Polityka
Ochrony Danych Osobowych

Niniejsza Polityka Ochrony Danych Osobowych w Fundacji Centaurus z siedzibą we Wrocławiu, ul. Wałbrzyska nr 6-8, 52-315Wrocław, wpisana do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej prowadzonego w Krajowym Rejestrze Sądowym przez Sąd Rejonowy we Wrocławiu, VI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000257551, Regon 020319750, NIP 8982093147

wprowadzona została uchwałą Zarządu Fundacji Centaurus z dnia 24 maja 2018 r. w sprawie wprowadzenia w Fundacji Centaurus Polityki Ochrony Danych Osobowych.

Spis treści oraz załączników

Spis załączników

Wstęp

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez administratora danych tj. Fundację Centaurus z siedzibą we Wrocławiu, ul. Wałbrzyska nr 6-8, 52-315Wrocław, wpisana do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej prowadzonego w Krajowym Rejestrze Sądowym przez Sąd Rejonowy we Wrocławiu, VI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000257551, Regon 020319750, NIP 8982093147 w celu spełnienia wymagań:

1. 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) (Tekst mający znaczenie dla EOG) - **dalej jako RODO lub rozporządzenie ogólne,**
2. ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000), **dalej jako ustawa.**

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa w podmiocie będącym administratorem danych osobowych i jest zgodnie z powyższym rozporządzeniem ogólnym oraz ustawą.

Użyte w polityce zwroty oznaczają:

1. **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 przypadku tej polityki Fundację Centaurus z siedzibą we Wrocławiu, ul. Wałbrzyska nr 6-8, 52-315Wrocław, wpisana do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej prowadzonego w Krajowym Rejestrze Sądowym przez Sąd Rejonowy we Wrocławiu, VI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000257551, Regon 020319750, NIP 8982093147.

2. **RODO** lub **rozporządzenie ogólne** – 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) (Tekst mający znaczenie dla EOG).

3. **Dane osobowe** - wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych (fizycznych, fizjologicznych, genetycznych, umysłowych, ekonomicznych, kulturowych lub społecznych) odnoszących się do tożsamość tej osoby fizycznej.

4. **Przetwarzanie danych osobowych** - 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.

5. **Ograniczenie przetwarzania** - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania u Administratora.

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

7. **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.

8. **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.

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

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

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

12. **Inspektor Ochrony Danych Osobowych (IODO) -** to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/Podmiotowi przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

13. **Pseudonimizacja -** oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez 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.

14. **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 życie 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.

15. **Profilowanie** – jest dowolną forma 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,

16. **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.

Ocena skutków (analiza ryzyka).

Ocena skutków jest formalną, określoną w art. 35 RODO procedurą przeprowadzenia analizy ryzyka za wykonanie której odpowiada Administrator. 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.

Jeżeli Administrator nie jest zobowiązany do przeprowadzenia oceny skutków, może mimo to stosować poniższą procedurę do przeprowadzenia analizy ryzyka na potrzeby wykazania rozliczalności spełnienia wymagań przewidzianych w rozporządzeniu ogólnym.

W przypadku powołania Inspektora Ochrony Danych Osobowych (IODO) – ocena skutków musi być wykonana z jego współudziałem.

Opis operacji przetwarzania (inwentaryzacja aktywów).

1. W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć. **Dane te w postaci zbiorów (kategorii osób) zostały wykazane w załączniku nr 2 tj. rejestr czynności przetwarzania danych (wykaz zbiorów danych osobowych).**
2. Opis zbiorów (kategorii osób) powinien obejmować takie informacje, jak:
    1) nazwę zbioru (opis kategorii osób);
    2) opis celów przetwarzania;
    3) charakter, zakres, kontekst danych osobowych;
    4) odbiorcy danych;
    5) funkcjonalny opis operacji przetwarzania;
    6) aktywa służące do przetwarzania danych osobowych (informacje, programy, systemy operacyjne, Infrastruktura IT, Infrastruktura, pracownicy i współpracownicy, outsourcing);
    7) informacja o konieczności wpisu do rejestru czynności przetwarzania;
    8) informacja o konieczności przeprowadzenia oceny skutków dla zbioru.

Niezależnie od powyższego, opracowano klauzule informacyjne dla powyższych osób (zob. załącznik nr 3 Klauzule informacyjne).

Ocena niezbędności oraz proporcjonalności (zgodność z przepisami RODO).

W ramach przeprowadzenia oceny skutków (analizy ryzyka) Administrator zobowiązany jest do spełnienia obowiązków prawnych wobec danych w zbiorach (dla kategorii osób) określonych w załączniku nr 2 do polityki tj. rejestr czynności przetwarzania danych osobowych.

Administrator, w szczególności powinien zapewnić, że :

1) dane te są legalnie przetwarzane (na podstawie art. 6 i/lub/oraz art. 9 RODO);
2) dane te są adekwatne w stosunku do celów przetwarzania;
3) dane te są przetwarzane przez określony czas (retencja danych);
4) wobec tych osób wykonano tzw. obowiązek informacyjny - na podstawie 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 (zob. załącznik nr 3 klauzule informacyjne);
6) istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28 RODO) zgodnie z **załącznikiem nr 4 - wzór umowy powierzenia;**
7) wykaz podmiotów przetwarzających prowadzony jest w **załączniku nr 5 - rejestr umów powierzenia;**
8) potwierdzenie spełnienia powyższych wymagań prawnych RODO znajduje się w załączniku 2 tj. rejestr czynności przetwarzania danych (wykaz zbiorów danych osobowych).

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.

Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru lub grupy zbiorów (kategorii osób) lub dla procesów przetwarzania. W przypadku Fundacji Centaurus z siedzibą we Wrocławiu poddano analizie i ocenie pod kątem zasadności przeprowadzenie analizy ryzyka dla każdego z wykazanych zbiorów danych tj.:

1) Kandydaci do pracy;
2) Pracownicy etatowi, umowy zlecenia, byli pracownicy;
3) Dostawcy towarów na potrzeby fundacji;
4) Rejestr korespondencji;
5) Rejestr wejść i wyjść;
6) Monitoring;
7) Rejestr zawiadomień i interwencji;
8) Zbiór adresowy darczyńców;
9) Newsletter;
10) Eko Klub;
11) Zbiór SMS;
12) Klienci sklepu internetowego;
13) Wolontariusze;
14) Petycje;
15) Adopcje - zwierząt gospodarskich;
16) Adopcje – psy i koty.

Definicje odnoszące się do analizy ryzyka:

1. Aktywa – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych.
2. Naruszenie (Incydent) ochrony danych osobowych - to 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.
3. Zagrożenie - potencjalne naruszenie (potencjalny incydent).

4. Skutki - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia).
5. Ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów.

Wyznaczenie zagrożeń

1. Administrator jest odpowiedzialny za określenie listy zagrożeń naruszenia poufności, dostępności i integralności, które mogą wystąpić w przetwarzaniu danych w zbiorze, dla kategorii osób lub w procesie przetwarzania.
2. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zidentyfikowanych aktywów.
3. **Wykaz potencjalnych zagrożeń znajduje się w załączniku nr 6.**

Wyliczenie ryzyka dla zagrożeń

1. Administrator określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze (dla kategorii osób) lub w procesie przetwarzania.
2. Proponowaną skalę prawdopodobieństwa prezentuje Tabela A.
3. Administrator określa Skutki (**S**) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne
4. Proponowaną Skalę skutków prezentuje Tabela B
5. Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: **R = P * S**

Tabela A PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
małe (1.000,00 zł incydent prasowy lokalny)	1
średnie (1.001,00-10.000,00 zł., incydent prasowy ogólnopolski)	2

duże (od 10.001,00 zł. naruszenie prawa)	3

Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem

1. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem.
2. Proponowaną skalę Ryzyka prezentuje Tabela C

Tabela C POZIOM RYZYKA	**WARTOŚĆ [R = P*S]**
ryzyko pomijalne i akceptowalne (akceptujemy)	1-2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3-6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

Reakcja na wartość ryzyka

1. Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń.
2. Działania obniżające ryzyko, które może zastosować Administrator:
    a. Przeniesienie –przerzucenie ryzyka (outsourcing, ubezpieczenie)
    b. Unikanie – eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza obszar organizacji)
    c. Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. zaszyfrowanie pendrivów z danymi wynoszonych poza firmę)

Wykaz przykładowych zabezpieczeń do znajduje się w załączniku nr 7. tj. lista potencjalnych zabezpieczeń.

3. Analizę ryzyka przeprowadza się w specjalnym szablonie, którego przykładowy wzór stanowi **załącznik nr 8 tj. arkusz analizy ryzyka.**

Ponowna analiza ryzyka

Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów/kategorii osób, realizacja nowych procesów przetwarzania, zmiany prawne).

Plan postępowania z ryzykiem

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne, w celu wdrożenia Planu postępowania z ryzykiem. **Wzór planu postępowania z ryzykiem stanowi załącznik nr 9 do polityki.**
2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

Upoważnienia

1. Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach (dla kategorii osób) w postaci papierowej oraz w systemach informatycznych dla wybranych osób.
2. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.
3. Upoważnienia nadawane są na wniosek przełożonych osób. Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie – zob. **załącznik nr 10 wzór upoważnienia do przetwarzania danych osobowych**.
4. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia administratora w postaci umowy powierzenia.
5. Administrator lub Inspektor Ochrony Danych Osobowych prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych dla osób upoważnionych. **Ewidencja osób upoważnionych stanowi załącznik nr 11 do upoważnienia.**

Środki organizacyjne i techniczne zabezpieczające dane osobowe

Administrator jest zobowiązany do stosowania środków technicznych i organizacyjnych (zabezpieczeń) adekwatnych do zagrożeń naruszenia praw i wolności osób.

1. Administrator prowadzi uproszczony wykaz stosowanych zabezpieczeń. **Wykaz zabezpieczeń na dzień 25 czerwca 2018 r. stanowi załącznik nr 12 do polityki.**
2. Administrator opracował **załącznik nr 13 tj. procedura zabezpieczenia danych osobowych** w którym zabezpieczenia są opisane w formie procedur.
3. Wykaz powinien być aktualizowany, jeśli zajdzie taka potrzeba po przeprowadzeniu analizy ryzyka lub oceny skutków.

Regulamin Ochrony Danych Osobowych

Regulamin (rozumiany jako zabezpieczenie) ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania. **Regulamin ochrony danych osobowych stanowi załącznik nr 14 do polityki.**

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania oraz w zależności od potrzeb dodatkowego złożenia oświadczenia woli dotyczącego:

1. **załącznik nr 15 oświadczenie o poufności dla pracownika/zleceniobiorcy;**
2. **załącznik nr 16 oświadczenie o poufności dla os. sprzątającej/ochrony;**
3. **załącznik nr 17 polityka kluczy;**
4. **załącznik nr 18 procedura niszczenia danych;**
5. **załącznik nr 19 procedura postępowania z nośnikami i sprzętem poza siedzibą fundacji;**
6. **załącznik nr 20 regulamin używania komputerów przenośnych.**

Szkolenia

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu lub zapoznana z przepisami RODO.
2. Za przeprowadzenie szkolenia odpowiada Administrator.
3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia zawierającego następujące informacje:

Plan szkolenia wewnętrznego z zakresu znajomości zasad ochrony danych osobowych

Zakres szkolenia:

- Definicje dot. Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.
- Definicje dot. Ustawy o ochronie danych osobowych
- Legalność przetwarzania danych osobowych
- Obowiązek informacyjny
- Zasady ujawniania oraz powierzania danych osobowych
- Prowadzenie rejestru czynności przetwarzania
- Przepisy karne
- Przegląd zbiorów danych osobowych oraz programów służących do ich przetwarzania
- Przegląd treści Polityki Ochrony Danych Osobowych
- Zabezpieczenia fizyczne obszarów przetwarzania
- Zasady bezpiecznego użytkowania sprzętu IT
- Zasady bezpiecznego korzystania z oprogramowania
- Zasady bezpiecznego korzystania z internetu
- Zasady bezpiecznego korzystania z poczty elektronicznej
- Nadawanie upoważnień do przetwarzania danych osobowych
- instrukcja postępowania w przypadku wystąpienia incydentu
- Postępowanie dyscyplinarne

4. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania przez podpisanie Oświadczenia o poufności - załącznik nr 15.

Instrukcja postępowania z incydentami

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego. Przełożony powiadamia niezwłocznie Inspektora Ochrony Danych Osobowych.
2. Do typowych podatności bezpieczeństwa danych osobowych należą:
   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
   a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),
   c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
4. W przypadku stwierdzenia wystąpienia incydentu, Administrator (lub w przypadku powołania – Inspektor Ochrony Danych Osobowych) prowadzi postępowanie wyjaśniające w toku, którego:
   a) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki,
   b) inicjuje ewentualne działania dyscyplinarne,
   c) działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu,
   d) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.
5. Administrator lub działający w fundacji IODO dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych,

jego skutki oraz podjęte działania zaradcze – w sposób określony w **załączniku nr 21 formularz rejestracji incydentu.**

6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.

7. **W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – Administrator zgłasza je organowi nadzorczemu.**

8. 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.

Rejestr czynności przetwarzania

1. Administrator prowadzi rejestr zgodnie z załącznikiem nr 2.

Audyty

Na podstawie art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

W tym celu Administrator stosuje **procedurę audytów określoną w załączniku nr 22** do polityki.

Procedura przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego (BCP)

Zgodnie z art. 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. Administrator opracował procedury przywracania, opisane w **załączniku nr 23 plan ciągłości działania.**