zgody;

6) **prawo do sprzeciwu** - na podstawie, którego osoba fizyczna, ma prawo sprzeciwić się przetwarzaniu jej danych dotyczących;

7) **prawo do wycofania zgody** - na podstawie, którego osoba fizyczna, ma prawo zmienić zdanie i wycofać udzieloną wcześniej zgodę;

8) **prawo do niepodlegania zautomatyzowanemu podejmowaniu decyzji** - na podstawie, którego osoba fizyczna, ma prawo wnieść sprzeciw i żądać aby decyzje w jej sprawie podejmował człowiek, a nie maszyna lub system.

6.2. **Należy pamiętać, że** osoba fizyczna, której dane dotyczą ma prawo skorzystać z praw jej przysługujących w chwili zwrócenia się z takim wnioskiem do administratora.

6.3. Wniosek, o którym mowa powyżej **może przybrać formę: ustną lub pisemną. Nie można żądać od osoby fizycznej pisemnego wniosku ale na własne potrzeby należy udokumentować chęć skorzystania przez osobę z jej praw dotyczących.**

6.4. **Przed realizacją w/w praw należy**:

1) **dokonać identyfikacji osoby fizycznej**, która chce skorzystać z praw zawartych w przepisach dotyczących ochrony danych osobowych. **Dokonać identyfikacji można poprzez**:

   a) poproszenie o wgląd w dowód osobisty / paszport lub inny ustawowo ważny dokument (najlepiej ze zdjęciem);

   b) poproszenie osoby o udzielenie odpowiedzi na zadane przez nas pytania, na które posiadamy odpowiedzi. (odpowiedzi na pytania powinny być znane raczej tylko osobie, której dane dotyczą. Najlepiej jest zadać ok. 4-5 pytań).

2) **niedopuszczalne jest aby** pracownik przystąpił do realizacji prawa osoby, której dane dotyczą bez uprzedniej identyfikacji osoby fizycznej, jak również niedopuszczalne jest odmówienie osobie fizycznej skorzystanie z jej praw gdy składa ona swój wniosek zdalnie np. telefonicznie lub z wykorzystaniem e-maila.

3) **w przypadku gdy pracownik stwierdzi**, że osoba które jest identyfikowana posiada **nielegalny dokument tożsamości zobowiązany jest do zatrzymania dokumentu oraz powiadomienia policji**.

4) **w przypadku gdy osoba byłaby uwierzytelniania przez telefon lub e-mail, a proces zostałby oceniony jako nieskuteczny lub niemożliwy do realizacji, należy zaprosić taką osobę z dokumentem tożsamości do siedziby** w celu uwierzytelnienia osobistego.

6.5. Po pozytywnym uwierzytelnieniu **należy zweryfikować czy posiada się jakiekolwiek dane osobowe osoby, która chce skorzystać z praw jej przysługujących**. W przypadku gdy:

1) administrator nie posiada danych osobowych osoby fizycznej, należy przekazać takiej osobie informację, że jej dane osobowe nie są przetwarzane przez administratora.

2) administrator posiada dane osobowe osoby fizycznej, należy przystąpić do weryfikacji czy można zrealizować prawa, o które prosi osoba fizyczna. **Realizacja jakiegokolwiek prawa musi zostać potwierdzona z IOD przed jego wykonaniem.**

6.6. **Następnie** po konsultacji z IOD, **należy przejść do wykonania prawa** lub stwierdzenia, że jest to niezgodne z przepisami prawa lub jest to niemożliwe ze względu na brak danych osobowych osoby fizycznej.

6.7. **Treść odpowiedzi** kierowana do osoby fizycznej **musi zostać skonsultowana z Inspektorem Ochrony Danych przed jej wysłaniem** lub przekazaniem wnioskodawcy.

6.8. Należy przygotować i wysłać do wnioskodawcy odpowiedź zawierającą informacje o wykonaniu lub niewykonaniu prawa, o które wnioskowała oraz podaniu ewentualnej przyczyny odmowy wykonania prawa.

6.9. Realizacja prawa osoby fizycznej oraz odpowiedź, o której mowa w powyższym punkcie muszą zostać zrealizowane w **terminie nie dłuższym niż 30 dni od daty wpłynięcia wniosku.**

6.10. **W przypadku gdy pracownik** mający zrealizować prawo osoby, której dane dotyczą **nie będzie wiedział w jaki sposób należy obsłużyć osobę wnioskującą i powołującą się na prawa dotyczące danych osobowych, zobowiązany jest do kontaktu z Inspektorem Ochrony Danych**, w jak najszybszym możliwym terminie w celu uzyskania stosownych informacji wyjaśniających.

9. Rejestrowanie czynności przetwarzania danych osobowych

9.1. **Rejestracji podlega każdy proces oraz czynności w nim realizowane w ramach, których przetwarzane są dane osobowe**, bez względu na to czy pełni się rolę Administratora czy też Podmiotu Przetwarzającego.

9.2. **Rejestracji procesu** oraz czynności w ramach, których przetwarzane będą dane osobowe, **o ile jest to możliwe należy dokonać przed rozpoczęciem przetwarzania danych**, jednakże nie później niż pierwszego dnia funkcjonowania procesu.

9.3. W celu zarejestrowania procesu osoba, która odpowiada za zarządzanie tym procesem zobowiązana jest do kontaktu z IOD w celu wprowadzenia wszelkich niezbędnych informacji do właściwego rejestru.

9.4. **Za aktualność rejestru czynności przetwarzania lub kategorii czynności przetwarzania odpowiedzialność ponosi właściwy kierownik lub wskazany przez Administratora Pracownik.**

9.5. W przypadku braku rejestracji procesu, IOD ma prawo wstrzymać działania związane z przetwarzaniem danych osobowych w komórce organizacyjnej, do czasu uzupełnienia rejestrów przez administratora lub wyznaczonego przez administratora pracownika.

9.6. Rejestry muszą zawierać minimum informacje wymagane przez art. 30 RODO, a forma ich prowadzenia musi umożliwiać wydrukowanie danych lub ich skopiowanie do pliku worda lub excela.

9.7. **IOD dokonuje przeglądu zawartości rejestrów nie rzadziej niż raz na pół roku.**

10. Powierzenie przetwarzania danych osobowych

8.1. Administrator w celu zapewnienia jednolitego i efektywnego podejścia do procesu powierzenia danych osobowych ustanowił proces realizacji powierzenia przetwarzania danych osobowych, który wymaga współpracy administratora lub wyznaczonego przez niego pracownika z Inspektorem Ochrony Danych.

8.2. **Proces zawarcia umowy powierzenia odbywa się poprzez uzupełnienie szablonu umowy powierzenia** przez administratora lub wyznaczonego przez niego pracownika. Wzór umowy powierzenia stanowi załącznik do niniejszej polityki. (W wyjątkowych sytuacjach dopuszcza się zawieranie umowy powierzenia na innych szablonach niż administratora)

8.3. **Uzupełniony dokument musi być zweryfikowany i zaopiniowany przez Inspektora Ochrony Danych.** W przypadku gdy dokument spełnia wszystkie ustalone wymagania, jest on parafowany przez Inspektora Ochrony Danych. W innym wypadku do dokumentu wprowadzane są uwagi lub bezpośrednie modyfikacje .

8.4. **Administrator ma prawo akceptacji umowy bez opinii Inspektora Ochrony Danych** oraz ma możliwość odstąpienia od uwag bądź zmian wprowadzonych przez Inspektora Ochrony Danych.

8.5. **Po zaopiniowaniu dokumentu oraz po jego podpisaniu** przez 2 strony umowy, **jest on** skanowany i rejestrowany w rejestrze umów powierzenia.

8.6. Za zarejestrowanie umowy powierzenia odpowiada Kierownik Komórki Organizacyjnej lub pracownik, któremu powierzono te zadanie.

11. Udostępnienie danych osobowych

11.1. **Przed udostępnieniem danych, weryfikowana jest tożsamość wnioskodawcy** jak również powiadamiany jest Inspektor Ochrony Danych, z którym pracownik chcący udostępnić dane zobowiązany jest się skontaktować.

11.2. **Dokonać identyfikacji można poprzez**:

1) poproszenie o wgląd w dowód osobisty / paszport lub inny ustawowo ważny dokument (najlepiej ze zdjęciem);

2) poproszenie osoby o udzielenie odpowiedzi na zadane przez nas pytania, na które posiadamy odpowiedzi. (odpowiedzi na pytania powinny być znane raczej tylko osobie, której dane dotyczą. Najlepiej jest zadać ok. 4-5 pytań).

11.3. Zaleca się aby wnioskodawca o ile jest to możliwe udokumentował chęć udostępnienia danych, a jeżeli jest to niemożliwe powinien dokonać tego pracownik.

11.4. **Osoba lub podmiot,** który wnioskuje o udostępnienie danych **musi wskazać**:

1) **że posiada podstawę** prawną **do udostępnienia** danych **oraz cel** zgodny z przepisami prawa, na które się powołała;

2) **zakres danych**, który miałby zostać udostępniony oraz **formę ich udostępnienia**.

11.5. Po otrzymaniu w/w danych **pracownik zobowiązany jest do skontaktowania się z IOD**, który następnie dokonuje analizy wniosku oraz weryfikacji zgodności udostępnienia danych z przepisami prawa.

11.6. Po przeprowadzonej analizie, IOD informuje Pracownika oraz Administratora o zajętym stanowisku i o czynnościach, które jego zdaniem są do zrealizowania.

11.7. Administrator może zaakceptować stanowisko IOD lub się z nim nie zgodzić. Administrator odpowiada za podjęcie ostatecznej decyzji czy należy udostępnić dane.

11.8. **Wszelkie udostępnienia danych osobowych lub ich odmowy są rejestrowane we właściwym rejestrze**.

11.9. **Za zarejestrowanie udostępnienia danych lub jego odmowy odpowiada Kierownik Komórki Organizacyjnej** lub pracownik, któremu powierzono te zadanie

12. Podstawowe zasady bezpieczeństwa dot. danych osobowych

12.1. Zasady bezpieczeństwa osobowego:

1) Każda osoba, która przetwarza dane osobowe musi posiadać upoważnienie do przetwarzania danych osobowych lub umowę powierzenia przetwarzania.
2) Każda osoba, która przetwarza dane osobowe, zobowiązana jest do złożenia oświadczenia o zachowaniu poufności lub podpisania umowy powierzenia.
3) Każda osoba, która przetwarza dane osobowe ma prawo przetwarzać wyłącznie te informacje, które są mu niezbędne do wykonania zdań.
4) Każdy pracownik, który przetwarza dane osobowe musi zostać przeszkolony przez Inspektora Ochrony Danych.
5) Każda osoba, która przetwarza dane osobowe zobowiązany jest do przestrzegania przepisów prawa oraz polityk, reguł i zasad ustanowionych w podmiocie.

12.2. Zasady bezpieczeństwa dotyczące aktywów:

1) Wszystkie aktywa w organizacji muszą być inwentaryzowane zgodnie z przepisami prawa oraz formalnymi procedurami w organizacji.
2) Wszystkie aktywa w organizacji muszą być przypisane na stanie do konkretnej komórki organizacyjnej / stanowiska lub pracownika.
3) Przekazanie pracownikowi aktywa na stan musi być zawsze formalnie udokumentowane, a zapis z przekazania musi być przechowywany.
4) Na wykorzystanie aktywa do celów prywatnych należy posiadać pisemną zgodę kierownictwa. Dotyczy to również wykorzystywania prywatnego aktywa.

12.3. Zasady bezpieczeństwa dotyczące wykorzystywania komputera:

1) Komputer stacjonarny lub laptop jest przekazywany wyłącznie na potrzeby realizacji zadań służbowych.
2) Zabrania się wykorzystywania sprzętu służbowego do celów prywatnych z wyłączeniem przerwy.
3) Zabrania się użytkownikom wykonywania wszelkich czynności eksploatacyjno-konserwacyjnych bez zgody informatyka i najwyższego kierownictwa.
4) Zabrania się wynoszenia stacji roboczej lub laptopa poza siedzibę organizacji bez posiadania pisemnej zgody najwyższego kierownictwa.
5) Zabrania się pozostawienia uruchomionej stacji roboczej lub laptopa bez fizycznego nadzoru użytkownika.
6) W przypadku zaprzestania chwilowego korzystania ze stacji roboczej lub laptopa, użytkownik jest zobowiązany do wylogowania się.
7) W przypadku wyniesienie poza organizację stacji roboczej lub laptopa, sprzęt należy zaszyfrować, a wyjątki muszą być potwierdzone przez kierownictwo. (Dotyczy to sytuacji gdy na sprzęcie znajdują się dane osobowe)
8) Zabrania się użytkownikom instalacji jakiegokolwiek oprogramowania na stacjach roboczych lub laptopach bez pisemnej zgody najwyższego kierownictwa.

9) Zabrania się użytkownikom wyłączania oprogramowania zabezpieczającego stację roboczą lub laptopa przed złośliwym oprogramowaniem.

10) Użytkownik jest zobowiązany zwrócić przypisany do niego sprzęt ostatniego dnia pracy. Zwrot musi zostać udokumentowany.

12.4. Zasady bezpieczeństwa dotyczące wykorzystywania telefonu służbowego:

1) Telefony zarówno stacjonarne jak również komórkowe mogą być wykorzystywane przez użytkowników wyłącznie na potrzeby realizacji zadań służbowych.

2) Zabrania się użytkownikom wykonywania wszelkich czynności eksploatacyjno-konserwacyjnych bez zgody informatyka i najwyższego kierownictwa.

3) Zabrania się użytkownikom instalacji jakiegokolwiek oprogramowania na telefonach stacjonarnych i komórkowych bez posiadania zgody kierownictwa.

4) Użytkownicy telefonów komórkowych mają obowiązek ustawić blokadę wyświetlacza na telefonie składającą się z minimum 4 różnych cyfr.

5) Urządzenia komórkowe, które są wykorzystywane do odbierania lub wysłania maili muszą być obowiązkowo szyfrowane.

6) Użytkownik jest zobowiązany zwrócić przypisany do niego sprzęt ostatniego dnia pracy. Zwrot musi zostać udokumentowany.

12.5. Zasady bezpieczeństwa dotyczące wykorzystywania przenośnych pamięci:

1) W organizacji dopuszcza się wykorzystywanie przenośnych pamięci. Zaszyfrowane muszą być te nośniki które zawierają dane osobowe.

2) Należy pamiętać, że pamięć przenośna służy wyłącznie do przenoszenia danych, a nie do ich przechowywania.

3) Zabrania się zapisywania przez użytkownika hasła do pamięci przenośnej w taki sposób aby było one dostępne dla innych użytkowników.

4) W przypadku przekazania przez użytkownika nośnika z danymi osobowymi innemu podmiotowi musi zostać zawarta umowa powierzenia.

5) Naprawy wszelkich urządzeń, które posiadają w sobie pamięć należy dokonać bez udostępniania dysku podmiotom zewnętrznym.

6) Użytkownik jest zobowiązany zwrócić przypisany do niego sprzęt ostatniego dnia pracy. Zwrot musi zostać udokumentowany.

12.6. Zasady bezpieczeństwa dotyczące wykorzystywania poczty e-mail:

1) Poczta służbowa użytkowników musi być wykorzystywana wyłącznie do celów służbowych organizacji.

2) Istotne wiadomości w szczególności te, które zawierają dane szczególnej kategorii muszą być szyfrowane za pomocą 7-zip'a.

3) Hasło do wiadomości elektronicznej nie może być wysłane przez użytkownika tym samym kanałem do odbiorcy co zaszyfrowany dokument.

4) Należy zawsze zweryfikować nadawcę / odbiorcę oraz zwrócić uwagę czy wszyscy użytkownicy, którzy mieli być dodani są dołączeni za pomocą opcji „*Ukryj DW*".

5) Nie wolno otwierać otrzymanych załączników, których rozszerzenie może spowodować uruchomienie / zainstalowanie złośliwego oprogramowania.

6) Wszelkie podejrzane pliki, które użytkownik otrzymał muszą zostać przesłane do pracownika odpowiedzialnego za informatyzację, w celu ich weryfikacji.

7) Użytkownikowi zabrania się zapisywania hasła zarówno w przeglądarkach, jak również na kartkach przy stacji roboczej lub laptopie.

12.7. Zasady dotyczące bezpiecznego wykorzystywania podpisów / certyfikatów:

1) Podpisy elektroniczne oraz certyfikaty elektroniczne, które zostały nabyte przez jednostkę dla użytkownika stanowią własność jednostki.

2) Użytkownik ma prawo i obowiązek stosować zakupione mu podpisy elektroniczne oraz certyfikaty do zadań służbowych.

3) Do autoryzacji podpisu elektronicznego lub certyfikatu muszą być stosowane dane uwierzytelniające.

4) W/w dane uwierzytelniające mogą być znane wyłącznie użytkownikowi, do którego zostały one przypisane.

5) Zabrania się pozostawiania niezabezpieczonych podpisów elektronicznych lub certyfikatów w miejscu ogólnodostępnym lub miejscu pracy.

12.8. Zasady dot. kontroli dostępu do aplikacji, programów i systemów informatycznych:

1) Każdy użytkownik, który posiada dostęp do aplikacji, programu, systemu informatycznego musi być zarejestrowany.

2) Każdemu pracownikowi lub innemu użytkownikowi przypisuje się minimalne uprawnienia dostępowe.

3) Każdemu pracownikowi lub użytkownikowi przypisuje się indywidualne dane do uwierzytelnienia.

4) Hasła do aplikacji, programów, systemów informatycznych lub sprzętu komputerowego muszą się składać z:
   a) minimum 10 znaków;
   b) małych i dużych liter;
   c) cyfr
   d) znaków specjalnych;
   e) ciągu przypadkowych znaków.

5) Nie wolno zapisywać danych do uwierzytelnienia w aplikacjach, programach, systemach informatycznych oraz przeglądarkach internetowych.

6) Wszelkie hasła, które są danymi do uwierzytelnienia należy zmieniać maksymalnie co 90 dni z uwzględnieniem faktu, że nie mogą się one powtarzać.

7) Dane do uwierzytelnienia, które posiada użytkownik, stanowią jego własność i nikt nie może ich znać. Zabrania się przekazywania danych uwierzytelniających.

8) Nie rzadziej niż raz na pół roku należy dokonać przeglądu zarejestrowanych użytkowników jak również przeglądu praw dostępowych.

12.9. Zasady bezpieczeństwa dotyczące obszarów fizycznych:

1) W pomieszczeniach biurowych mogą przebywać osoby nie będące pracownikami tylko i wyłącznie przy obecności personelu lub za zgodą kierownictwa.
2) W przypadku opuszczenia biura lub pomieszczenia pracy, gdy nie ma tam już żadnej osoby, należy zamknąć na klucz biuro, pomieszczenie, budynek.
3) Wszelkie pomieszczenia, w których przetwarzane są dane osobowe na koniec dnia pracy muszą zostać zamknięte na klucz lub za pomocą kodu.
4) W pomieszczeniach, w których przetwarzane są dane osobowe na koniec dnia pracy muszą zostać zamknięte okna, szafy, szafki, drzwi.
5) Budynki i pomieszczenia, w których jest alarm na koniec dnia pracy muszą zostać zakodowane przez uprawnionych pracowników.
6) Każdy pracownik jest uprawniony do pobierania kluczy wyłącznie do pomieszczeń, w których wykonuje swoją pracę.
7) Zabrania się pracownikom pozostawiania w drzwiach do biur i pomieszczeń od strony zewnętrznej kluczy.
8) Zabrania się pracownikom dorabiania kluczy do pokoi bez pisemnej zgody najwyższego kierownictwa.
9) Zabrania się pracownikom wynoszenia kluczy poza miejsce pracy bez zgody najwyższego kierownictwa.

12.10. Zasady dotyczące udostępniania danych:

1) Każdy pracownik zobowiązany jest przed udostępnieniem danych osobowych do identyfikacji osoby lub podmiotu, który zwraca się z taką intencją.
2) Każdy pracownik, który zamierza udostępnić dane osobowe zobowiązany jest do powiadomienia Inspektora Ochrony Danych przed udostepnieniem danych.
3) Każdy pracownik, który udostępni dane osobowe zobowiązany jest do odnotowania takiej czynności w odpowiednim rejestrze.

12.11. Zasady bezpieczeństwa ze stronami trzecimi:

1) Z każdym podmiotem, któremu powierza się przetwarzanie danych osobowych musi zostać zawarta umowa powierzenia danych.
2) W umowach ze stronami trzecimi należy zawrzeć parametry SLA, które będą chronić organizację zapewniając, że usługi będą na odpowiednim poziomie.
3) Strony trzecie muszą mieć pisemną zgodę najwyższego kierownictwa do pracy na terenie siedziby pracodawcy bez nadzoru pracownika organizacji.
4) Strony trzecie świadczące pracę lub inne usługi dla organizacji muszą mieć pisemną zgodę najwyższego kierownictwa na wynoszenie z organizacji aktywów.

Załączniki

Zał. nr 1 – Wykaz skrótów i pojęć

Wykaz skrótów i pojęć

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.
Aktywo	wszystko, co ma wartość dla Podmiotu
Audyt	systematyczny, niezależny i udokumentowany proces uzyskiwania dowodów oraz ich oceny w celu określenia stopnia spełnienia kryteriów audytu
Audytor	specjalista, który zajmuje się przeprowadzaniem audytów, czyli rewizji różnych obszarów działalności danej instytucji, w oparciu o przepisy prawa wewnętrzne regulacje i najlepsze praktyki
Bezpieczeństwo	zapewnienie poufności, integralności i dostępności informacji oraz odporności procesów funkcjonujących w Podmiocie na zakłócenia
Dane dotyczące zdrowia	dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej wraz z informacjami o wszelkich świadczonych jej usługach medycznych
Dane osobowe	oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej
Dostępność	właściwość zapewniająca, że informacja jest dostępna na żądanie uprawnionej osoby w ustalonym czasie
Incydent	pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń, które stwarzają prawdopodobieństwo zakłócenia działalności Podmiotu i zagrażają bezpieczeństwu informacji lub ochrony danych osobowych
Inspektor Ochrony Danych (IOD)	osoba fizyczna wyznaczona przez Administratora do wykonywania zadań, o których mowa jest w art. 39 RODO
Integralność	właściwość polegająca na tym, że informacja nie uległa zmianie od ostatniej autoryzowanej modyfikacji lub nie została usunięta w niekontrolowany sposób.
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
Niezgodność	niespełnienie wymagania wynikającego z przepisu prawa, wewnętrznych regulacji lub normatywnych praktyk

Organ Nadzorczy	Prezes Urzędu Ochrony Danych Osobowych, realizujący zadania przy pomocy Urzędu Ochrony Danych Osobowych
Personel	wszystkie osoby świadczące swoją pracę na rzecz Podmiotu np. pracownicy, współpracownicy, stażyści, rezydenci
Podmiot przetwarzający	oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora
Poufność	właściwość zapewniająca, że informacje są dostępne wyłącznie dla osób uprawnionych do ich przetwarzania.
Pracownik	osoba zatrudniona u administratora na podstawie umowy o pracę np. umowy o pracę na okres próbny, umowy o pracę na czas określony, umowy o pracę na czas nieokreślony, inne.
Przetwarzanie danych osobowych	oznacza 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
RODO	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
Ryzyko	prawdopodobieństwo, że określone zagrożenie wykorzysta podatność aktywa lub grupy aktywów aby spowodować straty lub inne niechciane negatywne skutki
Zabezpieczenie	praktyka, procedura lub mechanizm redukujący ryzyko
Zagrożenie	potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu lub instytucji
Zarządzanie incydentem	obsługa incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu
Zgodność	cecha wskazująca, że proces/ produkt /usługa / itp. spełnia wymagania np.: prawne, wewnętrzne, normatywne