

## **POLITYKA BEZPIECZEŃSTWA FUNDACJI ORCHIDEA**

Administrator danych - Fundacja ORCHidea ul. Bukowa 55c, 62-052 Walerianowo, NIP  
7773256099.

### **Wstęp**

Polityka bezpieczeństwa jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań rozporządzenia PE i RE 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, zwane dalej RODO.

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z tym rozporządzeniem, a także usprawnienie i usystematyzowanie organizacji pracy Administratora.

### **DEFINICJE**

**Administrator (danych)** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych, w ramach niniejszego dokumentu jest to Fundacja ORCHidea ul. Bukowa 55c, 62-052 Walerianowo, NIP 7773256099.

**RODO** – rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 4 maja 2016 r.).

**Dane osobowe** - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną przez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego. tożsamość tej osoby fizycznej.

**Przetwarzanie danych osobowych** to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.

**Ograniczenie przetwarzania** - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania

**Anonimizacja** - zmiana danych osobowych, w wyniku której dane te tracą charakter danych osobowych.

**Zgoda osoby, której dane dotyczą** - oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić.

**Ocena skutków w ochronie danych** - to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.

**Podmiotem danych** jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.

**Odbiorca** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

**Podmiot przetwarzający (procesor)** to osoba fizyczna lub prawna, organ publiczny, agencja lub jakiegokolwiek inny organ przetwarzający dane osobowe w imieniu Administratora.

**Inspektor Ochrony Danych (IOD)** - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/podmiotowi przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i tej

polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

**Pseudonimizacja** - oznacza przetwarzanie danych osobowych w taki sposób (np. przez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

**Szczególne kategorie danych osobowych** - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące naturalnego życia seksualne osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.

**Profilowanie** – jest dowolną formą zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

**Naruszenie ochrony danych osobowych** - jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

## **1. Ocena skutków (analiza ryzyka)**

Ocena skutków jest formalną, określoną w art. 37 RODO procedurą przeprowadzenia analizy ryzyka, za wykonanie której odpowiada Administrator. Jeżeli Administrator nie jest zobowiązany do przeprowadzenia oceny skutków, może mimo to stosować tę procedurę do przeprowadzenia analizy ryzyka na potrzeby wykazania rozliczalności spełnienia wymagań RODO.

W przypadku powołania Inspektora Ochrony Danych – ocena skutków musi być wykonana z jego współudziałem oraz po wyrażeniu przez niego opinii.

Ocena skutków winna być dokonywana każdorazowo, w przypadku zmiany okoliczności związanych z przetwarzaniem danych osobowych (np. wprowadzenia nowych wzorów dokumentów, nowego oprogramowania itp.) w tym zmian dotyczących nośników komputerowych czy oprogramowani (zmian w EWIDENCJI NOŚNIKÓW i OPROGRAMOWAŃ KOMPUTEROWYCH ZAWIERAJĄCYCH DANE OSOBOWE (zał. nr 9 do POLITYKI BEZPIECZEŃSTWA – Druk-EK, w oparciu o WZÓR RAPORT Z OCENY SKUTKÓW DLA OCHRONY DANYCH (zał. nr 1 do POLITYKI BEZPIECZEŃSTWA Druk- ROc).

Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

Administrator konsultuje się z organem nadzorczym przed rozpoczęciem przetwarzania, jeżeli ocena skutków dla ochrony danych, wykazała, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka.

### **1.1. Opis operacji przetwarzania (inwentaryzacja aktywów)**

W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć.

### **1.2. Ocena niezbędności oraz proporcjonalności (zgodność z przepisami RODO)**

W ramach przeprowadzenia oceny skutków (analizy ryzyka) Administrator zobowiązany jest do spełnienia wobec nich obowiązków prawnych. Należy przede wszystkim zapewnić, że :

- 1) dane te są legalnie przetwarzane (na podstawie art. 6, 9 RODO),
- 2) dane te są adekwatne w stosunku do celów przetwarzania,
- 3) dane te są przetwarzane przez określony czas – zasada ograniczonego czasu,

- 4) wobec tych osób wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14 RODO) wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody),
- 5) opracowano klauzule informacyjne dla powyższych osób,
- 6) istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28 RODO).

### **1.1. Analiza ryzyka**

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Analiza ryzyka powinna być dokonana na podstawie raportu oceny ryzyka.

### **1.3. Plan postępowania z ryzykiem**

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne
2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

## **1. Upoważnienia**

1. Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach papierowych, systemach informatycznych.
2. Wzór upoważnienia stanowi załącznik nr 2 do POLITYKI BEZPIECZEŃSTWA
3. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie Administratora lub na podstawie przepisu prawa.
4. Upoważnienia określają zakres operacji na danych podgląd, wprowadzanie, zmienianie, usuwanie.
5. Administrator prowadzi rejestr osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych według wzoru, który stanowi załącznik nr 3 do POLITYKI BEZPIECZEŃSTWA.

## 1. Instrukcja postępowania z incydentami

a.i.1. Zagrożeniem bezpieczeństwa informacji jest sytuacja, w której występuje zagrożenie zaistnienia incydentu. Przykładowy katalog zagrożeń:

- 2) nieprzestrzeganie Polityki przez osoby przetwarzające dane, np. niezamykanie pomieszczeń, szaf, biurek, brak stosowania zasad ochrony haseł,
- 3) niewłaściwe zabezpieczenie fizyczne dokumentów, urządzeń lub pomieszczeń,
- 4) niewłaściwe zabezpieczenie oprogramowania lub sprzętu IT przed wyciekiem, kradzieżą lub utratą danych osobowych.

2. Postępowanie Administratora danych osobowych lub osoby przez niego upoważnionej w przypadku stwierdzenia wystąpienia zagrożenia:

- 1) ustalenie zakresu i przyczyn zagrożenia oraz jego ewentualnych skutków,
- 2) w miarę możliwości przywrócenie stanu zgodnego z zasadami ochrony danych osobowych,
- 3) w razie konieczności zainicjowanie działań dyscyplinarnych,
- 4) zarekomendowanie działań zapobiegawczych w kierunku wyeliminowania podobnych zagrożeń w przyszłości,
- 5) sporządzenie RAPORTU Z NARUSZENIA DANYCH OSOBOWYCH wg załącznika nr 4 do niniejszej POLITYKI BEZPIECZEŃSTWA (druk – RN).
- 6) zawiadomienie osoby, której dane dotyczą o naruszeniu danych osobowych wg załącznika nr 5 do niniejszej POLITYKI BEZPIECZEŃSTWA (druk-ZawN).
- 7) załączenie raportu do rejestru naruszeń bezpieczeństwa.

3. Incydem jest sytuacja naruszenia bezpieczeństwa informacji ze względu na dostępność, integralność i poufność. Incydenty powinny być wykrywane, rejestrowane i monitorowane w celu zapobieżenia ich ponownemu wystąpieniu. Przykładowy katalog incydentów:

- 1) losowe zdarzenie wewnętrzne, np. awaria komputera, serwera, twardego dysku, błąd użytkownika, informatyka, zgubienie danych,

- 2) losowe zdarzenie zewnętrzne, np. klęski żywiołowe, zalanie, awaria zasilania, pożar,
- 3) incydent umyślny, np. wyciek informacji, ujawnienie danych nieupoważnionym osobom, świadome zniszczenie danych, działanie wirusów komputerowych, włamanie do pomieszczeń lub systemu informatycznego (wewnętrzne i zewnętrzne).
4. Postępowanie Administratora/Inspektora Ochrony Danych lub właściwej osoby przez niego upoważnionej w przypadku stwierdzenia wystąpienia incydentu:
  - 1) ustalenie czasu zdarzenia będącego incydem,
  - 2) ustalenie zakresu incydem,
  - 3) określenie przyczyn, skutków oraz szacowanych zaistniałych szkód,
  - 4) zabezpieczenie dowodów,
  - 5) ustalenie osób odpowiedzialnych za naruszenie,
  - 6) usunięcie skutków incydem,
  - 7) ograniczenie szkód wywołanych incydem,
  - 8) zainicjowanie działań dyscyplinarnych,
  - 9) zarekomendowanie działań zapobiegawczych w kierunku wyeliminowania podobnych zagrożeń w przyszłości,
  - 10) udokumentowanie prowadzonego postępowania w rejestrze naruszeń.
5. Postępowanie Upoważnionego w przypadku stwierdzenia wystąpienia zagrożenia do czasu przybycia Administratora lub upoważnionej przez niego osoby:
  - 1) powstrzymanie się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,
  - 2) zabezpieczenie elementów systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osób nieupoważnionych,

- 3) podjęcie, stosownie do zaistniałej sytuacji, wszelkich niezbędnych działań celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.
- 4) Zawiadomienie organu nadzoru zgodnie z obowiązującymi przepisami prawa przez Administratora/Inspektora ochrony danych osobowych w ciągu 72 godzin od wystąpienia naruszenia.
- 5) Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie, o którym mowa powyżej nie jest wymagane, w następujących przypadkach:
- 6) a) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
- 7) b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa powyżej;
- 8) c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skutecznym sposobie.

## **1. Szkolenia**

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi powinna być poddana przeszkoleniu i zapoznana z przepisami RODO.
2. Za przeprowadzenie szkolenia odpowiada Administrator/Inspektor Ochrony Danych o ile zostanie powołany.
3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia



4. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

## **1. Rejestr czynności przetwarzania**

W przypadku konieczności prowadzenia rejestru czynności przetwarzania przez Administratora, Administrator/Inspektor Ochrony Danych taki odpowiedni rejestr prowadzi w formie pisemnej i elektronicznej według wzoru stanowiącego załącznik nr 6 do niniejszej POLITYKI BEZPIECZEŃSTWA.

## **2. Audyty**

Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania, przynajmniej raz na rok.

## **3. Wykaz zabezpieczających środków organizacyjnych**

1. Opracowano i wdrożono politykę bezpieczeństwa..
2. Do przetwarzania danych dopuszczono wyłącznie osoby posiadające ważne upoważnienia nadane przez Administratora Danych.
3. Prowadzona jest ewidencja - rejestr osób upoważnionych do przetwarzania danych.
4. Osoby zatrudnione przy przetwarzaniu danych zaznajomiono z przepisami dotyczącymi ochrony danych osobowych.
5. Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.
6. Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązano do zachowania ich w tajemnicy;
7. Monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

8. Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.
9. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
10. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.
11. Stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe według wzoru stanowiącego załącznik nr 7 do POLITYKI BEZPIECZEŃSTWA oraz prowadzi się REJESTR umów powierzenia, który stanowi wzór nr 8 do POLITYKI BEZPIECZEŃSTWA.
12. W podmiocie prowadzi się politykę czystego biurka i ekranu.

### **Środki ochrony fizycznej danych**

1. Dane osobowe przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).
2. Dane osobowe przechowywane są w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej.
3. Pomieszczenia, w którym przetwarzane są dane osobowe chronione są przez firmę ochroniarską.
4. Dane osobowe w formie papierowej jest przechowywany w zamkniętej metalowej szafie z atestami oraz w szafie pancerniej.
5. Kopie zapasowe/archiwalne danych osobowych są przechowywane w zamkniętej szafie lub kase pancerniej.
6. Pomieszczenie, w którym przetwarzane są dane osobowe zabezpieczone jest przed skutkami pożaru za pomocą wolnostojącej gaśnicy.

7. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

### **Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej**

1. Dane osobowe przetwarzane są przy użyciu komputera stacjonarnego i przenośnego.
2. Komputery służące do przetwarzania danych osobowych nie jest połączony z lokalną siecią komputerową.
3. Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej/ komputerze przenośnym zabezpieczono go przed nieautoryzowanym uruchomieniem za pomocą hasła – oddzielne profile .
4. Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
5. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.

Załączniki :

Nr 1 RAPORT Z OCENY SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH Druk -ROc

Nr 2 WZÓR UPOWAŻNIENIA Druk- UP

Nr 3 REJESTR OSÓB UPOWAŻNIONYCH Druk- RU

Nr 4 RAPORT Z NARUSZENIA DANYCH OSOBOWYCH Druk- RN

Nr 5 ZAWIADOMIENIE OSOBY, KTÓREJ DANE DOTYCZĄ O NARUSZENIU Druk- ZawN

Nr 6 REJESTR CZYNNOŚCI PRZETWARZANIA

Nr 7 UMOWA POWIERZENIA Druk-UmP

Nr 8 REJEST UMÓW POWIERZENIA Druk- RUmP

Nr 9 EWIDENCJA NOŚNIKÓW i OPROGRAMOWAŃ KOMPUTEROWYCH ZAWIERAJĄCYCH DANE OSOBOWE – Druk-EK.