FUNDACJA GOSPODARCZA PRO EUROPA
87-100 Toruń, ul. Warszawska 4/7, tel. 56 658 59 08, tel./fax 56 658 59 09,
80-809 Gdańsk, ul. Milskiego 1/6, tel./fax 58 550 09 97, 601 37 49 37
mail: proeuropa@fundacja-proeuropa.org.pl, www.fundacja-proeuropa.org.pl

Polityka bezpieczeństwa danych osobowych

I Postanowienia ogólne.

1. Polityka bezpieczeństwa przetwarzania danych osobowych w **Fundacji Gospodarczej Pro Europa, 87-100 Toruń, ul. Warszawska 4/7** zwaną dalej „Polityką" została ustanowiona z związku z art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE - zwanym dalej RODO.
2. Celem Polityki jest zapewnienie ochrony danych osobowych przetwarzanych przez Fundację Gospodarczą Pro Europa, 87-100 Toruń, ul. Warszawska 4/7 zwaną dalej, „Fundacją",
3. Zastosowane zabezpieczenia mają zapewnić:
   a. poufność danych – rozumianą, jako właściwość polegająca na tym, że dane osobowe nie są udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
   b. integralności danych – rozumianą, jako właściwość polegającą na tym, że dane osobowe nie zostały zmodyfikowane lub zniszczone w sposób nieuprawniony;
   c. dostępność danych – rozumianą, jako właściwość polegającą na tym, że informacja jest możliwa do wykorzystania przez uprawniony podmiot na jego żądanie, w założonym czasie;
   d. autentyczność danych – rozumianą, jako właściwość polegającą na tym, że pochodzenie lub zawartość danych opisujących obiekt są takie, jak deklarowane;
   e. rozliczalność danych - rozumianą, jako właściwość pozwalająca przypisać określone działanie osoby w sposób jednoznaczny tej osobie oraz umiejscowić je w czasie;
   f. niezaprzeczalność – rozumianą, jako brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie;
4. Fundacja zobowiązuje się do podjęcia odpowiednich kroków, mających na celu zapewnienie prawidłowej ochrony danych osobowych.
5. Zasady określone w niniejszej Polityce oraz w dokumentach powiązanych powinny być znane i stosowane przez wszystkie osoby, które biorą udział w procesie przetwarzania danych osobowych w Fundacji, bez względu na zajmowane stanowisko, jak również charakter stosunku pracy.
6. Osoby mające dostęp do danych osobowych są zobligowane do stosowania niezbędnych środków zapobiegających ujawnieniu tych informacji osobom nieupoważnionym.
7. Zachowanie tajemnicy obowiązuje zarówno podczas trwania stosunku pracy jak i po jego ustaniu.
8. Żadne odstępstwa od zasad bezpieczeństwa przedstawionych w przedmiotowym dokumencie nie są dopuszczalne bez uzyskania zgody Administratora Danych Osobowych.

II Definicje.

1. Użyte w niniejszej Polityce pojęcia są wspólne dla wszystkich dokumentów powiązanych z niniejszą Polityką oraz dla wszystkich pozostałych dokumentów, które zostały przyjęte , w zakresie ochrony danych osobowych.
2. **Administrator Danych Osobowych (ADO)** - należy przez to rozumieć Fundację, która ustala cele i sposoby przetwarzania danych osobowych i jest reprezentowana przez Zarząd.
3. **Administrator Systemu Informatycznego (ASI)** - należy przez to rozumieć osobę wyznaczoną przez ADO, będącą odpowiedzialną za poprawne funkcjonowanie, zabezpieczenie oraz nadzór nad infrastrukturą i systemami informatycznymi służącymi do przetwarzania danych osobowych w Fundacji. Dopuszcza się, aby funkcje ASI realizował podmiot zewnętrzny;
4. **Aktywa -** zasoby niezbędne do realizacji czynności związanych z operacjami przetwarzania danych osobowych tj. procesy, informacje, personel, sprzęt, oprogramowanie, sieć, siedziba;
5. **Analiza ryzyka** – systematyczne podejście mające na celu zidentyfikowanie w systemie źródeł ryzyka i przypisanie zidentyfikowanym ryzykom wartości;
6. **Dane osobowe** - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą");
7. **Grupa aktywów** - zbiór aktywów rozpatrywanych wspólnie ze względu na podobny charakter i funkcjonalność;
8. **Incydent** – zamierzone lub przypadkowe naruszenie środków technicznych i organizacyjnych zastosowanych w celu ochrony danych osobowych. Następuje w szczególności, gdy stan urządzenia, zawartości informacji, ujawnione metody pracy, sposób działania programu lub jakości

komunikacji w sieci teleinformatycznej mogą wskazywać na naruszenie bezpieczeństwa danych osobowych;

9. **Inspektor Ochrony Danych (IOD)** – należy przez to rozumieć wyznaczoną osobę przez ADO, odpowiedzialną za nadzorowanie stosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszenia bezpieczeństwa danych osobowych.
10. **Ocena ryzyka** – proces porównywania wartości ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka;
11. **Osoba upoważniona** – osoba przeszkolona z zakresu bezpieczeństwa danych osobowych oraz posiadająca imienne upoważnienie wydane przez ADO;
12. **Podatność** – słabość aktywów, która może być wykorzystana przez zagrożenie. Podatność charakteryzuje łatwość, z jaką dane zagrożenie może wyrządzić szkodę;
13. **Podmiot przetwarzający** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
14. **Polityka** – Polityka bezpieczeństwa danych osobowych – zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania zatwierdzony przez ADO, będący zbiorem reguł dotyczących ochrony danych osobowych Spektrum;
15. **Postępowanie z ryzykiem** – proces wyboru i wdrażania środków sterowania ryzykiem mających na celu zmianę wartości poziomu ryzyka;
16. **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;
17. **Ryzyko –** prawdopodobieństwo, że określone zagrożenie wykorzysta podatność aktywu lub grupy aktywów, aby spowodować straty lub szkody, co spowoduje niepożądane konsekwencje;
18. **Ryzyko szczątkowe–** ryzyko, którego poziom nie przekracza akceptowanej wartości;
19. **Skutek (ze strony zagrożenia**) - rezultat niepożądanego incydentu. Stopień strat powstałych w przypadku zaistnienia zagrożenia.
20. **Fundacja** – Fundacja Gospodarcza Pro Europa - ADO
21. **UODO -** Ustawa z dnia 10.05.2018 r. o ochronie danych osobowych;
22. **Właściciel aktywa** osoba lub podmiot, który ma zatwierdzoną kierowniczą odpowiedzialność w organizacji za nadzorowanie produkcji, rozwój, utrzymanie, korzystanie i bezpieczeństwo aktywów. Pojęcie to nie oznacza, że osoba ta rzeczywiście posiada jakiekolwiek prawa własności do aktywów;
23. **Zagrożenie** – potencjalna przyczyna niepożądanego incydentu, która może wywołać naruszenie praw i wolności osób fizycznych lub bezpieczeństwa danych osobowych;
24. **Zarządzanie ryzykiem** – jest to ciągły nadzór nad stanem bezpieczeństwa systemu. Zarządzanie ryzykiem jest to proces identyfikacji, kontrolowania, eliminacji lub ograniczania prawdopodobieństwa zaistnienia ewentualnych zdarzeń (zagrożeń), które mogą mieć wpływ na bezpieczeństwo danych osobowych;
25. **Zbiór danych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

III Dokumenty powiązane.

1. Na dokumentację ochrony danych osobowych w Fundacji składają się:
    a. Polityka bezpieczeństwa danych osobowych (Polityka) – dokument określający prawa i obowiązki osób funkcyjnych biorących udział w procesie przetwarzania danych osobowych, odpowiedzialność oraz procedury postępowania w procesie przetwarzania w/w informacji.
    b. Metodyka zarządzaniem ryzykiem w ochronie danych osobowych (Metodyka) - wypełniających wymogi art. 32 RODO.
    c. Sprawozdanie z analizy ryzyka - wypełniających wymogi art. 32 RODO.
    d. Rejestr czynności przetwarzania danych osobowych; - wypełniających wymogi art. 30 RODO.
    e. Ewidencja osób upoważnionych do przetwarzania danych osobowych, - wypełniający wymogi art. 29 RODO.
    f. Rejestr incydentów bezpieczeństwa i działań korygujących – wypełniający wymogi art. 33 ust 5 RODO.
    g. Oryginały i kopie dokumentów dotyczących ochrony danych osobowych.
    h. Protokoły z przeprowadzonych kontroli wewnętrznych i zewnętrznych w zakresie ochrony danych osobowych.

i. Jeżeli dotyczy – Ocena skutków dla przetwarzania danych osobowych – wypełniający wymogi art. 35 RODO.
j. Protokoły z niszczenia dokumentów, nośników oraz sprzętu zawierające dane osobowe.

2. Wymienione dokumenty stanowią komplet dokumentacji z zakresu bezpieczeństwa danych osobowych w Fundacji.

IV Obowiązki oraz odpowiedzialność osób funkcyjnych.

1. Administrator danych osobowych wdraża odpowiednie środki techniczne i organizacyjne mające na celu zapewnić przetwarzanie danych zgodnie z RODO, uwzględniając charakter, zakres, kontekst i cel przetwarzania oraz ryzyko naruszenia praw lub wolności osoby fizycznej a także utraty atrybutów danych.
2. Do kompetencji **administratora danych osobowych** należy w szczególności:
   a. Wyznaczenie administratora systemu informatycznego.
   b. Określenie celów i strategii ochrony danych osobowych.
   c. Podział zadań i obowiązków związanych z organizacją ochrony danych osobowych.
3. Do obowiązków **Administratora Danych Osobowych** należy:
   a. uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdrażanie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO. Administrator musi być w stanie wykazać adekwatność zastosowanych środków bezpieczeństwa. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane;
   b. zapewnienie szkoleń dla pracowników w zakresie przepisów o ochronie danych osobowych oraz zagrożeń związanych z ich przetwarzaniem;
   c. przyjmowanie i zatwierdzanie niezbędnych, wymaganych przez przepisy prawa dokumentów regulujących ochronę danych osobowych w Fundacji;
   d. nadawanie, zmienianie oraz cofanie uprawnień do przetwarzania danych osobowych;
   e. zapewnienie środków finansowych na ochronę fizyczną pomieszczeń, systemów informatycznych oraz zbiorów tradycyjnych, w których przetwarzane są dane osobowe;
   f. zapewnienie środków finansowych na merytoryczne przygotowanie osób odpowiedzialnych za nadzór nad ochroną danych osobowych;
   g. uwzględnianie bezpieczeństwa danych osobowych na etapie projektowania sposobów przetwarzania, zakresu, podstawy prawnej oraz ochrony technicznej i organizacyjnej tych danych;
   h. zapewnia wykonanie analizy ryzyka
   i. monitorowanie przestrzegania przepisów prawa
   j. nadzorowanie i aktualizowanie dokumentacji w zakresie ochrony danych osobowych;
   k. zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami w tym zakresie;
   l. prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych
   m. prowadzenie i stała aktualizacja Rejestru czynności przetwarzania danych osobowych
4. Administrator danych osobowych wskazuje administratora systemów informatycznych – obowiązki te mogą być realizowane poprzez firmę zewnętrzną bez wskazywania konkretnej osoby.
5. Administrator systemu informatycznego realizuje zadania w zakresie bezpieczeństwa ochrony danych, a w szczególności poprzez:
   a. zapewnienie ochrony i bezpieczeństwa danych osobowych zawartych w systemach informatycznych Fundacji;
   b. przeciwdziałanie próbom naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych;
   c. zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych z RODO oraz z niniejszą Polityką:
   d. administrowanie oprogramowaniem systemowym i sieciowym zabezpieczającym osobowe przed nieupoważnionym dostępem;
   e. nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisyjnych;
   f. nadzór i kontrolę systemów informatycznych służących do przetwarzania danych osobowych a także osoby przy nich zatrudnionych w zakresie bezpieczeństwa teleinformatycznego;
   g. zakładanie kont użytkowników ze ściśle określonym zakresem praw dostępu oraz blokowanie dostępu do kont w przypadku cofnięcia użytkownikowi upoważnienia dostępu do przetwarzania danych osobowych;
   h. konfigurowanie komputerów użytkowników i instalację oprogramowania;

i. wnioskowanie do ADO o zastosowanie rozwiązań technicznych i organizacyjnych, które mają minimalizować zagrożenia utraty bezpieczeństwa informacji;

5. Pracownicy/ osoby upoważnione są zobowiązane do:
   a. znajomości zasad bezpieczeństwa zawartych w dokumentach: Polityka bezpieczeństwa oraz dokumentach powiązanych a także zasadach zawartych w przepisach prawa RODO i Ustawy w zakresie niezbędnym do zajmowanego stanowiska i zakresu upoważnienia;
   b. bezwzględnego przestrzegania zapisów Polityki oraz pozostałych dokumentów regulujących zasady przetwarzania danych osobowych;
   c. zachowania w tajemnicy wiedzy o przetwarzanych danych osobowych oraz o sposobach ich zabezpieczenia;
   d. ochrony danych osobowych oraz aktywów wykorzystywanych do ich przetwarzania przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
   e. zmiany hasła do systemów służących do przetwarzania danych osobowych nie rzadziej niż raz na trzy miesiące.

V Zarządzanie ochroną danych osobowych.

1. Przetwarzanie danych osobowych dopuszczalne jest jedynie w ramach zbiorów i czynności przetwarzania danych osobowych, które są zawarte w „Rejestrze czynności przetwarzania danych osobowych".
2. Likwidację zbioru przeprowadza komisja powołana przez Administratora Danych Osobowych. W protokole potwierdzającym likwidację zbioru wskazuje się: skład osobowy komisji, datę likwidacji i sposób usunięcia zgromadzonych danych, zakres likwidowanych danych.
3. Likwidację dokumentów zawierających dane osobowe a powstałe w trybie normalnym pracy (w tym między innymi: błędnych i próbnych wydruków), niszczy użytkownik w sposób trwały uniemożliwiający odczytanie zniszczonych danych.
4. Zestawienie środków organizacyjnych i technicznych zapewniających ochronę danych osobowych u ADO:
   a. została opracowana i wdrożona „Polityka bezpieczeństwa danych osobowych";
   b. została opracowana i wdrożona „Metodyka zarządza ryzykiem danych osobowych";
   c. został opracowany i wdrożony „Rejestr czynności przetwarzania danych osobowych";
   d. zastosowane techniczne i organizacyjne środki bezpieczeństwa informacji oparte zostały na analizie ryzyka, posiadanej wiedzy oraz posiadanych środkach finansowych;
   e. do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych;
   f. prowadzona jest ewidencja osób upoważnionych do przetwarzania danych;
   g. osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
   h. osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy oraz metod zastosowanych do ich zabezpieczeń;
   i. wszystkie pomieszczenia, w których przetwarza się dane osobowe, są zamykane na klucz w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych osobowych – także w godzinach pracy;
   j. została opracowana i wdrożona „Polityka kluczy";
   k. nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarkach;
   l. dostęp do systemu operacyjnego komputerów na których przetwarzane są dane osobowe został zabezpieczony hasłem;
   m. dostęp do zbioru danych osobowych w systemie teleinformatycznym wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika i hasła;
   n. zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe;
   o. wyznaczono pomieszczenie do obsługi klientów w którym nie znajdują się komputery i dokumenty z danymi osobowymi
   p. cyklicznie wykonywane są kopie bezpieczeństwa, z których w przypadku awarii odtwarzane są dane;
   q. do zabezpieczenia stanowisk komputerowych przed oprogramowaniem złośliwym i wirusami stosowane jest oprogramowanie antywirusowe.

VI Szkolenia użytkowników.

1. Każdy użytkownik przed przystąpieniem do przetwarzania danych osobowych musi zostać przeszkolony z zakresu:
   a. przepisów o ochronie danych osobowych, a także Polityki wprowadzonej przez ADO;

b. zasad przetwarzania danych osobowych;
c. procedur dotyczących bezpiecznego przetwarzania danych osobowych w systemach informatycznych;
d. zasady użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych;
e. zagrożeń na jakie może być narażone przetwarzanie danych osobowych, a w szczególności zagrożeń informacji przetwarzanych w systemach informatycznych;
f. zasad dostępu do pomieszczeń, w których przetwarzane są dane osobowe;
g. sposobu postępowania w przypadku naruszenia ochrony danych osobowych.

2. Potwierdzenie odbytego szkolenia oraz zapoznanie się z dokumentami dotyczącymi przetwarzania danych osobowych pracownik potwierdza własnoręcznym podpisem na liście obecności ze szkolenia.

VII Upoważnienie do przetwarzania danych osobowych.

1. Do przetwarzania danych osobowych mogą być dopuszczone jedynie osoby posiadające upoważnienie wydane przez ADO.
2. Upoważnienie wydawane jest pracownikom zgodnie z zasadą „wiedzy uzasadnionej". Wnioskujący o wydanie upoważnienia w oparciu o analizę zakresu obowiązków, określa zakres i okres ważności upoważnienia.
3. W przypadku długotrwałej nieobecności pracownika (co najmniej przez trzy miesiące) upoważnienie powinno być czasowo cofnięte.

VIII Ewidencja osób upoważnionych.

1. Osoby upoważnione do przetwarzania danych osobowych, ewidencjonowane są w „Ewidencji osób upoważnionych do przetwarzania danych osobowych" prowadzonej w Fundacji
2. Ewidencjonowanie następuję bez zbędnej zwłoki po nadaniu lub cofnięciu upoważnienia.

IX Powierzanie przetwarzania danych osobowych.

1. ADO może powierzyć dane do dalszego przetwarzania tylko takiemu podmiotowi przetwarzającemu, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
2. Powierzenie przetwarzania danych osobowych może mieć miejsce tylko na podstawie pisemnej umowy określającej w szczególności przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora oraz podmiotu przetwarzającego a także zakres odpowiedzialności podmiotu przetwarzającego z tytułu niewykonania lub nienależytego wykonania umowy.
3. Podmiot przetwarzający przy przetwarzaniu danych osobowych zobowiązany jest stosować wszelkie środki wymagane art. 32 RODO. W celu wykonania obowiązku, o którym mowa w zdaniu poprzedzającym, podmiot przetwarzający zobowiązany jest prowadzić dokumentację opisującą sposób przetwarzania danych i realizację wymogu art. 32 RODO.
4. Podmiot przetwarzający nie jest uprawniony do przekazywania danych osobowych osobom trzecim,

X Udostępnianie danych osobowych.

1. Udostępnienie danych osobowych podmiotowi zewnętrznemu (w tym organom publicznym) może nastąpić wyłącznie po pozytywnym zweryfikowaniu ustawowych przesłanek dopuszczalności takiego udostępnienia.
2. Przez weryfikację, o którym mowa w pkt 10.1 należy rozumieć przepis prawa nakazujący udostępnienie danych organom publicznym lub pisemny wniosek podmiotu uprawnionego z wskazaną podstawą prawną.
3. Udostępnianie danych osobowych podmiotom innym niż dla organów publicznych może nastąpić wyłącznie za zgodą Administratora Danych Osobowych lub inną uprawnioną przez niego osobę.
4. Na wniosek pochodzący od osoby, której dane dotyczą, informacje o danych osobowych dotyczących tej osoby muszą być udzielone w terminie nie dłuższym niż 30 dni od daty złożenia wniosku.

XI Prawa osób, których dane dotyczą.

1. Zakres informacji, jaki musi uzyskać osoba, której dane dotyczą został określony we wzorze dokonania obowiązku informacyjnego stanowiący załącznik do Polityki

2. Można odstąpić od informowania osoby, której dane dotyczą w zakresie wymienionym w pkt 11.1 w przypadku, gdy:
   a. przepis prawa ogranicza zakres obowiązku informacyjnego;
   b. osoba, której dane dotyczą, posiada informacje, o których mowa w pkt 11.1.
3. Wymóg określony w pkt 11.1 może być dokonywany na formularzach służących do zbierania danych.
4. W przypadku przetwarzania danych pozyskanych z innego źródła niż od osoby, której dane dotyczą obowiązek informacyjny należy zrealizować w najkrótszym rozsądnym terminie jednak nie dłuższym niż miesiąc od chwili pozyskania danych, a w przypadku, gdy dane mają służyć do komunikacji najpóźniej przy pierwszej komunikacji z tą osobą.
5. Każdy osoba, której dane dotyczą ma prawo uzyskania informacji o tym czy jego dane są przetwarzane.
6. Osoba, której dane dotyczą ma prawo żądania sprostowania i uzupełnienia niekompletnych danych wykazując się dowodami na niekompletność lub nieprawidłowość danych.
7. Poprawienie lub uzupełnienie danych następuję bez zbędnej zwłoki i realizowane jest bezpośrednio przez pracownika upoważnionego do przetwarzania przedmiotowych danych.
8. W przypadku, gdy:
   a. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
   b. osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie;
   c. dane osobowe były przetwarzane niezgodnie z prawem;
   d. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie, któremu podlega administrator;
9. Osoba, której dane dotyczą ma prawo żądania usunięcia danych.
10. Punkt 11.09 nie ma zastosowania, gdy dane są przetwarzane:
    a. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
    b. do ustalenia, dochodzenia lub obrony roszczeń
11. Za realizację pkt. 11.09 odpowiada kierownik komórki organizacyjnej w której są przetwarzane dane lub osoba wskazana przez ADO, z podaniem dla ADO przyczyny przetwarzania danych.
12. Osobie, której dane dotyczą przysługuje prawo żądania ograniczenia przetwarzania danych osobowych w następujących sytuacjach:
    a. osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;
    b. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
    c. administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń.
13. ADO nie profiluje oraz nie podejmuje decyzji dotyczących osób, których dotyczą dane w sposób zautomatyzowany.