**ZARZĄDZENIE NR 56**
**Dyrektora Ośrodka Rozwoju Edukacji w Warszawie**
**z dnia 9 listopada 2023 r.**

**w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Ośrodku Rozwoju Edukacji w Warszawie**

Na podstawie § 12 ust. 1 pkt 1) Regulaminu Organizacyjnego Ośrodka Rozwoju Edukacji w Warszawie wprowadzonego zarządzeniem nr 6 Dyrektora Ośrodka Rozwoju Edukacji w Warszawie z dnia 6 grudnia 2016 r. oraz § 5 ust. 1 Statutu Ośrodka Rozwoju Edukacji w Warszawie wprowadzonego Zarządzeniem Ministra Edukacji i Nauki z dnia 26 lipca 2022 r. w sprawie nadania statutu Ośrodkowi Rozwoju Edukacji w Warszawie ogłoszonego w Dzienniku Urzędowym Ministra Edukacji i Nauki (poz. 71), a także 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. z 2016 r. Nr 119, str. 1 z późn. zm.) zarządza się, co następuje:

**§1**

W Ośrodku Rozwoju Edukacji w Warszawie wprowadza się dokumentację opisującą sposób przetwarzania danych osobowych oraz środki organizacyjne i techniczne zapewniające ochronę przetwarzanych danych osobowych, na którą składają się:

1) Polityka Bezpieczeństwa Informacji stanowiąca załącznik nr 1 do niniejszego Zarządzenia;

**§2**

Dokumentacja, o której mowa w § 1 niniejszego Zarządzenia stanowi komplementarny zbiór wewnętrznych aktów z zakresu ochrony danych osobowych, obowiązujących w Ośrodku Rozwoju Edukacji w Warszawie.

**§3**

Traci moc Zarządzenie nr 5/2023 Dyrektora Ośrodka Rozwoju Edukacji w Warszawie z dnia 27 stycznia 2023 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Ośrodku Rozwoju Edukacji w Warszawie.

**§4**

Zarządzenie wchodzi w życie z dniem podpisania.

p.o. DYREKTOR
Ośrodka Rozwoju Edukacji
w Warszawie
mgr inż. Tomasz Madej

**Załącznik Nr 1**
**do Zarządzenia Nr 56**
**Dyrektora ORE**
**z dnia 09 listopada 2023 r.**

ORE Ośrodek Rozwoju Edukacji

# POLITYKA BEZPIECZEŃSTWA INFORMACJI

## Ośrodek Rozwoju Edukacji

ORE Ośrodek Rozwoju Edukacji
Aleje Ujazdowskie 28
00-478 Warszawa
tel. 22 345 37 00
fax 22 345 37 70
www.ore.edu.pl

## Spis treści

## 1. Wprowadzenie

W związku ze swoją statutową działalnością Ośrodek Rozwoju Edukacji w Warszawie (ORE) przetwarza dane osobowe. Przetwarzaniu podlegają dane osobowe pracowników, nauczycieli, uczestników szkoleń oraz innych osób współpracujących, lub zaangażowanych w działalność Ośrodka.

Polityka Bezpieczeństwa Informacji jest podstawowym elementem dokumentacji opisującej zasady przetwarzania danych osobowych w ORE oraz opisuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze.

Polityka Bezpieczeństwa Informacji opisuje sposób realizacji przez ORE obowiązku zapewnienia poufności, integralności i dostępności danych osobowych, wynikający z przepisów 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. z 2016 r. Nr 119, str. 1 z późn. zm.), oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781).

## 2. Zakres stosowania Polityki Bezpieczeństwa Informacji

Polityka Bezpieczeństwa Informacji obowiązuje wszystkich pracowników ORE, jak również osoby i podmioty współpracujące z ORE w oparciu o umowy cywilno-prawne, porozumienia oraz na podstawie innych aktów prawnych, biorące udział w przetwarzaniu danych osobowych administrowanych przez ORE lub uzyskujące do nich dostęp.

Stosowanie Polityki Bezpieczeństwa Informacji obejmuje także przetwarzanie danych osobowych, których Administratorem nie jest ORE, a które ORE przetwarza jako Podmiot Przetwarzający na podstawie zawartych umów powierzenia przetwarzania danych w tym związanych z realizacją projektów finansowanych ze środków Unii Europejskiej.

Zasady określone w Polityce Bezpieczeństwa Informacji mają zastosowanie przy przetwarzaniu danych osobowych w każdej formie (utrwalonych w zbiorach elektronicznych, papierowych, w przekazach ustnych, nagraniach audio i wideo itp.).

Obowiązkiem wszystkich biorących udział w przetwarzaniu danych osobowych jest bezwzględne przestrzeganie Polityki Bezpieczeństwa Informacji. Niestosowanie się do Polityki stanowi istotne naruszenie obowiązków wynikających ze stosunku pracy, innych umów czy porozumień i wiąże się z konsekwencjami określonymi w rozdziale 5.

## 3. Definicje

W dokumencie **Polityki Bezpieczeństwa Informacji** wykorzystywane są poniższe definicje:

1) **Administrator Danych (AD)** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
2) **Inspektor Ochrony Danych (IOD)** - osoba powołana przez Administratora Danych, co do powołania której dokonano zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych, której zadaniem jest wspieranie Administratora Danych w realizacji obowiązków dotyczących ochrony danych osobowych.
3) **Administrator Systemów Informatycznych (ASI)** - osoba odpowiedzialna za utrzymanie, administrację i techniczne aspekty systemów i infrastruktury informatycznej.
4) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej, lub możliwej do zidentyfikowania osoby fizycznej.
5) **PUODO** – Prezes Urzędu Ochrony Danych Osobowych - organ nadzorczy do spraw ochrony danych osobowych.
6) **kierownik komórki organizacyjnej** - osoba kierująca pracą komórki organizacyjnej ORE, biorąca udział w procesie przetwarzania danych osobowych, odpowiedzialna za składanie wniosków o przyznanie i odebranie uprawnień w systemach informatycznych oraz upoważnień do przetwarzania danych osobowych.

7) **odbiorca danych osobowych** – każdy, komu udostępnia się dane osobowe, z wyłączeniem osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, podmiotu, któremu powierzono przetwarzanie danych w drodze umowy zawartej na piśmie, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
8) **ORE** - Ośrodek Rozwoju Edukacji z siedzibą w Warszawie (00-478), Aleje Ujazdowskie 28,
9) **osoba upoważniona** – pracownik lub współpracownik ORE upoważniony do przetwarzania danych osobowych na podstawie pisemnego upoważnienia.
10) **Polityka** – niniejsza Polityka Bezpieczeństwa Informacji.
11) **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.
12) **system informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych; za system informatyczny nie uważa się aplikacji biurowych (edytor tekstu, arkusz kalkulacyjny, itp.),
13) **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 (ogólne rozporządzenie o ochronie danych) ) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).
14) **Upoważniony pracownik Zespołu Kadr** – pracownik Zespołu Kadr upoważniony przez Dyrektora ORE do wystawiania upoważnień i prowadzenia ewidencji wydanych upoważnień.
15) **Ustawa** - Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781).
16) **użytkownik** – osoba korzystająca z Systemów Informatycznych w ORE,

## 4. Środki techniczne i organizacyjne zastosowane w celu ochrony przetwarzanych danych osobowych

W celu zapewnienia adekwatnej do zagrożeń ochrony danych osobowych, tj. zapewnienia ich poufności, integralności i dostępności, zastosowano szereg środków zarówno technicznych, jak i organizacyjnych opisanych poniżej.

### Zarządzanie ryzykiem

Podstawowym elementem zarządzania bezpieczeństwem informacji w ORE jest przeprowadzanie okresowej analizy ryzyka i opracowanie planów postępowania z ryzykiem. Wyniki analizy ryzyka stanowią podstawę podejmowania wszelkich działań w zakresie utrzymania i doskonalenia zabezpieczeń informacji.
Analiza ryzyka prowadzona jest zgodnie z procedurą zarządzania ryzykiem opisaną w dokumencie **Instrukcja zarządzania ryzykiem w Ośrodku Rozwoju Edukacji w Warszawie**

### Struktura organizacyjna

Obowiązek poprawnego i bezpiecznego przetwarzania danych osobowych spoczywa na wszystkich osobach upoważnionych do przetwarzania danych osobowych (pracownikach i osobach spoza ORE).
Szczegółowy zakres obowiązków dla poszczególnych ról w strukturze organizacyjnej przedstawiono poniżej:

I. **Administrator Danych** ponosi ostateczną odpowiedzialność za ochronę danych osobowych w ORE, realizuje następujące zadania wynikające z Polityki Bezpieczeństwa Informacji:

1) wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z przepisami prawa.
2) udziela upoważnień do przetwarzania danych osobowych.
3) powołuje i odwołuje **IOD** oraz jego zastępców,
4) zawiadamia PUODO o powołaniu i odwołaniu **IOD** oraz jego zastępców,
5) zatwierdza i wdraża dokumentację dotyczącą przetwarzania danych osobowych, w tym Politykę Bezpieczeństwa Informacji,
6) akceptuje wdrożenia nowych systemów, aplikacji i elektronicznych zbiorów danych osobowych
7) akceptuje stosowane środki zabezpieczeń danych osobowych.
8) akceptuje wnioski o nadanie upoważnienia do przetwarzania danych osobowych i uprawnień w systemach informatycznych.
9) Zgłasza do PUODO naruszenia ochrony danych osobowych w przypadku stwierdzenia, że naruszenie to stanowi wysokie ryzyko naruszenia praw i wolności osób których dane dotyczą

II. **Zespół Kadr – realizuje następujące zadania wynikające z Polityki Bezpieczeństwa Informacji:**

1) kieruje nowozatrudnionych pracowników na wewnętrzne szkolenie z zakresu ochrony danych osobowych,
2) wnioskuje o upoważnienie nowozatrudnionych pracowników do przetwarzania danych osobowych i nadanie im uprawnień w systemach: domena ORE, Poczta elektroniczna ORE, System EZD,
3) **upoważniony pracownik Zespołu Kadr** przygotowuje upoważnienia do przetwarzania danych osobowych dla pracowników ORE i osób spoza ORE,
4) **upoważniony pracownik Zespołu Kadr** prowadzi ewidencję osób upoważnionych do przetwarzania danych,
5) **upoważniony pracownik Zespołu Kadr** przechowuje kopie upoważnień pracowników.

III. **Inspektor Ochrony Danych (IOD) – odpowiada za nadzór nad przestrzeganiem zasad ochrony danych osobowych określonych w Polityce, realizuje następujące zadania wynikające z Polityki Bezpieczeństwa Informacji:**

1) weryfikuje i nadzoruje przestrzeganie przepisów dotyczących przetwarzania danych osobowych w tym Polityki,
2) bierze udział w tworzeniu i aktualizowaniu Polityki i dokumentacji przetwarzania danych osobowych (instrukcje, regulaminy, procedury),
3) bierze udział w procesie wdrażania nowych systemów, aplikacji i elektronicznych zbiorów danych osobowych
4) opiniuje środki zabezpieczeń (informatycznych, fizycznych i organizacyjnych) przed ich implementacją,
5) zapewnia szkolenia użytkowników w zakresie ochrony danych osobowych,
6) prowadzi rejestr czynności przetwarzania oraz rejestr kategorii czynności przetwarzania.

**IV. Administrator Systemów Informatycznych (ASI) odpowiada za utrzymanie systemów informatycznych w ORE, zgodnie z zasadami określonymi w Polityce oraz uznanymi praktykami w zakresie bezpieczeństwa informacji, realizuje następujące zadania wynikające z Polityki Bezpieczeństwa Informacji:**

1) zakłada i usuwa konta użytkowników, nadaje/usuwa/modyfikuje uprawnienia w systemach informatycznych na pisemny wniosek , **Administratora Danych**, **kierowników komórek organizacyjnych ORE** lub **IOD,**
2) ewidencjonuje identyfikatory w systemie informatycznym, jeżeli system nie pozwala na automatyczne wygenerowanie raportu zawierającego identyfikatory użytkowników oraz przekazuje **upoważnionemu pracownikowi Zespołu Kadr** informacje o identyfikatorach przydzielonych użytkownikom w poszczególnych systemach w celu uzupełnienia zapisów w **ewidencji osób upoważnionych,**
3) utrzymuje i administruje systemami informatycznymi, przeprowadza okresowy przegląd systemów informatycznych,
4) konfiguruje i zabezpiecza systemy informatyczne zgodnie z Polityką i zaleceniami **IOD**,
5) zapewnia bezpieczeństwo danych i systemów informatycznych,
6) utylizuje nośniki i sprzęt wycofane z użytku,
7) akceptuje instalację nowego oprogramowania na komputerach ORE.

Zadania **ASI** mogą być realizowane przez podmiot zewnętrzny na zlecenie ORE na podstawie pisemnej umowy lub porozumienia. W takim przypadku podmiot zewnętrzny wskazuje na piśmie osobę, która będzie pełnić funkcję **ASI**.

**V. Kierownicy komórek organizacyjnych ORE odpowiadają za nadzór nad podległymi im pracownikami, także w zakresie stosowania się ich do wymogów Polityki, RODO oraz Ustawy, realizują następujące zadania wynikające z Polityki :**

1) biorą udział w procesie zarządzania uprawnieniami poprzez składanie pisemnych wniosków do ASI o przyznanie i odebranie podległym pracownikom uprawnień w systemach informatycznych, w przypadku zmiany zakresu ich obowiązków lub potrzeby nadania **dodatkowych uprawnień** .
2) nadzorują przestrzeganie zasad przetwarzania danych osobowych przez podległych pracowników,
3) wyrażają zgodę na instalację dodatkowego oprogramowania na stacjach roboczych,
4) wnioskują do **ASI** o odtworzenie danych z kopii zapasowej,
5) informują **IOD** o nowych czynnościach przetwarzania danych osobowych, prowadzonych w formie tradycyjnej (papierowej) lub elektronicznej,
6) współpracują z **IOD, ASI** i **Administratorem Danych** w celu zapewnienia bezpieczeństwa danych osobowych.

**VI. Osoby upoważnione – pracownicy lub współpracownicy ORE, upoważnieni do przetwarzania danych osobowych mają obowiązek:**

1) przestrzegają przepisów w zakresie ochrony danych osobowych, Polityki Bezpieczeństwa Informacji i dokumentów powiązanych,
2) posiadają ważne upoważnienie przed przystąpieniem do przetwarzania danych osobowych i przechowują je w sposób umożliwiający okazanie go na żądanie.
3) zgłaszają naruszenia bezpieczeństwa informacji do przełożonego lub **IOD,**
4) nadzorują osoby nieupoważnione w obszarze przetwarzania danych osobowych,
5) biorą udział w organizowanych szkoleniach, w razie potrzeby zgłaszają do kierownika komórki organizacyjnej potrzeby szkoleniowe z zakresu ochrony danych osobowych,
6) zapewniają odpowiednie zabezpieczenie danych osobowych, zgodnie z zaleceniami **IOD**, w przypadku korzystania z nośników lub sprzętu komputerowego poza siedzibą ORE,

7) korzystają z systemów informatycznych w sposób gwarantujący ich bezpieczeństwo i poprawne działanie, współpracują z **IOD** i **Administratorem Danych** w celu zapewnienia bezpieczeństwa danych osobowych.

## Zasady przetwarzania danych osobowych i korzystania z systemów informatycznych

Poprawne przetwarzanie danych osobowych i korzystanie z systemów informatycznych jest fundamentem ochrony danych osobowych. Dane osobowe powinny być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed utratą ich poufności, niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. W ORE wprowadzono następujące zasady w tym zakresie:

1) przed przystąpieniem do przetwarzania danych osobowych, każdy użytkownik musi zostać upoważniony do przetwarzania danych osobowych. Upoważnienie do przetwarzania danych osobowych dla nowo zatrudnionych pracowników jest nadawane na wniosek **Kierownika Zespołu Kadr** lub upoważnionego przez niego pracownika. Za poprawność danych podanych we wniosku odpowiedzialna jest osoba wnioskująca. Ewidencja upoważnień do przetwarzania danych osobowych jest prowadzona przez **pracownika ORE upoważnionego do wystawiania upoważnień**;
2) przed opuszczeniem stanowiska pracy należy (zasada czystego biurka):
   a) wyłączyć komputer lub wylogować się ze stacji roboczej,
   b) zabezpieczyć dokumenty papierowe i nośniki wykorzystywane podczas pracy, poprzez umieszczenie ich w zamykanych szafach lub biurkach, w razie potrzeby zniszczyć kopie dokumentów w niszczarce,
3) dokumenty papierowe i nośniki nie nadające się do dalszego wykorzystania mogą zostać zniszczone wyłącznie po uzyskaniu akceptacji pracownika Wydziału Administracyjnego wyznaczonego do obsługi Archiwum.
4) w pobliżu koszy na śmieci nie należy pozostawiać przedmiotów i materiałów nieprzeznaczonych do utylizacji,
5) niemieszczące się w koszach na śmieci przedmioty i materiały przeznaczone do utylizacji a nie zawierające danych osobowych, innych danych chronionych lub podlegających archiwizacji należy układać obok koszy na śmieci z widocznym i wyraźnym opisem „do wyrzucenia",
6) materiały przeznaczone do zniszczenia w niszczarce należy układać obok koszy na śmieci z widocznym i wyraźnym opisem „do zniszczenia".
7) komputery i systemy informatyczne w Ośrodku Rozwoju Edukacji w Warszawie mogą być wykorzystywane wyłącznie do przetwarzania informacji należących do Ośrodka Rozwoju Edukacji w Warszawie;
8) należy korzystać z systemów informatycznych, komputerów i infrastruktury informatycznej Ośrodka Rozwoju Edukacji w Warszawie wyłącznie w celu realizacji zadań na rzecz Ośrodka Rozwoju Edukacji w Warszawie;
9) kategorycznie zabronione jest korzystanie z zasobów informatycznych Ośrodka Rozwoju Edukacji w Warszawie w celu osiągnięcia korzyści materialnych, niezwiązanych z wykonywaniem obowiązków dla Ośrodka Rozwoju Edukacji w Warszawie (zlecenia realizowane dla innych podmiotów, itp.);
10) Ośrodek Rozwoju Edukacji w Warszawie zastrzega sobie prawo do dostępu do informacji związanych z wykonywaniem obowiązków dla Ośrodka Rozwoju Edukacji w Warszawie przetwarzanych w systemach informatycznych i komputerach będących jego własnością;
11) zabronione jest w szczególności:
   a) odwiedzanie niezabezpieczonych lub wykazywanych jako niebezpieczne przez program antywirusowy, stron internetowych;
   b) korzystanie z poczty prywatnej w celach służbowych i poczty służbowej w celach prywatnych;
   c) korzystanie z zewnętrznych nośników pamięci nie należących do ORE bez zgody Administratora Danych i Administratora Systemów Informatycznych;
   d) wykorzystywanie poczty elektronicznej do rozsyłania żartów, SPAM-u, ogłoszeń, łańcuszków itp.
   e) korzystanie z systemów informatycznych w sposób naruszający obowiązujące przepisy prawa (np. pobieranie nielegalnego oprogramowania, filmów, muzyki, itp.);
12) rozpoczęcie, zakończenie i przerwanie pracy w systemach informatycznych powinno się odbywać zgodnie z zasadami określonymi w Instrukcji Przetwarzania Danych Osobowych i Korzystania z Systemów Informatycznych;
13) przy korzystaniu z komputerów i nośników przenośnych należy uwzględniać specyficzne zagrożenia związane z tymi zasobami:
   a) należy chronić urządzenia przenośne i nośniki przed zgubieniem lub kradzieżą,

b) dostęp do urządzeń mobilnych (telefony komórkowe, tablety, laptopy) powinien być zabezpieczony co najmniej hasłem lub numerem PIN
c) zaleca się stosowanie szyfrowania danych;
d) zabronione jest korzystanie z nośników nie należących do Ośrodka Rozwoju Edukacji w Warszawie;
e) na stacjach roboczych będących własnością Ośrodka Rozwoju Edukacji zablokowana jest możliwość korzystania z nośników przenośnych (dyski zewnętrzne, pamięci flash, pendrive)
f) zakaz wymieniony w pkt. d) nie dotyczy stacji roboczych użytkowanych przez pracowników Kancelarii oraz Archiwum Zakładowego.
g) dane na nośnikach wielokrotnego zapisu (flash, pendrive, dyski zewnętrzne itp.) powinny być usunięte po ich wykorzystaniu (przeniesieniu danych na stacje roboczą);
h) nie należy wynosić nośników lub komputerów przenośnych poza siedzibę Ośrodka Rozwoju Edukacji w Warszawie bez zgody Dyrektora ORE.
i) w przypadku utraty nośnika lub urządzenia przenośnego należy niezwłocznie zawiadomić Inspektora Ochrony Danych.

14) Wprowadza się zakaz korzystania ze służbowej poczty za pośrednictwem narzędzi teleinformatycznych (w szczególności: laptopów, tel. komórkowych, tabletów itp.) będących prywatną własnością pracowników Ośrodka Rozwoju Edukacji w Warszawie.
15) Zakaz wymieniony w pkt 14 nie obejmuje pracowników wykonujących swoje obowiązki poza siedzibą ORE, pod warunkiem zachowania zasad dotyczących bezpiecznego przetwarzania danych osobowych opisanych w Polityce Bezpieczeństwa Informacji ORE oraz zastosowania następujących minimalnych wymagań dotyczących zabezpieczenia komputerów:
a) wejście i zmiana ustawień BIOS/UEFI powinna wymagać podania hasła,
b) możliwość uruchamiania systemu z sieci lub innych nośników niż dysk twardy komputera powinna zostać wyłączona,
c) długość hasła BIOS/UEFI: nie mniej niż 10 znaków (co najmniej 1 wielka litera i 1 cyfra),
d) zainstalowany i działający system zabezpieczający przed atakami zewnętrznymi typu firewall,
e) wdrożone mechanizmy zapewniające aktualizację systemu firewall,
f) wdrożony i uruchomiony mechanizm aktualizacji systemu operacyjnego oraz jego składników,
g) zainstalowane i działające oprogramowanie antywirusowe czasu rzeczywistego,
h) wdrożone mechanizmy zapewniające aktualizację sygnatur antywirusowych nie rzadziej niż raz w tygodniu,
i) wdrożone regulacje zapewniające pełne skanowanie antywirusowe co najmniej raz w tygodniu,
j) Wdrożony wymóg podania loginu i hasła przed uzyskaniem dostępu do danych umieszczonych na komputerze,
k) Hasło użytkownika powinno być zmieniane co 90 dni,
l) Hasło powinno być różne od 20 poprzednich haseł,
m) Hasło nie powinno być łatwe do odgadnięcie to znaczy:
i. Powinno się składać z minimum 12 znaków,
ii. Hasła nie mogą zawierać nazwy konta użytkownika ani części jego pełnej nazwy dłuższej niż dwa kolejne znaki,
iii. Hasła muszą zawierać znaki z co najmniej trzech spośród następujących czterech kategorii:
(1) wielkie litery alfabetu łacińskiego (od A do Z),
(2) małe litery alfabetu łacińskiego (od A do Z),
(3) cyfry systemu dziesiętnego (od 0 do 9),
(4) znaki niealfabetyczne (np. !, @, #, $, %).
n) Po 5-krotnej nieudanej próbie uzyskania dostępu, konto użytkownika jest blokowane na 10 minut,
o) Użytkownik jest zobowiązany do nie pozostawiania komputera bez nadzoru oraz nie udostępniania go osobom trzecim,
p) Bieżąca praca powinna odbywać się z wykorzystaniem konta użytkownika nieposiadającego uprawnień administracyjnych, chyba że bieżąca praca tego wymaga,

q) Login i hasło do konta umożliwiającego dostęp do danych na komputerze lub poczcie elektronicznej nie mogą być przekazywane osobom trzecim,
r) Hasło powinno być chronione przed dostępem osób trzecich; w każdym przypadku gdy hasło zostało ujawnione innej osobie, pracownik jest zobowiązany do jego zmiany,
s) Po skasowaniu danych należy opróżnić kosz systemowy,
t) W przypadku wątpliwości lub dodatkowych pytań związanych z zapewnieniem minimalnych wymagań dotyczących zabezpieczeń komputerów istnieje możliwość uzyskania wsparcia pod adresem it.ore.edu.pl.

Szczegółowe zasady przetwarzania danych osobowych i korzystania z systemów informatycznych określono w **Instrukcji Przetwarzania danych osobowych i korzystania z systemów informatycznych"** która stanowi **Załącznik nr 2** do Polityki Bezpieczeństwa Informacji.

## Zbieranie danych osobowych

Zbieranie danych osobowych, bezpośrednio lub przy użyciu systemów informatycznych, wiąże się z koniecznością spełnienia następujących wymogów:

1) Określenia podstawy prawnej przetwarzania danych osobowych zgodnie z obowiązującymi w tym zakresie przepisami,
2) Określenia celu przetwarzania danych i nie przetwarzania ich niezgodnie z zadeklarowanym celem,
3) Ograniczenia zakresu zbieranych danych tylko do takich. które są niezbędne dla realizacji celu,
4) Poinformowania osób, której dane dotyczą o:
   a) nazwie i siedzibie Administratora oraz jego danych kontaktowych,
   b) danych kontaktowych Inspektora Ochrony Danych,
   c) celach i podstawach prawnych przetwarzania,
   d) odbiorcach danych osobowych lub o kategoriach odbiorców,
   e) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu,
   f) prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
   g) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) - informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
   h) o prawie wniesienia skargi do organu nadzorczego,
   i) o tym czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
   j) o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu,
   k) o kategoriach przetwarzanych danych oraz ich źródle jeżeli dane zbierane są z innego źródła niż osoba, której dotyczą.
5) w przypadku gdy dane zbierane są na podstawie zgody (art. 6 ust. 1 lit. a RODO), zgoda taka powinna zostać udokumentowana
6) wzór zgody na przetwarzanie danych stanowi **Załącznik nr 12 - Zgoda na Przetwarzanie Danych Osobowych**.

## Przetwarzanie danych osobowych przez podmioty lub osoby spoza ORE

W uzasadnionych przypadkach możliwe jest dopuszczenie osób niebędących pracownikami ORE, do przetwarzania danych osobowych administrowanych przez ORE. Dotyczyć to może zewnętrznych konsultantów, audytorów, stażystów i praktykantów oraz osób świadczących na rzecz ORE usługi w oparciu o umowy cywilno-prawne, którzy wykonując zlecone im zadania mogą uzyskiwać dostęp do danych osobowych. W takim przypadku należy:

1) zapoznać w/w osoby z Polityką Bezpieczeństwa Informacji i dokumentami powiązanymi oraz podstawowymi zasadami przetwarzania danych osobowych;
2) potwierdzić znajomość Ustawy przez te osoby poprzez złożenie przez nie stosownego oświadczenia;
3) upoważnić osoby do przetwarzania danych osobowych zgodnie z zakresem wynikającym z zakresu realizowanych zadań;

4) uzyskać od osób zobowiązanie do zachowania poufności w zakresie przetwarzanych danych osobowych i innych informacji mogących mieć wpływ na bezpieczeństwo tych danych a także stosowania się do Polityki Bezpieczeństwa Informacji poprzez złożenie przez nie stosownego oświadczenia.

Wzór upoważnienia do przetwarzania danych osobowych, klauzuli potwierdzających znajomość RODO, Ustawy, Polityki, oraz zobowiązanie do zachowania poufności stanowi **Załącznik nr 5 – Wzór Upoważnienia do Przetwarzania Danych Osobowych.**

W uzasadnionych przypadkach możliwe jest przyznanie tymczasowego dostępu do sieci ORE w celu:

1) dostępu do sieci Internet dla gości – w takim przypadku należy umożliwić gościom skorzystanie z wydzielonej, dedykowanej podsieci, z której nie jest możliwy dostęp do sieci lokalnej ORE;
2) Wykonania czynności serwisowych lub audytu w systemach ORE – w tym przypadku konieczne jest:
   a) nadzorowanie pracy serwisantów lub audytorów przez pracowników ORE,
   b) upoważnienie serwisanta lub audytora do przetwarzania danych osobowych (jeśli dochodzi do przetwarzania danych osobowych bez nadzoru upoważnionych pracowników ORE).

Zgodnie z Art. 28 RODO możliwe jest również **powierzenie przetwarzania danych osobowych innym podmiotom** w drodze umowy zawartej na piśmie. Taka sytuacja może mieć miejsce w przypadku współpracy z firmami lub organizacjami zewnętrznymi przetwarzającymi dane osobowe administrowane przez ORE – np. usługi w zakresie realizacji procesów kadrowych, księgowych, utrzymania systemów informatycznych itp. W takim wypadku należy:

1) zapoznać przedstawicieli podmiotu z wymogami Polityki Bezpieczeństwa Informacji ORE,
2) zawrzeć z podmiotem umowę o zachowaniu poufności,
3) zawrzeć z podmiotem umowę o powierzeniu przetwarzania danych osobowych w zakresie wynikającym z zakresu świadczonych usług.
4) Zakres klauzul umownych, który winien znaleźć się w umowach dotyczących powierzenia przetwarzania danych osobowych zawiera **Załącznik nr 13 – Wzór umowy powierzenia przetwarzania**

### Udostępnianie danych osobowych

W uzasadnionych przypadkach dane osobowe mogą zostać udostępnione podmiotom lub osobom spoza ORE na podstawie przepisów prawa lub w przypadku, gdy odbiorca przedstawi uzasadnioną prawnie przyczynę udostępnienia tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą. W takim wypadku należy:

1) otrzymać pisemny wniosek o udostępnienie danych od podmiotu lub osoby występującej o dostęp do danych osobowych zawierający co najmniej:
   a) dane adresowe i kontaktowe wnioskującego
   b) podstawę prawną udostępnienia
   c) informacje umożliwiające wyszukanie danych osobowych w zbiorze,
   d) informacje o zakresie i przeznaczeniu danych;
2) odnotować w systemie informatycznym służącym do przetwarzania zbioru danych osobowych lub w osobnym dedykowanym do tego celu systemie:
   a) informacje o odbiorcach danych, którym dane osobowe zostały udostępnione,
   b) daty i zakresy tego udostępnienia.

   Szczegółowe informacje dotyczące udostępniania danych osobowych zawarto w dokumencie **Instrukcja Zarządzania Systemami Informatycznymi.**

### Kształcenie z zakresu ochrony danych osobowych

Przed rozpoczęciem przetwarzania danych osobowych, **IOD** zapewnia szkolenie pracowników w zakresie ochrony danych osobowych i umożliwia im zapoznanie się z treścią **RODO**, **Ustawy** oraz **Polityką Bezpieczeństwa Informacji**

Szkolenie może mieć formę stacjonarną lub odbywać się przy użyciu środków komunikacji elektronicznej w tym kursu on-line. Pracownicy lub inne osoby upoważnione do przetwarzania danych osobowych mają obowiązek:

1) zapoznać się z Polityką Bezpieczeństwa Informacji i dokumentami powiązanymi;
2) zapoznać się z przepisami powszechnie obowiązującego prawa dotyczącymi przetwarzania danych osobowych;
3) zapoznać się z zasadami bezpiecznego korzystania z systemów informatycznych i przetwarzania danych osobowych.

Okresowo, w razie uzasadnionej potrzeby, Administrator Danych zleca IOD przeprowadzenie szkolenia wybranej grupy lub konkretnych osób z zakresu przetwarzania i ochrony danych osobowych oraz bezpiecznego korzystania z systemów informatycznych.

Przełożeni pracowników powinni okresowo weryfikować znajomość w/w zagadnień przez pracowników. W wyniku weryfikacji mogą skierować pracownika na ponowne przeszkolenie i/lub zgłosić wniosek do Administratora Danych o cofnięcie upoważnienia dla pracownika.

### Uwierzytelnienie, kontrola dostępu i rozliczalność

Uwierzytelnienie i kontrola dostępu są podstawowym środkiem ochrony systemów informatycznych i danych osobowych przetwarzanych w formie elektronicznej przed dostępem osób lub procesów nieupoważnionych.

Uwierzytelnienie pozwala potwierdzić tożsamość użytkownika, tj. potwierdzić, że jest on tą osobą, za którą się podaje.

Kontrola dostępu ma na celu przydzielenie użytkownikowi odpowiednich uprawnień do danych lub funkcji systemu, w zależności od tego jakie zadania wynikają z jego obowiązków na stanowisku pracy.

Rozliczalność oznacza możliwość przypisania osoby do konkretnych działań w systemie informatycznym, lub bezpośrednio na danych osobowych, tj. możliwość wskazania dla konkretnej operacji przeprowadzonej w systemie informatycznym lub na danych osobowych konkretnej osoby, która wykonała tę operację.

W ORE stosowane są następujące środki w celu uwierzytelnienia użytkowników:

1) każda osoba korzystająca z systemu informatycznego posiada własny unikalny identyfikator w poszczególnych systemach informatycznych, identyfikator ten nie jest przypisywany do innej osoby nawet, gdy jego właściciel zaprzestanie korzystania z niego;
2) jeżeli w systemie są przetwarzane dane osobowe zabronione jest korzystanie ze wspólnego identyfikatora (konta) przez wielu użytkowników;
3) niedopuszczalne jest udostępnianie plików lub innych zasobów zawierających dane osobowe w sieci lokalnej, bez uwierzytelnienia użytkownika;
4) zaleca się stosowanie systemów informatycznych umożliwiających sporządzenie czytelnego raportu pozwalającego na przyporządkowanie identyfikatorów poszczególnym użytkownikom; raport powinien zawierać:
   a) nazwę identyfikatora użytkownika,
   b) imię i nazwisko użytkownika,
   c) stan konta użytkownika (zablokowany/aktywny itp.),
   d) datę założenia/zablokowania identyfikatora;
5) jeżeli system informatyczny nie pozwala na stworzenie w/w raportu, ewidencja identyfikatorów w systemie jest prowadzona manualnie przez ASI w formie dokumentu elektronicznego lub papierowego (chyba, że z systemu korzysta jeden użytkownik), na podstawie którego pracownik prowadzący ewidencję upoważnień uzupełnia **Załącznik nr 6 - Wykaz Osób Upoważnionych** o informacje o identyfikatorach;
6) podstawowym środkiem uwierzytelnienia jest indywidualne hasło użytkownika; podstawowe zasady stosowania haseł określono poniżej:
   a) hasło powinno składać się z co najmniej 12 znaków,
   b) hasło powinno być złożone (trudne do odgadnięcia) i składać się z małych i wielkich liter, cyfr i/lub znaków specjalnych, nie powinno składać się z prostych wyrazów,
   c) hasło powinno być zmieniane raz na 90 dni i różnić się od 20 poprzednich haseł,

d) identyfikator (konto) użytkownika jest blokowany na 10 minut po wielokrotnej (5 razy) niepoprawnej próbie uzyskania dostępu (poprzez podanie nieprawidłowego hasła) jeśli system na to pozwala; zdarzenia takie powinny być odnotowywane w dziennikach systemowych,

e) pod żadnym pozorem hasło nie może być komukolwiek przekazywane czy ujawniane (w tym przełożonemu czy osobom odpowiedzialnym za utrzymanie systemów informatycznych),

f) zabrania się zapisywania haseł lub takiego z nimi postępowania, które umożliwia lub ułatwia dostęp do haseł osobom trzecim,

g) jeżeli zachodzi podejrzenie, że hasło zostało ujawnione innej osobie, konieczna jest jego natychmiastowa zmiana,

h) po założeniu identyfikatora w systemie informatycznym użytkownikowi przydzielane jest początkowe hasło, którego zmiana jest systemowo wymuszana przy pierwszym logowaniu;

7) o ile to możliwe zasady haseł powinny zostać wymuszone w systemie informatycznym;

8) w systemach i sieciach teleinformatycznych hasła powinny być przechowywane w taki sposób, aby zminimalizować ryzyko ich poznania przez inne osoby w tym także administratorów, w tym celu systemy informatyczne powinny spełniać następujące warunki:

   a) hasła powinny być przesyłane w formie niejawnej lub poprzez bezpieczne kanały,

   b) hasła powinny być przechowywane w systemach informatycznych w formie niejawnej;

9) wszyscy użytkownicy posiadający dostęp do danych osobowych powinni stosować uwierzytelnienie przy dostępie do swoich stacji roboczych (unikalny identyfikator stworzony przez ASI oraz hasło);

10) szczegółowe informacje dotyczące korzystania z haseł przedstawiono w **Instrukcji przetwarzania danych osobowych i korzystania z systemów informatycznych.**

Obok uwierzytelnienia w systemach informatycznych (tam gdzie to możliwe) zalecane jest stosowanie mechanizmów kontroli dostępu. Kontrola dostępu pozwala na przydzielenie użytkownikowi minimalnych uprawnień wymaganych do realizacji obowiązków. Podstawowe metody kontroli dostępu:

1) użytkownicy posiadają dostęp do danych i funkcji systemu niezbędnych do realizacji swoich obowiązków;
2) uprawnienia są nadawane przez administratorów systemu, nie jest możliwe samodzielne nadawanie sobie uprawnień przez użytkowników;
3) nie jest możliwe usuniecie przez użytkownika informacji o działaniach użytkownika (lub innych użytkowników) na danych lub w systemie informatycznym.

## Nadawanie, odbieranie i zmiana uprawnień w systemach informatycznych

Poprawne zarządzanie uprawnieniami do danych i systemów informatycznych jest kluczowym środkiem zastosowanym w celu ochrony danych osobowych. Zarządzanie uprawnieniami w ORE opiera się na następujących zasadach:

1) zakładanie identyfikatorów oraz nadawanie/odbieranie/zmiana uprawnień w systemach:

   a) domena ORE

   b) Poczta elektroniczna ORE

   c) EZD

   jest realizowane przez Administratora Systemów Informatycznych na wniosek upoważnionego pracownika Zespołu Kadr zaakceptowany przez Dyrektora ORE,

2) Wnioski o przyznanie uprawnień dodatkowych lub kont w systemach innych niż wymienione w punkcie 1 składają kierownicy komórek organizacyjnych ORE, IOD lub Administrator Danych;

3) wnioski o nadanie uprawnień i/lub założenie identyfikatora powinny być udokumentowane (mieć formę pisemną lub elektroniczną);

4) w procesie nadawania uprawnień obowiązuje zasada minimalnych uprawnień – nie jest dopuszczalne nadawanie uprawnień wyższych niż wymagane do realizacji obowiązków na danym stanowisku;

5) uprawnienia w systemach informatycznych mogą być przydzielone wyłącznie osobom upoważnionym do przetwarzania danych osobowych;

6) w przypadku zakończenia stosunku pracy lub zmiany stanowiska pracownika, kierownik Zespołu Kadr lub kierownicy komórek organizacyjnych ORE mają obowiązek złożyć wniosek o odebranie/zmianę uprawnień, IOD okresowo weryfikuje czy informacja o zmianie uprawnień została przekazana do ASI;

7) Identyfikatory i uprawnienia w systemach informatycznych są okresowo weryfikowane przez ASI na podstawie informacji z Zespołu Kadr

8) Szczegółowa procedura nadawania uprawnień została określona w dokumencie **Instrukcja Zarządzania Systemami Informatycznymi Służącymi do Przetwarzania Danych Osobowych**

### Ochrona przed zagrożeniami z sieci zewnętrznej i szkodliwym oprogramowaniem

Dane i systemy informatyczne powinny być odpowiednio zabezpieczone przed zagrożeniami z sieci zewnętrznej (takimi jak hakerzy, szkodliwe oprogramowanie, SPAM, itp.) oraz działaniem szkodliwego oprogramowania (wirusy, spyware, itp.) W tym celu w ORE stosowane są następujące środki:

1) na stacjach roboczych zainstalowane są systemy antywirusowe, które automatycznie aktualizują sygnatury antywirusowe nie rzadziej niż raz w tygodniu;

2) systemy operacyjne stacji roboczych i serwerów są aktualizowane, tak aby wszystkie niezbędne poprawki związane z lukami bezpieczeństwa były zainstalowane niezwłocznie po ich udostępnieniu;

3) sieć lokalna jest oddzielona od sieci publicznej poprzez Firewall, nie ma możliwości bezpośredniego dostępu z sieci Internet do stacji lub serwerów w sieci lokalnej. Usługi internetowe są udostępniane przez serwery umieszczone w DMZ;

4) poczta elektroniczna jest sprawdzana pod kątem szkodliwego oprogramowania i SPAMu.

Szczegółowe informacje dotyczące stosowanych zabezpieczeń określono w dokumencie Błąd! Nie można odnaleźć źródła odwołania. która stanowi **Załącznik nr 1** do **Polityki**.

### Ochrona danych przed utratą

Zapewnienie dostępności danych osobowych, a wiec ich ochrona przed utratą jest kluczowym elementem zapewnienia bezpieczeństwa danych. W celu ochrony przed utratą danych stosowane są następujące środki:

1) dane osobowe przetwarzane w systemach informatycznych w miarę możliwości są przechowywane na serwerach;

2) zbiory danych osobowych w arkuszach kalkulacyjnych i innych dokumentach elektronicznych są w miarę możliwości trzymane na serwerach;

3) cyklicznie wykonywane są kopie zapasowe danych trzymanych na serwerach, częstotliwość tworzenia kopii zapasowych jest adekwatna do częstotliwości zmian w systemie;

4) nie należy trzymać jedynych egzemplarzy danych na stacjach roboczych;

5) w przypadku danych osobowych przechowywanych na stacjach roboczych zalecane jest okresowe tworzenie kopii zapasowych danych trzymanych na stacji roboczej, w tym celu należy zgłosić się do ASI;

6) zabronione jest samowolne tworzenie kopi zapasowych na nośniki przenośne (USB, CD/DVD, inne);

7) zabronione jest wynoszenie kopii zapasowych poza siedzibę ORE bez zgody Administratora;

8) odtworzenie danych z kopii zapasowych jest realizowane przez ASI na wniosek kierowników komórek organizacyjnych ORE lub Administratora Danych;

9) nośniki, na których zapisane są kopie zapasowe powinny być zabezpieczone przed kradzieżą oraz działaniem negatywnych czynników zewnętrznych takich jak pożar, powódź itp.;

10) przydatność kopi zapasowych jest okresowo weryfikowana przez ASI;

11) serwery są zabezpieczone przed utratą danych w przypadku awarii zasilania poprzez urządzenia podtrzymujące napięcie (UPS). Sprawność urządzeń jest okresowo weryfikowana przez ASI.

Szczegółowe informacje dotyczące zabezpieczeń przed utratą danych określono w dokumencie Błąd! Nie można odnaleźć źródła odwołania..

### Wdrożenie Systemów Informatycznych w ORE

W celu zapewnienia odpowiedniego poziomu bezpieczeństwa, zgodności z niniejszą Polityką oraz Ustawą, wdrożenie systemów informatycznych oraz utworzenie nowych zbiorów danych osobowych powinno być odpowiednio nadzorowane.
Przed wdrożeniem nowego systemu informatycznego (bez względu na to czy przetwarzane są w nim dane osobowe), należy:

1) zgłosić do IOD w formie pisemnej, chęć wdrożenia systemu, przedstawić IOD koncepcje systemu, określić jakie dane będą przetwarzane w systemie, kto będzie odpowiedzialny za wdrożenie i utrzymanie systemu, etc.:
   a) IOD na podstawie uzyskanych informacji opiniuje wdrożenie systemu informatycznego i określa wymagane zabezpieczenia systemu,
   b) wszelkie kwestie techniczne IOD konsultuje z ASI,
   c) nie jest dopuszczalne wdrożenie systemu bez spełnienia wymogów określonych przez IOD;
2) wystąpić o formalną zgodę na wdrożenie systemu do Administratora Danych;
3) wdrożenie jest dozwolone:
   a) po formalnej akceptacji Dyrektora ORE,
   b) pozytywnej opinii IOD,
   c) spełnieniu wymogów określonych przez IOD;
4) w przypadku gdy system służy do przetwarzania danych osobowych, IOD aktualizuje dokumentację i w razie potrzeby dokonuje wpisu w Rejestrze czynności przetwarzania.

W przypadku utworzenia/otrzymania/usunięcia nowego zbioru danych osobowych lub modyfikacji struktury zbioru, bez względu na to czy jest to zbiór w formie elektronicznej czy papierowej, należy:

1) niezwłocznie zgłosić ten fakt **IOD**;
2) powstrzymać się od przetwarzania danych osobowych do momentu akceptacji dalszego przetwarzania danych w zbiorze przez **IOD**;
3) uzyskać zgodę **IOD** na przetwarzanie danych osobowych w zbiorze.

### Dostęp fizyczny i zabezpieczenia środowiskowe

Obszar, w którym przetwarzane są dane osobowe jest zabezpieczony poprzez zastosowanie następujących środków zabezpieczeń fizycznych:

1) dostęp do budynków wiąże się z weryfikacją tożsamości odwiedzających;
2) w siedzibach ORE wykorzystywany jest system monitoringu wizyjnego nadzorowanego przez pracowników ochrony;
3) pomieszczenia biurowe w których ma miejsce przetwarzanie danych osobowych są zamykane pod nieobecność pracowników a klucze do tych pomieszczeń wydawane są wyłącznie osobom upoważnionym;
4) Każdorazowe wydanie i odebranie kluczy do pomieszczeń biurowych odnotowywane jest w książce ewidencji kluczy;
5) w pomieszczeniach, w których przetwarzane są dane osobowe, obowiązuje zasada czystego biurka, po zakończeniu pracy dokumenty i nośniki zawierające dane osobowe są zamykane w szafach i biurkach lub niszczone;
6) osoby nieupoważnione do przetwarzania danych osobowych przebywają w obszarach przetwarzania danych osobowych wyłącznie pod nadzorem osób upoważnionych.

Sprzęt informatyczny (serwery, sieć) znajdują się w zabezpieczonych pomieszczeniach.

Pomieszczenia, w których znajdują się serwery wykorzystywane przez Systemy informatyczne, są dodatkowo zabezpieczone, zarówno przed nieautoryzowanym dostępem, jak i przed niekorzystnym wpływem czynników atmosferycznych:

1) dostęp do serwerowni jest ograniczony tylko dla upoważnionych pracowników;
2) wejście do serwerowni objęte jest systemem monitoringu wizyjnego;
3) serwerownie są wyposażone w urządzenia wentylacyjno-klimatyzacyjne;
4) serwery są wyposażone w urządzenia podtrzymujące zasilanie (UPS) urządzenia te są okresowo testowane.

## 5. Naruszenie Polityki Bezpieczeństwa Informacji

Polityka Bezpieczeństwa Informacji jest traktowana, jako wewnętrzny regulamin ORE obowiązujący wszystkich pracowników. Naruszenie zasad określonych w Polityce Bezpieczeństwa Informacji jest traktowane jako naruszenie regulaminu pracy ORE i może stanowić podstawę do wyciągnięcia konsekwencji służbowych, w tym także może być przyczyną wypowiedzenia umowy o pracę lub rozwiązania umowy bez wypowiedzenia, z winy pracownika, zgodnie z przepisami ustawy z dnia 26 czerwca 1974 Kodeks Pracy.

Osoby lub podmioty związane z ORE umowami są zobowiązane do przestrzegania Polityki Bezpieczeństwa Informacji. Naruszenie zasad określonych w Polityce Bezpieczeństwa Informacji może stanowić podstawę do wypowiedzenia umowy, a także dochodzenia dalszych roszczeń na drodze cywilnej.

## 6. Procedury, wzory dokumentów, instrukcje i inne dokumenty tworzące Politykę Bezpieczeństwa Informacji

1) Załącznik nr 1 – Instrukcja zarządzania systemami informatycznymi
2) Załącznik nr 2 - Instrukcja przetwarzania danych osobowych i korzystania z systemów informatycznych
3) Załącznik nr 3 – Procedura postępowania w przypadku naruszeń bezpieczeństwa przetwarzania danych osobowych
4) Załącznik nr 4 - Wniosek o nadanie lub odebranie upoważnienia do przetwarzania danych osobowych oraz uprawnień w systemach informatycznych
5) Załącznik nr 5 – Wzór upoważnienia do przetwarzania danych osobowych
6) Załącznik nr 6 – Wykaz osób upoważnionych.
7) Załącznik nr 7 – Arkusz informacji o udostępnieniu danych.
8) Załącznik nr 8 – Oświadczenie o zachowaniu poufności danych osobowych.
9) Załącznik nr 9 – Oświadczenie o wyrażeniu zgody na używanie prywatnego sprzętu do celów służbowych
10) Załącznik nr 10 – Spis systemów informatycznych
11) Załącznik nr 11 – Rejestr czynności przetwarzania
12) Załącznik nr 12 – Wzór zgody na przetwarzanie danych osobowych.
13) Załącznik nr 13 – Wzór umowy powierzenia przetwarzania danych osobowych.

Aleje Ujazdowskie 28
00-478 Warszawa
tel. 22 345 37 00
fax 22 345 37 70
www.ore.edu.pl

**Podpisy**

Administrator Danych (AD)

Inspektor Ochrony Danych (IOD)

**Załącznik Nr 1**
**do Polityki Bezpieczeństwa Informacji**


# INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI SŁUŻĄCYMI DO PRZETWARZANIA DANYCH OSOBOWYCH

## Ośrodek Rozwoju Edukacji

ORE Ośrodek Rozwoju Edukacji
Aleje Ujazdowskie 28
00-478 Warszawa
tel. 22 345 37 00
fax 22 345 37 70
www.ore.edu.pl

**Spis treści**

## 1. Informacje wstępne

Instrukcja Zarządzania Systemami Informatycznymi, w których przetwarzane są dane osobowe stanowi integralną część dokumentacji przetwarzania danych osobowych w Ośrodku Rozwoju Edukacji w Warszawie.

Instrukcja opisuje zasady utrzymania i zarządzania wszelkimi systemami w ORE, w których przetwarzane są dane osobowe. Instrukcja dotyczy systemów utrzymywanych przez ORE.

W wypadku systemów utrzymywanych przez podmioty spoza ORE, w związku z powierzeniem im przetwarzania danych osobowych, podmioty te mają obowiązek opracować własną instrukcję zarządzania systemem informatycznym zgodną z RODO i wymogami ORE.

Instrukcja jest przeznaczona przede wszystkim dla ASI (Administratorów Systemów Informatycznych). Informacje przeznaczone dla użytkowników systemów informatycznych umieszczono w **Instrukcji Przetwarzania Danych Osobowych i Korzystania z Systemów Informatycznych,** która stanowi **załącznik nr 2 do Polityki Bezpieczeństwa Informacji**.

## 2. Definicje

W dokumencie **Instrukcja Zarządzania Systemami Informatycznymi Służącymi do Przetwarzania Danych Osobowych** wykorzystywane są poniższe definicje:

1) **Administrator Danych (AD)** - organ, jednostka organizacyjna, podmiot lub osoba, decydująca o celach i środkach przetwarzania danych osobowych. Administratorem Danych Osobowych w ORE jest dyrektor Ośrodka.
2) **Administrator Systemów Informatycznych (ASI)** - osoba odpowiedzialna za utrzymanie, administrację i techniczne aspekty systemów i infrastruktury informatycznej.
3) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej, lub możliwej do zidentyfikowania osoby fizycznej.
4) **Inspektor Ochrony Danych (IOD)** - osoba powołana przez Administratora Danych, co do powołania której dokonano zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych, której zadaniem jest wspieranie Administratora Danych w realizacji obowiązków dotyczących ochrony danych osobowych.
5) **Odbiorca danych osobowych** – osoba fizyczna lub prawna, której udostępnia się dane osobowe, z wyłączeniem osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, podmiotu, któremu powierzono przetwarzanie danych w drodze umowy zawartej na piśmie, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
6) **ORE** - Ośrodek Rozwoju Edukacji z siedzibą w Warszawie (00-478), Aleje Ujazdowskie 28,.
7) **Osoba upoważniona** – pracownik lub współpracownik ORE, upoważniony do przetwarzania danych osobowych.
8) **Polityka** –Polityka Bezpieczeństwa Informacji.
9) **Przetwarzanie danych osobowych** – jakiekolwiek czynności wykonywane na danych osobowych takie jak zbieranie, utrwalanie, przechowywanie, odczytywanie, zmienianie, udostępnianie, usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
10) **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych. Za system informatyczny nie uważa się aplikacji biurowych (edytor tekstu, arkusz kalkulacyjny, itp.).
11) **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 (ogólne rozporządzenie o ochronie danych) ) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).
12) **Użytkownik** – osoba korzystająca z Systemów Informatycznych ORE.
13) **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

## 3. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym

Zgodnie z zasadami określonymi w Polityce Bezpieczeństwa Informacji, przed przystąpieniem do przetwarzania danych osobowych konieczne jest:

1) zapoznanie użytkownika z Polityką Bezpieczeństwa Informacji i dokumentami powiązanymi (przeznaczonymi dla użytkowników),
2) potwierdzenie znajomości RODO oraz Ustawy przez użytkownika;
3) uzyskanie upoważnienia Administratora Danych do przetwarzania danych osobowych;
4) w razie potrzeby, zapoznanie użytkownika z podstawowymi zasadami przetwarzania danych osobowych (także w systemach informatycznych);

   Za powyższe zadania odpowiada pracownik Zespołu Kadr. Pracownik Zespołu Kadr udostępnia użytkownikowi Politykę i dokumenty powiązane oraz wskazuje gdzie dostępna jest treść RODO oraz ustawy, przygotowuje wniosek o upoważnienie pracownika do przetwarzania danych osobowych oraz nadanie uprawnień w systemach informatycznych zgodnie z zasadami opisanymi w punkcie 0. niniejszej Instrukcji.
5) założenie identyfikatora i hasła w systemie informatycznym oraz na stacji roboczej (jeśli wymagane),
6) nadanie odpowiednich uprawnień w systemach informatycznych, zgodnych z zakresem zadań realizowanych w ORE.

   Za powyższe odpowiada Administrator Systemu Informatycznego realizujący wniosek o nadanie uprawnień w systemach informatycznych

### 3.1. Upoważnienie do przetwarzania danych osobowych

Upoważnienie do przetwarzania danych osobowych jest wystawiane dla:

a) każdego pracownika Ośrodka Rozwoju Edukacji w Warszawie biorącego udział w przetwarzaniu danych osobowych,
b) osób spoza Ośrodka Rozwoju Edukacji w Warszawie realizujących przetwarzanie danych osobowych lub potencjalnie mogących przetwarzać dane osobowe w związku z realizacją zadań w Ośrodku Rozwoju Edukacji w Warszawie na podstawie umów cywilnoprawnych, umów o wolontariacie, umów o staż lub praktykę studencką.

Upoważnienia są wystawiane przy zatrudnieniu, zmianie stanowiska pracownika bądź zakresu jego obowiązków a także przy rozpoczęciu współpracy z osobami spoza Ośrodka Rozwoju Edukacji w Warszawie, które w ramach swoich zadań przetwarzają lub mogą przetwarzać dane osobowe. Przed wydaniem upoważnienia, Inspektor Ochrony Danych zapoznaje pracownika z zasadami i przepisami dotyczącymi przetwarzania danych osobowych (dotyczy nowozatrudnionych pracowników lub takich, którzy nie odbyli szkolenia).

**Poniżej określono zasady nadawania upoważnień do przetwarzania danych osobowych:**

1) Administrator Danych lub pracownik przez niego upoważniony przygotowuje wniosek o nadanie upoważnienia dla każdego pracownika, który podczas wykonywania obowiązków będzie przetwarzał dane osobowe.
2) Upoważnienie dla pracowników nowozatrudnionych wystawiane jest na wniosek pracownika **Zespołu Kadr**.
3) W przypadku zmiany stanowiska pracownika lub potrzeby rozszerzenia zakresu upoważnienia, wniosek o nadanie upoważnienia przygotowuje **bezpośredni przełożony pracownika**
4) Dla pracowników zatrudnionych na samodzielnych stanowiskach pracy, bądź wicedyrektorów wniosek, o którym mowa w zdaniu poprzedzającym, składa Dyrektor Ośrodka Rozwoju Edukacji w Warszawie, natomiast dla kierowników komórek organizacyjnych bądź zespołów projektowych wniosek składany jest przez właściwego wicedyrektora. Wzór wniosku stanowi **Załącznik nr 4** do Polityki Bezpieczeństwa Informacji;.
5) Powyższe zasady obowiązują także przy:
   a) przyjęciu praktykanta, stażysty, lub wolontariusza;
   b) rozpoczęciu współpracy w oparciu o umowy cywilno-prawne;
6) przy zmianie stanowiska pracownika, jeżeli nowe stanowisko będzie wiązać się z przetwarzaniem danych osobowych, pracownik upoważniony przez administratora przygotowuje upoważnienie do przetwarzania danych osobowych dla pracownika na wniosek bezpośredniego przełożonego. W przypadku absencji osoby uprawnionej do wnioskowania o nadanie uprawnień w systemach informatycznych

lub upoważnienia do przetwarzania danych osobowych, wniosek może być złożony przez wicedyrektora właściwego dla danej komórki organizacyjnej bądź zespołu projektowego lub Dyrektora ORE. Wzór wniosku stanowi załącznik nr 4 do niniejszego zarządzenia.

7) w przypadku podjęcia współpracy z osobami spoza Ośrodka Rozwoju Edukacji w Warszawie, kierownik komórki organizacyjnej lub kierownik projektu, który współpracuje z tymi osobami, ma obowiązek:
   a) pisemnie powiadomić Inspektora Ochrony Danych,
   b) w przypadku, gdy Inspektor Ochrony Danych uzna, że współpraca wiąże się z przetwarzaniem danych osobowych, wystąpić z wnioskiem o upoważnienie,
   c) niedopuszczalne jest rozpoczęcie przetwarzania danych bez upoważnienia;
8) Przed przedłożeniem pracownikowi upoważnionemu do wystawiania upoważnień, wniosku o upoważnienie, podpisanego przez wnioskującego, wymaga on akceptacji:
   a) Kierownika Zespołu Kadr
   b) Inspektora Ochrony Danych
   c) Administratora Danych

   Pozytywna weryfikacja wniosku potwierdzana jest przez wymienione wyżej osoby pieczęcią i podpisem wraz z datą jej dokonania lub akceptacją w systemie EZD.
9) Na podstawie prawidłowo wypełnionego wniosku, pracownik upoważniony do wystawiania upoważnień, wystawia upoważnienie, i przekazuje je upoważnionemu pracownikowi .
10) Pracownik upoważniony do wystawiania upoważnień, prowadzi rejestr upoważnień zawierający co najmniej następujące informacje:
   a) imię i nazwisko osoby upoważnionej,
   b) datę nadania upoważnienia,
   c) numer upoważnienia,
   d) datę ustania upoważnienia,
11) Rejestr wymieniony w pkt 10 może być prowadzony w formie elektronicznej lub papierowej. Wzór Rejestru stanowi **Załącznik nr 6 Wykaz osób upoważnionych;**
12) Wnioski o nadanie upoważnienia przechowuje pracownik upoważniony do wystawiania upoważnień. Wzór upoważnienia do przetwarzania danych osobowych, wraz z oświadczeniem użytkownika o zachowaniu poufności, zapoznaniu się z przepisami o ochronie danych osobowych i Polityką Bezpieczeństwa Informacji, zawarto w **Załączniku nr 5** do Polityki Bezpieczeństwa Informacji;
13) Odebranie upoważnienia następuje w chwili zakończenia stosunku pracy lub zmiany stanowiska pracownika bądź wygaśnięcia umowy cywilnoprawnej, na podstawie której pracownik wykonywał czynności związane z przetwarzaniem danych osobowych i odbywa się na wniosek:
   a) **Kierownika Zespołu Kadr,** w przypadku zakończenia stosunku pracy
   b) **bezpośredniego przełożonego,** w sytuacji zmiany stanowiska pracownika lub wygaśnięcia umowy cywilnoprawnej realizowanej w ramach realizacji zadań komórki.
14) W przypadku absencji osoby uprawnionej do wnioskowania o odebranie upoważnienia do przetwarzania danych osobowych, wniosek może być złożony przez wicedyrektora właściwego dla danej komórki organizacyjnej, wicedyrektora właściwego dla danego zespołu projektowego lub dyrektora Ośrodka Rozwoju Edukacji w Warszawie. Wniosek o odebranie upoważnienia składa się na druku, którego wzór stanowi **Załącznik nr 4** Polityki Bezpieczeństwa Informacji;

### 3.2 Nadawanie identyfikatorów i uprawnień w systemach informatycznych

Procedurą nadawania identyfikatorów i uprawnień w systemach informatycznych objęte są wszystkie systemy informatyczne wykorzystywane w Ośrodku Rozwoju Edukacji w Warszawie. Identyfikatory i uprawnienia w systemach informatycznych nadaje Administrator Systemów Informatycznych, upoważniony Administrator Techniczny lub inna osoba upoważniona przez dyrektora Ośrodka Rozwoju Edukacji w Warszawie.

Identyfikatory i uprawnienia mogą być nadawane na wniosek:

1) Kierownika Zespołu Kadr

2) dyrektora Ośrodka Rozwoju Edukacji w Warszawie;
3) wicedyrektorów Ośrodka Rozwoju Edukacji w Warszawie;
4) kierowników komórek organizacyjnych lub projektów (bezpośrednich przełożonych pracowników);

**Kierownik Zespół Kadr** wnioskuje o nadanie uprawnień dostępu do domeny ORE, poczty elektronicznej ORE oraz systemu EZD dla nowozatrudnionych pracowników.

W przypadku zmiany stanowiska pracy lub potrzeby nadania dodatkowych uprawnień dostępu, wnioski składa **bezpośredni przełożony** pracownika.

W przypadku absencji osoby uprawnionej do wnioskowania o odebranie uprawnień w systemach informatycznych lub upoważnienia do przetwarzania danych osobowych, wniosek może być złożony przez wicedyrektora właściwego dla danej komórki organizacyjnej, wicedyrektora właściwego dla danego zespołu projektowego lub dyrektora Ośrodka Rozwoju Edukacji w Warszawie. Wniosek o odebranie upoważnienia składa się na druku, którego wzór stanowi **Załącznik nr 4** do Polityki Bezpieczeństwa Informacji;.

Poniżej określono zasady nadawania identyfikatorów i uprawnień w systemach informatycznych:

1) wniosek o nadanie uprawnień może być złożony tylko dla osób upoważnionych, chyba że dostęp do systemu nie wiąże się z dostępem do danych osobowych;
2) w przypadku kiedy dostęp do systemu nie wiąże się z dostępem do danych osobowych, ale pracownik będzie wykonywał swoje obowiązki w obszarze przetwarzania danych osobowych lub będzie mógł mieć dostęp do tych danych (np. personel sprzątający), pracownik ten zostaje zapoznany z zasadami bezpieczeństwa w Ośrodku Rozwoju Edukacji w Warszawie oraz podpisuje oświadczenie o obowiązku zachowania poufności danych osobowych, stanowiące **Załącznik nr 8** do Polityki Bezpieczeństwa Informacji;
3) wniosek o nadanie uprawnień jest składany na formularzu , który stanowi **Załącznik nr 4** do Polityki Bezpieczeństwa Informacji;
4) wniosek podpisany przez wnioskującego, przed przedłożeniem go Administratorowi Systemów Informatycznych, wymaga akceptacji:
    a) Kierownika Zespołu Kadr
    b) Inspektora Ochrony Danych
    c) Administratora Danych
5) wniosek jest przekazywany do Administratora Systemów Informatycznych, w formie elektronicznej za pośrednictwem systemu EZD;
6) Administrator Systemów Informatycznych, Administrator Techniczny lub inna osoba upoważniona do nadawania uprawnień wykonuje następujące zadania:
    a) sprawdza czy wniosek zawiera wszystkie niezbędne informacje i podpisy;
    b) zakłada identyfikator na stacji roboczej i hasło początkowe jeżeli do tej pory użytkownik nie miał identyfikatora na stacji roboczej;
    c) zakłada identyfikator w systemie informatycznym i hasło początkowe jeżeli do tej pory użytkownik nie miał identyfikatora w systemie informatycznym;
    d) aktualizuje ewidencje identyfikatorów na stacji roboczej i w systemie informatycznym (jeżeli jest to konieczne) a następnie przesyła informacje o założonym identyfikatorze do pracownika prowadzącego Ewidencję osób upoważnionych w celu umieszczenia go w tej Ewidencji;
    e) nadaje wymagane uprawnienia w systemie informatycznym, jeżeli ma wątpliwości, co do zakresu uprawnień, konsultuje się z Inspektorem Ochrony Danych lub przełożonymi osoby, której dotyczy wniosek;
    f) przekazuje identyfikatory i hasła początkowe pracownikowi, którego dotyczy wniosek,
    g) instruuje pracownika o konieczności zmiany haseł początkowych ustawionych przez Administratora Systemu Informatycznego,
    h) informuje wnioskującego o nadaniu identyfikatora/uprawnień;
    i) przechowuje otrzymany wniosek o nadanie uprawnień.

7) W przypadku, gdy osoba upoważniona kończy współpracę z Ośrodkiem Rozwoju Edukacji w Warszawie lub gdy konkretne uprawnienia nie są już wymagane należy odebrać uprawnienia lub zablokować konto (identyfikator):
    a) w przypadku rozwiązania umowy o pracę, **Kierownik Zespołu Kadr** przesyła do Administratora Systemów Informatycznych, Administratora Technicznego lub innej osoby upoważnionej, wniosek o odebranie uprawnień i zablokowanie konta (wykorzystywany jest **Załącznik nr 4** do Polityki Bezpieczeństwa Informacji, przy czym wnioskujący przekreśla słowo „nadanie"). Wniosek może być złożony również przez wicedyrektora właściwego dla danej komórki organizacyjnej, wicedyrektora właściwego dla danego zespołu projektowego lub dyrektora Ośrodka Rozwoju Edukacji w Warszawie.
    b) wniosek podpisany przez wnioskującego, przed przedłożeniem go Administratorowi Systemów Informatycznych, wymaga akceptacji:
        i) Kierownika Zespołu Kadr
        ii) Inspektora Ochrony Danych
        iii) Administratora Danych
    c) Administrator Systemów Informatycznych, Administrator Techniczny lub inna osoba uprawniona odbiera uprawnienia lub blokuje identyfikator oraz informuje o tym wnioskującego,
    d) Administrator Systemów Informatycznych, Administrator Techniczny lub inna osoba uprawniona przechowuje otrzymany wniosek o odebranie uprawnień;
8) Okresowo, nie rzadziej niż raz na 3 miesiące, Administrator Systemów Informatycznych, Administrator Techniczny lub inna osoba uprawniona przeprowadza przeglądy identyfikatorów i uprawnień:
    a) Administrator Systemów Informatycznych, Administrator Techniczny lub inna osoba uprawniona weryfikuje czy w systemach informatycznych lub na stacjach roboczych nie występują aktywne identyfikatory osób, które zakończyły współpracę z Ośrodkiem Rozwoju Edukacji w Warszawie,
    b) wyniki przeglądu są przesyłane do Inspektora Ochrony Danych.

## 4. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

W ORE stosowane są następujące środki uwierzytelnienia przy dostępie do systemów informatycznych i stacji roboczych:

1) każda osoba posiada własny unikalny identyfikator, identyfikatory nie są współdzielone pomiędzy użytkownikami,
2) stosowane są złożone hasła zgodnie z niżej wymienionymi zasadami:
    a) hasło użytkownika powinno być zmieniane co 90 dni,
    b) hasło powinno być różne od 20 poprzednich haseł,
    c) hasło nie powinno być łatwe do odgadnięcia to znaczy:
        i) powinno się składać z minimum 12 znaków,
        ii) hasła nie mogą zawierać nazwy konta użytkownika ani części jego pełnej nazwy dłuższej niż dwa kolejne znaki,
        iii) hasła muszą zawierać znaki z co najmniej trzech spośród następujących czterech kategorii:
            (1) wielkie litery alfabetu łacińskiego (od A do Z),
            (2) małe litery alfabetu łacińskiego (od A do Z),
            (3) cyfry systemu dziesiętnego (od 0 do 9),
            (4) znaki niealfabetyczne (np. !, @, #, $, %).
3) Po 5-krotnej nieudanej próbie uzyskania dostępu, konto użytkownika jest blokowane na 10 minut
4) dopuszczalne są inne środki uwierzytelnienia zapewniające poziom bezpieczeństwa nie niższy niż złożone hasła (np. karty inteligentne wykorzystywane w systemie Płatnik),
5) identyfikator nie może być wykorzystywany ani przekazywany innym osobom (nawet w przypadku urlopów, zastępstw, itp.),

6) korzystanie z identyfikatora należącego do innych osób lub „wspólnego" identyfikatora jest zabronione,
7) użytkownicy powinni stosować się do zasad tworzenia i korzystania z haseł określonych w Polityce, o ile to możliwe ASI wymusza systemowo zasady haseł,
8) jeśli system na to pozwala, nieudana próba dostępu do systemu powinna być odnotowywana w dziennikach systemowych, administratorzy okresowo powinni przeglądać dzienniki systemu,
9) hasła ustawione przez administratora przy założeniu konta lub gdy użytkownik zapomniał hasła powinno być skomplikowane i unikalne, o ile to możliwe należy wymusić zmianę hasła przy pierwszym użyciu,
10) hasło ustawione przez administratora powinno być przekazane w sposób bezpieczny po weryfikacji tożsamości użytkownika,
11) weryfikacja tożsamości jest wymagana także w przypadku odblokowania konta użytkownika,
12) w systemach i sieciach teleinformatycznych hasła powinny być przechowywane w taki sposób, aby zminimalizować ryzyko ich poznania przez inne osoby w tym także administratorów, w tym celu systemy informatyczne powinny spełniać następujące warunki:
    a) hasła powinny być przesyłane w formie niejawnej lub poprzez bezpieczne kanały, w szczególności w systemach internetowych przesyłanie hasła powinno być zabezpieczone poprzez środki kryptograficzne, zalecane rozwiązania to SSL v3 lub TLS, długość klucza sesyjnego – co najmniej 112 bitów,

b) o ile to możliwe hasła powinny być przechowywane w systemach informatycznych w formie niejawnej.

## 5. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

Procedury rozpoczęcia zawieszenia i zakończenia pracy w systemach informatycznych dla użytkowników systemu zawarto w **Instrukcji Przetwarzania Danych Osobowych i Korzystania z Systemów Informatycznych**.

## 6. Procedury tworzenia kopii zapasowych

Administratorzy systemów informatycznych są zobowiązani do wykonywania okresowych cyklicznych kopi danych przetwarzanych w systemach. Obok danych, konieczne jest dokonywanie kopii konfiguracji systemów operacyjnych, kopi aplikacji oraz konfiguracji aplikacji.

Przy tworzeniu kopii zapasowych obowiązują następujące zasady:

1) o ile to możliwe istotne dane użytkowników powinny być przechowywane na serwerach. Należy minimalizować ilość danych przechowywanych na lokalnych stacjach roboczych,
2) kopie zapasowe danych na serwerach plikowych i aplikacyjnych oraz internetowych są robione codziennie w dni powszednie na nośniki magnetyczne lub na przestrzeń dyskową innego serwera, w innej lokalizacji;
3) w przypadku, gdy system informatyczny jest utrzymywany przez podmiot zewnętrzny (w oparciu o umowę) dopuszczalne jest powierzenie podmiotowi tworzenia kopii zapasowych, pod warunkiem, że spełnione zostaną wymogi ORE;
4) nowe systemy informatyczne powinny być niezwłocznie obejmowane polityką kopii zapasowych po rozpoczęciu użytkowania produkcyjnego;
5) ASI jest zobowiązany do przeglądu dzienników systemów do tworzenia kopii zapasowych i niezwłocznej reakcji w przypadku, gdy kopia nie wykonała się poprawnie;
6) kopie zapasowe stacji roboczych są wykonywane na nośnikach CD/DVD na wniosek użytkownika, docelowo jednak wszelkie istotne dane użytkowników powinny być przechowywane na serwerach;
7) w przypadku, gdy nośnik (wykorzystywany do kopii zapasowej, przenoszenia danych lub pochodzący ze zużytego sprzętu) straci swoją użyteczność powinien zostać zniszczony tak, aby nie było możliwe odtworzenie danych zapisanych na nośniku. Zasady utylizacji nośników określono w punkcie 9 niniejszej Instrukcji.

## 7. Przechowywanie kopii zapasowych zawierających dane osobowe

Kopie zapasowe powinny być przechowywane w bezpiecznej lokalizacji innej niż lokalizacja serwerów.
Kopie zapasowe (nośniki lub serwery, na których trzymane są kopie zapasowe) są przechowywane w budynku w Alejach Ujazdowskich i przy ul. Polnej oraz w budynku Ministerstwa Edukacji Narodowej al. J. Ch. Szucha 25 w Warszawie i zabezpieczone przed nieautoryzowanym dostępem poprzez następujące środki:

1) drzwi zamykane na klucz;
2) instalacja alarmowa;
3) metalowa szafa z zamkiem (nośniki).

## 8. Sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania i zagrożeń z sieci zewnętrznej

Zgodnie z wymogami Polityki Bezpieczeństwa Informacji, dane osobowe i systemy informatyczne powinny być odpowiednio zabezpieczone przed zagrożeniami z sieci zewnętrznej oraz działaniem szkodliwego oprogramowania W tym celu w ORE stosowane są następujące środki:

### 8.1. Zabezpieczenia przeciw wrogiemu oprogramowaniu

1) każda stacja robocza ma zainstalowany system antywirusowy spełniający następujące wymogi:
   a) system automatycznie pobiera nowe sygnatury – raz na kilka dni (zazwyczaj codziennie),
   b) system ma funkcjonalność automatycznego skanowania w momencie dostępu do obiektu (pliku, programu, wiadomości itp),
   c) brak możliwości zmiany konfiguracji systemu przez użytkownika,
   d) uniemożliwienie odinstalowania systemu przez użytkownika lub powiadomienie o odinstalowaniu systemu ze stacji roboczej,
   e) centralne monitorowanie systemu (nieudane aktualizacje, znalezienie wirusa);
2) w uzasadnionych przypadkach systemy antywirusowe są instalowane także na serwerach;
3) system pocztowy powinien zapewniać ochronę antywirusową i anty-spamową:
   a) możliwe jest korzystanie z zewnętrznej usługi poczty pod warunkiem zapewnienia przez dostawcę ochrony antywirusowej i anty-spamowej;
4) użytkownicy powinni zostać zapoznani z **Instrukcją Przetwarzania Danych Osobowych i Korzystania z Systemów Informatycznych** stanowiącą **Załącznik nr 2** do Polityki Bezpieczeństwa informacji, oraz z zasadami bezpiecznego korzystania z dostępu do Internetu i poczty elektronicznej;
5) wszelkie oprogramowanie powinno być instalowane przez ASI, należy ograniczyć możliwość instalacji programów przez użytkowników.

### 8.2. Zabezpieczenia sieciowe

1) sieć lokalna jest oddzielona od sieci publicznej poprzez zaporę sieciową *Firewall*;
2) nie ma możliwości bezpośredniego dostępu z sieci Internet do stacji lub serwerów w sieci lokalnej;
3) wszelkie usługi internetowe są udostępniane przez serwery umieszczone w strefie DMZ;
4) domyślnie firewall blokuje cały ruch przychodzący, poza usługami które zostały *explicite* dozwolone;
5) wszelkie niewykorzystywane reguły firewalla należy blokować lub usuwać;
6) reguły firewall powinny być okresowo weryfikowane przez ASI.

### 8.3. Aktualizacja systemów

1) za aktualizacje systemów odpowiada ASI;
2) w przypadku, gdy system informatyczny jest utrzymywany przez podmiot zewnętrzny (w oparciu o umowę) dopuszczalne jest powierzenie podmiotowi aktualizacji systemów, pod warunkiem, że spełnione zostaną wymogi ORE;
3) stacje robocze i serwery są aktualizowane, tak, aby wszystkie niezbędne poprawki związane z lukami bezpieczeństwa były niezwłocznie zainstalowane;
4) dla stacji roboczych należy zastosować aktualizacje automatyczne, serwery należy aktualizować manualnie;
5) ASI powinni okresowo weryfikować stan aktualizacji na serwerach i wybranej grupie stacji roboczych;

6) obok serwerów i stacji roboczych, należy w razie potrzeby aktualizować także aplikacje, bazy danych oprogramowanie urządzeń sieciowych takich jaki np. Firewall, Switch i inne wykorzystywane oprogramowanie.

### 8.4. Spis systemów informatycznych

1) Pracownik wyznaczony przez Dyrektora ORE prowadzi Spis systemów informatycznych wykorzystywanych w ORE;
2) ASI informuje pracownika prowadzącego Spis o każdym wdrożeniu lub wycofaniu z użytkowania systemu informatycznego;
3) Pracownik prowadzący aktualizuje Spis systemów informatycznych zgodnie z informacjami uzyskanymi od ASI;
4) Spis systemów informatycznych ORE może być prowadzony w formie papierowej lub elektronicznej;
5) Wzór Spisu systemów informatycznych stanowi **Załącznik nr 10** do Polityki Bezpieczeństwa Informacji

## 9. Postępowanie z nośnikami

1) termin nośniki oznacza zarówno nośniki przenośne jak i wbudowane w sprzęcie informatycznym, w szczególności:
   a) dyskietki,
   b) nośniki optyczne (CD\DVD\BlueRay),
   c) nośniki wykorzystywane do tworzenia kopi zapasowych (DDS\LTO, inne),
   d) nośniki przenośnie (Flash),
   e) nośniki wbudowane w sprzęcie informatycznym (dyski twarde, itp.);
2) jeżeli nośnik nie jest używany, należy usunąć z niego dane;
3) w przypadku gdy nośnik straci swoją użyteczność powinien zostać zutylizowany, tak, aby nie było możliwe odtworzenie danych zapisanych na nośniku:
   a) nośniki optyczne i dyskietki należy niszczyć w przystosowanych do tego niszczarkach dokumentów.
   b) nośniki wykorzystywane do tworzenia kopii zapasowych, dyski twarde, nośniki przenośne (Flash), itp. powinny być przekazywane do wyspecjalizowanych podmiotów gwarantujących bezpieczną utylizację nośników i ochronę przed wyciekiem informacji,
   c) za utylizacje nośników odpowiada ASI,
   d) w przypadku utylizacji nośników przez podmioty zewnętrzne, protokół zniszczenia należy przekazać do IOD.

## 10. Odnotowanie informacji o udostępnianiu danych osobowych

W przypadku udostępniania danych osobowych odbiorcom danych zgodnie z Art. 29 ustawy należy:

1) przed udostępnieniem zażądać pisemnego wniosku o udostępnienie danych zawierającego:
   a) dane wnioskodawcy,
   b) informacje pozwalające na jednoznaczne wyszukanie danych osobowych w zbiorze,
   c) uzasadnienie żądania udostępnienia danych;
2) Administrator Danych Osobowych po konsultacjach z IOD akceptuje lub pisemnie odmawia udostępnienia danych;
3) informacja o udostępnieniu jest odnotowywana w arkuszu Excel (**Załącznik nr 7 – Arkusz informacji o udostępnieniu danych**) prowadzonym przez IOD, chyba, że system informatyczny pozwala na odnotowanie informacji o odbiorcach;
4) należy odnotować:
   a) informacje o odbiorcach danych, którym dane osobowe zostały udostępnione,
   b) datę i zakres tego udostępnienia.

Aleje Ujazdowskie 28
00-478 Warszawa
tel. 22 345 37 00
fax 22 345 37 70
www.ore.edu.pl

## 11. Przeglądy i konserwacja systemów informatycznych i nośników

Przeglądy i konserwacje systemów informatycznych są realizowane przez administratorów lub podmioty zewnętrzne, którym zlecono utrzymanie systemów. Przegląd i konserwacja są wykonywane w razie potrzeby i zgodnie z zaleceniami producentów. Konieczne może okazać się realizowanie przeglądów i konserwacji poza godzinami pracy (np. ze względu na konieczność wyłączenia serwerów). Przy serwisie i konserwacji systemów informatycznych i nośników obowiązują następujące zasady:

1) serwis sprzętu komputerowego (serwery, PC) w razie możliwości należy serwisować w siedzibie ORE pod nadzorem ASI;
2) możliwe jest zlecenie prac osobom lub podmiotom spoza ORE. Jeżeli przeglądy lub konserwacja są realizowane przez osoby nieupoważnione powinny odbywać się pod nadzorem ASI;
3) w przypadku gdy sprzęt jest przekazywany do serwisu zewnętrznego dyski twarde (serwery, PC) nie mogą być przekazywane na zewnątrz bez zgody IOD (nawet jeżeli wiąże się to z brakiem możliwości skorzystania z gwarancji);
4) w przypadku awarii dysku twardego, dysk nie może być przesłany do serwisu bez zgody IOD (nawet jeżeli wiąże się to z brakiem możliwości skorzystania z gwarancji).

**Załącznik Nr 2**
**do Polityki Bezpieczeństwa Informacji**


# INSTRUKCJA PRZETWARZANIA DANYCH OSOBOWYCH I KORZYSTANIA Z SYSTEMÓW INFORMATYCZNYCH

## Ośrodek Rozwoju Edukacji

ORE Ośrodek Rozwoju Edukacji
Aleje Ujazdowskie 28
00-478 Warszawa
tel. 22 345 37 00
fax 22 345 37 70
www.ore.edu.pl

## Spis treści

## 1. Informacje wstępne

Niniejsza Instrukcja opisuje zasady poprawnego i bezpiecznego przetwarzania danych osobowych oraz korzystania z systemów informatycznych. Instrukcja uszczegóławia zapisy Polityki Bezpieczeństwa Informacji ORE i jest przeznaczona dla osób upoważnionych do przetwarzania danych osobowych i użytkowników systemów informatycznych. Pracownicy ORE oraz inne osoby dopuszczone do przetwarzania danych osobowych mają obowiązek zapoznać się z niniejszą Instrukcją i stosować się do zawartych w niej zasad.

## 2. Definicje

1) **Inspektor Ochrony Danych (IOD)** - osoba powołana przez Administratora Danych, co do powołania której dokonano zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych, której zadaniem jest wspieranie Administratora Danych w realizacji obowiązków dotyczących ochrony danych osobowych.
2) **Administrator Danych (AD)** - organ, jednostka organizacyjna, podmiot lub osoba, decydująca o celach i środkach przetwarzania danych osobowych. Administratorem Danych w ORE jest Ośrodek Rozwoju Edukacji w Warszawie reprezentowany przez Dyrektora ORE
3) **Administrator Systemów Informatycznych (ASI)** - osoba odpowiedzialna za utrzymanie, administrację i techniczne aspekty systemów i infrastruktury informatycznej;
4) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej, lub możliwej do zidentyfikowania osoby fizycznej;
5) **Instrukcja** – Niniejsza Instrukcja;
6) **IZSI** – Instrukcja Zarządzania Systemami Informatycznymi Służącymi do Przetwarzania Danych Osobowych;
7) **Odbiorca danych osobowych** – osoba fizyczna lub prawna, której udostępnia się dane osobowe, z wyłączeniem osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, podmiotu, któremu powierzono przetwarzanie danych w drodze umowy zawartej na piśmie, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;
8) **ORE** - Ośrodek Rozwoju Edukacji z siedzibą w Warszawie (00-478), Aleje Ujazdowskie 28;.
9) **Osoba upoważniona** – pracownik lub współpracownik ORE, upoważniony do przetwarzania danych osobowych;
10) **Polityka** –Polityka Bezpieczeństwa Informacji.
11) **Przetwarzanie danych osobowych** – jakiekolwiek czynności wykonywane na danych osobowych takie jak zbieranie, utrwalanie, przechowywanie, odczytywanie, zmienianie, udostępnianie, usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
12) **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych. Za system informatyczny nie uważa się aplikacji biurowych (edytor tekstu, arkusz kalkulacyjny, itp.);
13) **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 (ogólne rozporządzenie o ochronie danych) ) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).
14) **Użytkownik** – osoba korzystająca z Systemów Informatycznych w ORE;
15) **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
16) **Zespół Kadr** – Zespół Kadr ORE, który działa w imieniu i z upoważnienia Administratora Danych Osobowych, odpowiedzialny za upoważnienie pracowników i współpracowników ORE do przetwarzania Danych Osobowych, oraz prowadzenie ewidencji osób upoważnionych.

## 3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemów Informatycznych

### 3.1. Rozpoczęcie pracy

Rozpoczęcie pracy w systemach informatycznych wiąże się z wykonaniem przez użytkownika następujących czynności:

1) zalogowanie (uwierzytelnienie) do stacji roboczej przy wykorzystaniu własnego identyfikatora i hasła;
2) uruchomienie systemu informatycznego;
3) zalogowanie do systemu informatycznego przy wykorzystaniu własnego identyfikatora i hasła;
4) podczas rozpoczęcia pracy w systemie informatycznym należy zwrócić uwagę na następujące kwestie:
   a) należy chronić swoje hasło przed ujawnieniem, jeżeli istnieje obawa, że hasło zostało ujawnione należy je niezwłocznie zmienić,
   b) w razie problemów z logowaniem niezwłocznie zgłosić ten fakt ASI.

### 3.2. Tymczasowe zawieszenie pracy

Tymczasowe zawieszenie pracy w systemach informatycznych wiąże się z wykonaniem przez użytkownika następujących czynności:

1) zapisanie wszelkich danych w systemie tak, aby nie uległy one utracie (np. po wyłączeniu komputera);
2) wylogowanie się z systemu informatycznego lub zablokowanie sesji w systemie informatycznym;
3) zablokowanie lub wylogowanie się ze stacji roboczej poprzez naciśnięcie jednocześnie klawiszy CTRL ALT DEL i wybranie opcji **Wyloguj** lub **Zablokuj komputer**;
4) zabezpieczenie wszelkich nośników i wydruków danych znajdujących się w sąsiedztwie stacji roboczej.

### 3.3. Zakończenie pracy

Zakończenie pracy w systemach informatycznych wiąże się z wykonaniem przez użytkownika następujących czynności:

1) zapisanie wszelkich danych w systemie tak, aby nie uległy one utracie;
2) wylogowanie się z systemu informatycznego i zamknięcie systemu;
3) wylogowanie się ze stacji roboczej (poprzez naciśnięcie jednocześnie klawiszy CTRL ALT DEL i wybranie opcji **Wyloguj** lub **Zamknij System**);
4) wyłączenie stacji roboczej (opcja **Zamknij System**);
5) zabezpieczenie wszelkich nośników i wydruków, w razie potrzeby zniszczenie niepotrzebnych dokumentów i nośników w niszczarce.

## 4. Upoważnienie do przetwarzania danych osobowych i nadawania uprawnień w systemie informatycznym

Przed przystąpieniem do przetwarzania danych osobowych użytkownik powinien:

1) upewnić się, że posiada upoważnienie do przetwarzania danych osobowych;
2) korzystać wyłącznie z własnego identyfikatora na stacji roboczej i w systemie informatycznym;
3) w celu uzyskania upoważnienia do przetwarzania danych osobowych należy skontaktować się z Zespołem Kadr lub bezpośrednim przełożonym;
4) w celu uzyskania identyfikatora w systemie informatycznym lub na stacji roboczej należy zwrócić się do przełożonego.

## 5. Zasady stosowania haseł

Hasła stanowią podstawowe zabezpieczenie dostępu do systemów informatycznych, należy stosować się do zasad haseł określonych w Polityce (przytoczone je także poniżej):

1) hasło powinno składać się, z co najmniej 8 znaków;
2) hasło powinno być złożone (trudne do odgadnięcia) i składać się z małych i wielkich liter, cyfr i/lub znaków specjalnych, nie powinno składać się z prostych wyrazów:
   a) większość systemów wymusza reguły haseł tak, że hasło, które nie zawiera w/w rodzajów znaków nie zostanie zaakceptowane przez system, w razie problemów przy zmianie hasła należy upewnić się, że spełnia ono w/w kryteria;
3) hasło powinno być zmieniane raz na 30 dni i różnić się od 5 poprzednich haseł:
   a) większość systemów wymusza zmianę hasła, po 30 dniach uniemożliwia korzystanie z dotychczasowego hasła, w razie problemów przy zmianie hasła należy upewnić się, że różni się ono od 5 poprzednich haseł;
4) konto użytkownika jest blokowane po 5-krotnej niepoprawnej próbie uzyskania dostępu, wtedy nie ma możliwości dostania się do systemu – należy skontaktować się z ASI, który odblokuje konto i/lub ustawi nowe hasło początkowe;
5) pod żadnym pozorem hasło nie może być komukolwiek przekazywane czy ujawniane;
6) zabrania się zapisywania haseł, lub takiego z nimi postępowania, które umożliwia lub ułatwia dostęp do haseł osobom trzecim;
7) jeżeli zachodzi podejrzenie, że hasło zostało ujawnione innej osobie, konieczna jest jego natychmiastowa zmiana;
8) po założeniu identyfikatora w systemie informatycznym użytkownikowi przydzielane jest początkowe hasło, które powinno być zmienione przez użytkownika natychmiast po jego wykorzystaniu, hasło należy też niezwłocznie zmienić po ustawieniu hasła przez administratora;
9) wszelkie problemy związane z hasłami należy zgłaszać do ASI.

## 6. Korzystanie z systemów informatycznych

1) systemy informatyczne mogą być wykorzystywane wyłącznie do celów służbowych, nie wolno korzystać z systemów informatycznych i stacji roboczych w celach prywatnych, w szczególności w celu osiągnięcia korzyści materialnych, niezwiązanych z wykonywaniem obowiązków dla ORE;
2) wszelkie dane utworzone, przechowywane lub przetwarzane w systemach informatycznych lub komputerach ORE traktowane są, jako własność ORE, zabronione jest przechowywanie lub przetwarzanie danych prywatnych;
3) treści niezwiązane z pracą na rzecz ORE (dane prywatne, itp.) powinny być natychmiast usuwane z systemów i komputerów ORE;
4) ORE zastrzega sobie prawo do dostępu do wszelkich informacji przetwarzanych w systemach informatycznych i komputerach oraz monitorowania działań użytkowników, bez uprzedzenia ani podania przyczyn;
5) należy monitorować komunikaty systemów wyświetlanych na ekranie, w szczególności komunikaty systemu antywirusowego, w razie informacji o nieprawidłowościach należy zgłosić ten fakt ASI;
6) oprogramowanie jest instalowane wyłącznie przez ASI, samodzielna instalacja oprogramowania, zmiana konfiguracji systemów i stacji roboczych jest zabroniona. W celu instalacji oprogramowania lub zmiany konfiguracji należy zgłosić się do ASI;
7) oprogramowanie i inne treści (muzyka, książki, itp.) podlegają ochronie prawnej, należy przestrzegać praw autorskich wobec tego rodzaju treści, w przypadku wątpliwości należy skontaktować się z przełożonym;
8) wszelkie istotne dane powinny znajdować się na dyskach sieciowych na serwerze, w celu ich ochrony przed utratą w przypadku awarii stacji. W celu uzyskania uprawnień do dysków sieciowych należy zgłosić się do przełożonego;

9) w uzasadnionych przypadkach, gdy istotne dane trzymane są lokalnie na stacjach roboczych należy tworzyć ich kopie zapasowe. Zabronione jest samodzielne tworzenie kopii zapasowych, są one robione przez ASI na wniosek użytkownika. Kopie zapasowe nie mogą być wynoszone poza siedzibę ORE bez zgody IOD.

10) W pracy z dokumentami elektronicznymi, przechowywanymi na dysku twardym lokalnej stacji roboczej a zawierającymi robocze kopie danych osobowych, przetwarzanych w systemach informatycznych ORE, obowiązują wymienione niżej zasady.

   a) dokumenty przechowywane są na dysku wyłącznie w formie zaszyfrowanej przy pomocy oprogramowania do kompresji danych (7zip) a dostęp do nich zabezpieczony jest hasłem ustalonym zgodnie z zasadami określonymi w rozdziale 5 niniejszej Instrukcji;

   b) nazwa pliku powinna jednoznacznie wskazywać na jego zawartość oraz zawierać słowa „dane osobowe";

   c) pliki zawierające dane osobowe oraz załączniki przeznaczone do korespondencji elektronicznej, należy przechowywać w odrębnych, wyraźnie oznaczonych folderach;

   d) robocze kopie danych osobowych należy bezzwłocznie usuwać z lokalnego dysku twardego, po zakończeniu realizacji zadań dla których zostały utworzone.

## 7. Korzystanie z nośników i urządzeń przenośnych (dyski zewnętrzne, pamięci flash, pendrive)

1) zapis danych należących do ORE na nośnikach przenośnych jest dopuszczalny tylko przy użyciu autoryzowanych przez ASI nośników należących do ORE;

2) nie należy korzystać na komputerach ORE z nośników prywatnych lub pochodzących z nieznanego źródła;

3) na stacjach roboczych wyłączona jest możliwość wykorzystywania nośników, które nie zostały dopuszczone do użytkowania przez ASI za wyjątkiem stacji roboczych w Kancelarii oraz Archiwum Zakładowym

4) niewykorzystywane i zużyte nośniki optyczne i magnetyczne (CD\DVD, dyskietki) należy niszczyć w niszczarkach lub zwracać ASI, niesprawne nośniki Flash i przenośne dyski należy bezwzględnie zwracać ASI w celu ich utylizacji;

5) przy wynoszeniu nośników i laptopów poza siedzibę należy zachować szczególną ostrożność tak, aby zapobiec zgubieniu lub kradzieży nośnika;

6) nie należy wysyłać nośników zawierających dane inne niż publicznie dostępne, tradycyjną pocztą czy kurierem, o ile to możliwe należy takie nośniki szyfrować – w tym celu należy skontaktować się z ASI.

## 8. Poczta elektroniczna i Internet

1) zarówno pocztę elektroniczną, jak i dostęp do Internetu należy wykorzystywać wyłącznie w celach służbowych;

2) W szczególności zabronione jest:

   a) przesyłanie ogłoszeń i innej niechcianej poczty elektronicznej (SPAMu, łańcuszków, muzyki, filmów, itp.),

   b) przesyłanie treści nieprzyzwoitych, niecenzuralnych, obscenicznych, itp.,

   c) odwiedzanie stron o treściach nieprzyzwoitych, niecenzuralnych, obscenicznych, itp.,

   d) słuchanie radia, muzyki, oglądanie filmów i innych treści multimedialnych chyba, że jest to niezbędne do realizacji obowiązków,

   e) pobieranie oprogramowania, plików multimedialnych i innych utworów z Internetu;

3) należy podchodzić z ostrożnością do poczty od nieznanych nadawców, treść lub załączniki mogą zawierać wirusy;

4) w przypadku wprowadzania hasła lub poufnych danych do aplikacji internetowych należy upewnić się, że zapewniają one ochronę danych poprzez szyfrowanie sesji. W tym celu należy zidentyfikować symbol kłódki i klikając na niego uzyskać informacje o certyfikatach. Certyfikaty powinny być wystawione przez zaufanego dostawcę;

5) brak szyfrowania sesji lub problemy z certyfikatami stanowią zagrożenie dla poufności haseł i danych, przed wprowadzeniem jakichkolwiek danych należy skonsultować się z ASI.

## 9. Naruszenie bezpieczeństwa przetwarzania danych

1) Każdy pracownik, stażysta, wolontariusz, praktykant oraz osoba realizująca zadania na podstawie umowy cywilnoprawnej, który stwierdził lub podejrzewa wystąpienie zdarzenia, stanowiącego i naruszenie ochrony danych osobowych, ma obowiązek zgłoszenia tego faktu na piśmie **bezpośredniemu przełożonemu** oraz **IOD** na adres **iod@ore.edu.pl.** W przypadku gdy zgłoszenie dotyczy systemów informatycznych, stosowną informację należy przekazać również do **ASI**, na adres **zespol.informatykow@ore.edu.**

2) Zgłoszenie zdarzenia mogącego być naruszeniem ochrony danych osobowych powinno zawierać:
   a) opisanie symptomów naruszenia ochrony danych osobowych;
   b) określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych;
   c) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia, jak ilość danych, zakres danych, kategorie danych osobowych, itp.;
   d) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzeń.

3) Szczegółowa procedura postępowania z Incydentami zawarta jest w **Załączniku nr 3** do Polityki bezpieczeństwa Informacji

Załącznik nr 3 do Polityki Bezpieczeństwa Informacji

# PROCEDURA POSTĘPOWANIA W PRZYPADKU NARUSZEŃ BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

## Ośrodek Rozwoju Edukacji

**PROCEDURA POSTĘPOWANIA W PRZYPADKU NARUSZEŃ BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH**

**w Ośrodku Rozwoju Edukacji w Warszawie**

## CEL PROCEDURY

Określenie i wdrożenie w Ośrodku Rozwoju Edukacji w Warszawie jednolitej i przejrzystej procedury postępowania w przypadku naruszenia ochrony danych osobowych.

## ODPOWIEDZIALNI ZA WYKONANIE PROCEDURY

1. **Inspektor Ochrony Danych (IOD)** jest odpowiedzialny w zakresie:
   1) oceny czy zgłoszenie stanowi naruszenie ochrony danych osobowych:
      a) jeżeli tak - czy może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych i w związku z tym wymaga zgłoszenia organowi nadzorczemu,
      b) czy zidentyfikowane naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, co wiąże się z obowiązkiem zawiadomienia osób, których dane dotyczą;
   2) dokumentowania spraw z zakresu naruszeń;
   3) dokonanie oceny ryzyka naruszenia;
   4) przygotowanie treści zgłoszenia naruszenia do organu nadzorczego, jeżeli konieczność zgłoszenia wynika z oceny ryzyka naruszenia;
   5) przygotowanie treści zawiadomienia osób, których naruszenie dotyczy, jeżeli konieczność ich zawiadomienie wynika z oceny ryzyka naruszenia;
   6) pełnienie funkcji punktu kontaktowego dla osób, których dotyczy naruszenie.
2. **Administrator** danych jest odpowiedzialny za:
   1) zgłaszanie naruszeń w imieniu do organu nadzorczego (Prezes Urzędu Ochrony Danych Osobowych);
   2) informowanie osób, których dane dotyczą o wystąpieniu naruszenia;
   3) zatwierdzanie i nakazywanie działań minimalizujących ryzyko naruszenia oraz ryzyko jego ponownego wystąpienia w przyszłości.
3. **Administrator systemu informatycznego** (ASI) - w sytuacji, gdy naruszenie dotyczy systemów informatycznych jest odpowiedzialny za:
   1) ustalenie przyczyny naruszenia i przekazanie raportu do **IOD** oraz najwyższego kierownictwa;
   2) współdziałanie z **IOD**;
   3) podejmowanie działań minimalizujących ryzyko naruszenia;
   4) rekomendowanie działań zwiększających bezpieczeństwo systemów informatycznych.
4. **Osoby upoważnione do przetwarzania danych** są odpowiedzialne za zgłaszanie podejrzenia naruszenia lub naruszenia danych osobowych do **IOD**.

## POSTANOWIENIA OGÓLNE PROCEDURY

Procedura dotycząca postępowania w przypadku naruszeń ochrony danych osobowych realizowana jest w dwóch etapach:

1) wewnętrznym, którego celem jest ustalenie, czy zgłoszone zdarzenie jest naruszeniem oraz w jaki sposób zidentyfikowane zdarzenie wpłynie na ryzyko dla praw i wolności osób fizycznych;
2) zewnętrznym, którego celem jest zgłoszenie naruszenia ochrony danych osobowych do organu nadzorczego oraz poinformowanie osoby, której dane dotyczą, w przypadku, gdy istnieje wysokie ryzyko dla praw i wolności osób fizycznych.

## POSTANOWIENIA SZCZEGÓŁOWE PROCEDURY

### ROZDZIAŁ I - ETAP WEWNĘTRZNY

1. Każdy pracownik, stażysta, wolontariusz, praktykant oraz osoba realizująca zadania na podstawie umowy cywilnoprawnej, który stwierdził lub podejrzewa wystąpienie zdarzenia, stanowiącego i naruszenie ochrony danych osobowych, ma obowiązek zgłoszenia tego faktu na piśmie **bezpośredniemu przełożonemu** oraz **IOD** na adres **iod@ore.edu.pl** W przypadku gdy zgłoszenie dotyczy systemów informatycznych stosowną informację należy przekazać również do **ASI**, na adres **zespol.informatykow@ore.edu.**
2. Zgłoszenie zdarzenia mogącego być naruszeniem ochrony danych osobowych powinno zawierać:
   1) opisanie symptomów naruszenia ochrony danych osobowych;
   2) określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych;
   3) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia, jak ilość danych, zakres danych, kategorie danych osobowych, itp.;
   4) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzeń.
3. Stwierdzenie naruszenia następuje w momencie, gdy Administrator ma wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu, prowadzące do naruszenia bezpieczeństwa danych osobowych. W dokonaniu oceny ryzyka naruszenia pomaga **IOD**.
4. Jeżeli naruszenie ochrony danych osobowych dotyczy systemu informatycznego, **ASI** w porozumieniu z **IOD** podejmuje niezbędne działania mające na celu ograniczenie skutków naruszenia.
5. Jeżeli naruszenie ochrony danych nie dotyczy systemu informatycznego i ma związek z naruszeniem zabezpieczeń fizycznych, odpowiednie czynności zabezpieczające podejmuje **IOD**, tj.:
   1) jeśli to konieczne, nakazuje przerwanie pracy, zwłaszcza w zakresie przetwarzania danych osobowych, do czasu podjęcia decyzji o dalszym postępowaniu przez najwyższe kierownictwo **Administratora**;
   2) działa w celu wyjaśnienia okoliczności zdarzenia;
   3) przedstawia zalecenia mające na celu minimalizację skutków naruszenia i umożliwienie dalszego bezpiecznego przetwarzania danych.
   4) odnotowuje informacje dotyczące zdarzenia w Rejestrze naruszeń i incydentów;
6. Odmowa udzielenia wyjaśnień lub współpracy z **IOD** traktowana będzie jako naruszenie obowiązków pracowniczych.

7. Raport o naruszeniu danych osobowych opracowuje **IOD** według wzoru stanowiącego część niniejszej procedury.
8. **IOD** przekazuje **Administratorowi** danych raport, na którego podstawie jest podejmowana decyzja o dalszym postępowaniu.
9. Decyzja **Administratora** jest odnotowywana na raporcie, który po podpisaniu przez kierownictwo jest zwracany do **IOD**, w celu archiwizacji.

## ROZDZIAŁ II - ETAP ZEWNĘTRZNY

1. W przypadku, gdy naruszenie ochrony danych osobowych może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, musi być ono zgłoszone organowi nadzorczemu (PUODO) bez zbędnej zwłoki, ale nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.
2. Treść zgłoszenia przygotowuje **IOD**, zgodnie ze wzorem udostępnionym przez organ nadzorczy. W zgłoszeniu zamieszcza się w szczególności:
   1) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazuje się kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   2) imię i nazwisko oraz dane kontaktowe **IOD**;
   3) możliwe konsekwencje dla osoby, której dane dotyczą, naruszenia ochrony jej danych osobowych;
   4) środki zastosowane lub proponowane w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. Jeżeli informacji, o których mowa w ust. 2, nie da się udzielić w tym samym czasie, można ich udzielać sukcesywnie, bez zbędnej zwłoki, w następujący sposób:
   1) po dokonaniu pierwszego zgłoszenia (zgłoszenie wstępne) można przekazywać na bieżąco organowi nadzorczemu aktualne informacje;
   2) w przypadku uzyskania w toku dochodzenia dowodów na to, że opanowano zdarzenie, a w rzeczywistości żadne naruszenie nie miało miejsca, informację tę można dodać do informacji już przekazanych do organu nadzorczego, a następnie zarejestrować zaistniałe zdarzenie jako niestanowiące naruszenia ochrony danych osobowych.
4. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
5. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, bez zbędnej zwłoki zawiadamia się o tym osoby, których dane dotyczą.
6. Treść zawiadomienia przygotowuje **IOD**, za przekazanie zawiadomienia osobom, których dane dotyczą odpowiada **Administrator**.
7. Zawiadomienie o którym mowa w pkt. 5 powinno być napisane jasnym i prostym językiem oraz zawierać opis charakteru naruszenia ochrony danych osobowych, informacje o potencjalnych zagrożeniach z nim związanych i możliwych do podjęcia środkach zaradczych a także dane kontaktowe **IOD**.
8. Zawiadomienie, o którym mowa w ust. 5, nie jest wymagane w następujących przypadkach:
   1) wdrożono 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;

2) zastosowano następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
3) 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 skuteczny sposób.

9. Należy wykazać przed organem nadzorczym, że został spełniony przynajmniej jeden z warunków wskazanych w ust. 8 w przypadku braku powiadomienia osób, których dane naruszono.

..... dnia .....

Załączniki:

Załącznik nr 1: Wzór raportu o naruszeniu bezpieczeństwa danych osobowych

**Raport o naruszeniu bezpieczeństwa danych osobowych nr...../...r**

**Sporządzający raport:**

Imię i nazwisko .....

Stanowisko .....

1) miejsce, dokładny czas i data naruszenia bezpieczeństwa informacji w tym ochrony danych osobowych (piętro, nr pokoju, godzina itp.):
   .....
2) osoby powodujące naruszenie (które swoim działaniem lub zaniechaniem przyczyniły się do naruszenia bezpieczeństwa informacji w tym ochrony danych osobowych):
   .....
3) charakter naruszenia (tj. nieuprawnione lub przypadkowe ujawnienie lub udostępnienie danych, wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania, brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną):
   .....
4) informacje o danych, które zostały lub mogły zostać ujawnione:
   .....
5) zabezpieczone materiały lub inne dowody związane z wydarzeniem:
   .....
6) kategorie danych, których dotyczy naruszenie:
   .....
7) kategorie osób, których dotyczy naruszenie:
   .....
8) środki bezpieczeństwa zastosowane przed naruszeniem:
   .....
9) krótki opis wydarzenia związanego z naruszeniem bezpieczeństwa informacji, w tym ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania):
   .....
10) Rekomendacje w celu minimalizacji ryzyka naruszenia oraz uniknięcia jego powtórzenia w przyszłości:
    .....
    .....
11) Ocena ryzyka naruszenia
    .....
    .....

Data: .....  Podpis: .....

Decyzja Administratora w zakresie:

1. Rekomendacji: .....
2. Zgłoszenia do organu nadzorczego: .....
3. Zawiadomienia osób, których dotyczy naruszenie: .....
   .....

ORE Ośrodek Rozwoju Edukacji

# Załącznik nr 4 do Polityki Bezpieczeństwa Informacji

# Wzór wniosku o nadanie lub odebranie upoważnienia do przetwarzania danych osobowych oraz uprawnień w systemach informatycznych

## Wniosek o nadanie/odebranie upoważnienia i uprawnień w systemach informatycznych

| WNIOSKUJĄCY | | | |
|---|---|---|---|
| Imię | | Nazwisko | |
| Stanowisko | | | |
| **Zależność służbowa wobec osoby dla której przydzielone/odebrane zostaną uprawnienia** | | | |
| Bezpośredni przełożony | ☐ | | |
| Dyrektor ORE | ☐ | | |
| Inne (wymagany opis) | ☐ | | |

| UŻYTKOWNIK | | | |
|---|---|---|---|
| Imię | | Nazwisko | |
| Pracownik ORE | ☐ | Stanowisko | |
| Podstawa dostępu do systemów ORE (jeżeli dostęp wnioskowany dla osoby nie będącej pracownikiem) | | | |

| NADANIE/ODEBRANIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH | | | |
|---|---|---|---|
| Dostęp do danych osobowych | ☐ | Upoważnienie do przetwarzania danych osobowych | ☐ |
| Nadanie/odebranie uprawnień | | | |
| *Opis uprawnienia/dostęp do jakich danych/ dokładny opis funkcji/ wykonywanych czynności* | | | |
| *Uwagi* | | | |

| NADANIE/ODEBRANIE UPRAWNIEŃ W SYSTEMACH INFORMATYCZNYCH | | | |
|---|---|---|---|
| **Stacja Robocza \ Domena** | | | |
| Posiadany identyfikator | | Założenie nowego identyfikatora | ☐ |
| Dodatkowe uprawnienia np. na serwerze plików, w systemie pocztowym, itp. | | | |
| **Systemy Informatyczne** | | | |
| Nazwa systemu/ów | | | |
| Posiadany Identyfikator/y | | Założenie nowego identyfikatora | ☐ |
| Nadanie/odebranie uprawnień | | | |
| *System/opis uprawnienia* | | | |

| | |
|---|---|
| | |
| Uwagi | |

| REALIZUJĄCY WNIOSEK O NADANIE?ODEBRANIE UPRAWNIEŃ | | | |
|---|---|---|---|
| Imię | | Nazwisko | |
| Uwagi | | | |

| PODPISY | | | |
|---|---|---|---|
| Imię i nazwisko oraz stanowisko wnioskującego o uprawnienia | | Data i podpis wnioskującego o uprawnienia | |
| Imię i nazwisko kierownika Zespołu Kadr | | Data i podpis kierownika Zespołu Kadr | |
| Imię i nazwisko Inspektora Ochrony Danych | | Data i podpis Inspektora Ochrony Danych | |
| Imię i nazwisko Administratora | | Data i podpis Administratora | |


# Załącznik nr 5 do Polityki Bezpieczeństwa Informacji

## Wzory upoważnień do przetwarzania danych osobowych

## Ośrodek Rozwoju Edukacji

Warszawa, dnia ..... r.

..... .ODO.20...

# U P O W A Ż N I E N I E

do przetwarzania danych osobowych

**Upoważniam Pana/Panią:**

**.....**

**do przetwarzania danych osobowych**

w Ośrodku Rozwoju Edukacji w Warszawie, w zakresie niezbędnym do wykonywania zadań w komórce organizacyjnej: ..... **(nazwa komórki)**, zgodnie z powierzonymi obowiązkami pracowniczymi.

Upoważnienie wygasa z chwilą ustania stosunku prawnego łączącego upoważnionego z Ośrodkiem Rozwoju Edukacji w Warszawie.

.....
Czytelny podpis osoby upoważnionej
do wydawania i odwoływania upoważnień.

Upoważnienie otrzymałem/am:

.....

---

Oświadczam, że zapoznałem/am się z przepisami powszechnie obowiązującymi dotyczącymi ochrony danych osobowych, w tym z RODO, a także z obowiązującym w Ośrodku Rozwoju Edukacji opisem technicznych i organizacyjnych środków zapewniających ochronę i bezpieczeństwo przetwarzania danych osobowych i zobowiązuję się do przestrzegania zasad przetwarzania danych osobowych określonych w tych dokumentach.

Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych, z którymi zapoznałem/am się oraz sposobów ich zabezpieczania, zarówno w okresie trwania umowy jak również po ustaniu stosunku prawnego łączącego mnie z Ośrodku Rozwoju Edukacji.

Czytelny podpis osoby składającej oświadczenie

.....

Warszawa, dnia ..... r.

... .ODO.20..

# UPOWAŻNIENIE

do przetwarzania danych osobowych

Z dniem ..... r., na podstawie art. 29 w związku z art. 28 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 Urz. UE. L 119 z 04.05.2016, str.1) (RODO), upoważniam Panią/a ..... do przetwarzania danych osobowych w zbiorze **Program Operacyjny Wiedza Edukacja Rozwój** w zakresie projektu: .....

Upoważnienie wygasa z chwilą ustania stosunku prawnego łączącego upoważnionego z Ośrodkiem Rozwoju Edukacji w Warszawie.

.....
Czytelny podpis osoby upoważnionej
do wydawania i odwoływania upoważnień.

Upoważnienie otrzymałem/am:

.....

---

Oświadczam, że zapoznałem/am się z przepisami powszechnie obowiązującymi dotyczącymi ochrony danych osobowych, w tym z RODO, a także z obowiązującym w Ośrodku Rozwoju Edukacji opisem technicznych i organizacyjnych środków zapewniających ochronę i bezpieczeństwo przetwarzania danych osobowych i zobowiązuję się do przestrzegania zasad przetwarzania danych osobowych określonych w tych dokumentach.

Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych, z którymi zapoznałem/am się oraz sposobów ich zabezpieczania, zarówno w okresie trwania umowy jak również po ustaniu stosunku prawnego łączącego mnie z Ośrodku Rozwoju Edukacji.

.....
Czytelny podpis osoby składającej oświadczenie

Warszawa, dnia ..... r.

..... .ODO.20..

# UPOWAŻNIENIE

do przetwarzania danych osobowych

**Upoważniam Pana/Panią:**

**.....**

**do przetwarzania danych osobowych**

w Ośrodku Rozwoju Edukacji w Warszawie, w zakresie niezbędnym do wykonywania zadań wynikających z udziału w pracach ***Komisji Socjalnej*** zgodnie z powierzonymi obowiązkami pracowniczymi.

Upoważnienie jest ważne do chwili odwołania upoważnionego ze składu Komisji Socjalnej lub ustania stosunku prawnego łączącego upoważnionego z Ośrodkiem Rozwoju Edukacji w Warszawie.

Pieczęć i podpis:

.....

*Czytelny podpis osoby nadającej upoważnienie*

---

Oświadczam, że zapoznałem/am się z przepisami powszechnie obowiązującymi dotyczącymi ochrony danych osobowych, w tym z RODO, a także z obowiązującym w Ośrodku Rozwoju Edukacji opisem technicznych i organizacyjnych środków zapewniających ochronę i bezpieczeństwo przetwarzania danych osobowych i zobowiązuję się do przestrzegania zasad przetwarzania danych osobowych określonych w tych dokumentach.

Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych, z którymi zapoznałem/am się oraz sposobów ich zabezpieczania, zarówno w okresie trwania umowy jak również po ustaniu stosunku prawnego łączącego mnie z Ośrodku Rozwoju Edukacji.

Czytelny podpis osoby składającej oświadczenie

.....

ORE Ośrodek Rozwoju Edukacji

# Załącznik nr 6 do Polityki Bezpieczeństwa Informacji

# Wykaz osób upoważnionych do przetwarzania danych osobowych

## Ośrodek Rozwoju Edukacji

# Wykaz osób upoważnionych do przetwarzania danych osobowych (wzór)

| L.p. | Imię i Nazwisko | Data nadania upoważnienia | Data ustania upoważnienia | Zakres danych | Identyfikatory w Systemach Informatycznych (wypełniane tylko wtedy jeżeli system informatyczny nie pozwala na czytelny wydruk listy identyfikatorów w systemie przypisanych do osób upoważnionych) | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | *System 1* | *System 2* | *System 3* | *System 4* | *System 5* |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

ORE Ośrodek Rozwoju Edukacji

# Załącznik nr 7 do Polityki Bezpieczeństwa Informacji

# Arkusz informacji o udostępnieniu danych osobowych

# Arkusz informacji o udostępnieniu danych osobowych (wzór)

| L.p. | Dane odbiorcy | Nazwa zbioru z którego udostępniono dane osobowe | Data udostępnienia | Imię i nazwisko osoby, której dane dotyczą | Identyfikator pozwalający na wyszukanie rekordu Danych Osobowych w zbiorze (dla zbiorów w formie elektronicznej) | Zakres udostępnionych danych osobowych | Nr wniosku o udostępnienie danych osobowych |
|---|---|---|---|---|---|---|---|
| 1 | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Ośrodek Rozwoju Edukacji

# Załącznik nr 8 do Polityki Bezpieczeństwa Informacji

# Oświadczenie o zachowaniu poufności danych osobowych

## Ośrodek Rozwoju Edukacji

Warszawa, .....

imię: _____
nazwisko: _____
stanowisko: _____
wydział: _____

**OŚWIADCZENIE**

o obowiązku zachowania poufności danych osobowych w

**OŚRODKU ROZWOJU EDUKACJI W WARSZAWIE**

(dalej „administrator danych")

**TREŚĆ OŚWIADCZENIA**

W związku z dopuszczeniem do przetwarzania danych osobowych oświadczam, że:

1. Zapoznałem się i zobowiązuję się do przestrzegania obowiązków wynikających z:
   a) przepisów ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) oraz aktów wykonawczych wydanych na jej podstawie;
   b) 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. z 2016 r. Nr 119).
   c) regulacji wewnętrznych administratora danych obowiązujących w obszarze przetwarzania danych osobowych.
2. Zapewnię bezpieczeństwo przetwarzanych danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją i zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem.
3. Zachowam w tajemnicy dane osobowe oraz sposoby ich zabezpieczeń, do których uzyskam dostęp w trakcie współpracy z administratorem danych jak i po jej zakończeniu.
4. W razie uzyskania dostępu do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych zobowiązuję się zachować jej treść w tajemnicy w trakcie współpracy z administratorem danych jak i po jej zakończeniu.
5. Będę wykonywać polecenia w formie pisemnej Inspektora Ochrony Danych lub administratora danych odpowiedzialnych za bezpieczeństwo danych osobowych, które będą związane z zachowaniem bezpieczeństwa danych osobowych i sposobów ich zabezpieczenia.
6. W razie uzyskania nieuprawnionego dostępu do danych osobowych lub wykrycia incydentu godzącego w bezpieczeństwo danych osobowych, zobowiązuję się powiadomić o tym Inspektora Ochrony Danych, odpowiedzialnego za bezpieczeństwo danych osobowych.
7. Znane mi są zasady monitorowania sposobu używania sprzętu służbowego w szczególności (telefonów komórkowych, komputerów, poczty elektronicznej, itp.) obowiązujące u administratora danych. Zostałem poinformowany o zakresie i sposobach prowadzenia ww. monitorowania.
8. Znane mi są zasady odpowiedzialności prawnej za niezgodne z ustawą o ochronie danych osobowych przetwarzanie danych osobowych oraz mam świadomość, że za niedopełnienie obowiązków wynikających z niniejszego oświadczenia mogę odpowiadać prawnie na podstawie regulacji wewnętrznych obowiązujących u administratora danych, kodeksu pracy, kodeksu cywilnego oraz ustawy o ochronie danych osobowych.

Oświadczam, że treść niniejszego oświadczenia jest mi znana i jest dla mnie w pełni zrozumiała i zobowiązuję się do jej przestrzegania.

Potwierdzam odbiór 1 egz. niniejszego oświadczenia.

.....

data i podpis pracownika

ORE Ośrodek Rozwoju Edukacji

## Załącznik nr 9 do Polityki Bezpieczeństwa Informacji

# Oświadczenie o wyrażeniu zgody na używanie prywatnego sprzętu do celów służbowych oraz o obowiązku zachowania poufności danych osobowych w Ośrodku Rozwoju Edukacji w Warszawie

## Ośrodek Rozwoju Edukacji

Warszawa, .....

Imię: _____

Nazwisko: _____

Stanowisko _____

Wydział: _____

# OŚWIADCZENIE

o wyrażeniu zgody na używanie prywatnego sprzętu teleinformatycznego do celów służbowych oraz o obowiązku zachowania poufności danych osobowych w Ośrodku Rozwoju Edukacji w Warszawie

*Ja niżej podpisana(y), oświadczam, że zapoznałem się z przepisami dotyczącymi przetwarzania i ochrony danych osobowych i zobowiązuję się do przestrzegania:*

a) *przepisów ustawy z dnia 10 maja 2018 r o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781) oraz aktów wykonawczych wydanych na jej podstawie;*
b) *przepisów ogólnego 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;*
c) *regulacji wewnętrznych Dyrektora Ośrodka Rozwoju Edukacji w Warszawie (zwanym dalej "Administratorem danych" obowiązującym zarówno w obszarze przetwarzania danych osobowych w Ośrodku Rozwoju Edukacji w Warszawie jak i poza tym obszarem.*

Jednocześnie oświadczam, że:

1. Zachowam w poufności wszelkie informacje dotyczące bezpieczeństwa danych osobowych oraz sposobów ich zabezpieczenia, które przetwarzałam(em), przetwarzam lub będę przetwarzać w ramach wykonywanych obowiązków oraz metody ich zabezpieczeń, także po ustaniu wykonywania obowiązku lub świadczenia pracy;
2. Wyrażam zgodę na wykonywanie pracy zdalnej na swoim własnym sprzęcie teleinformatycznym (komputer, laptop, drukarka, telefon, itp.)
3. Dostosuję stacje roboczą w postaci swojego prywatnego komputera (laptopa), na którym będę pracował do minimalnych wymagań wynikających z Polityki Bezpieczeństwa Informacji;
4. Wyrażam zgodę, w uzasadnionych przypadkach, umożliwić administratorowi danych przeprowadzenie kontroli procesu przetwarzania i ochrony danych;
5. Będę wykonywać polecenia przedstawicieli administratora danych odpowiedzialnych za bezpieczeństwo danych osobowych, które będą związane z zachowaniem bezpieczeństwa danych osobowych;
6. Zapewnię bezpieczeństwo i ochronę przetwarzanym danym osobowym a w szczególności zabezpieczę je przed dostępem osób nieupoważnionych, kradzieżą, uszkodzeniem oraz nieuprawnioną modyfikacją lub zniszczeniem;
7. Niezwłocznie zgłoszę Inspektorowi Ochrony Danych w Ośrodku Rozwoju Edukacji w Warszawie na adres email: iod@ore.edu.pl, stwierdzenie próby lub faktu naruszenia ochrony danych osobowych oraz zagrożenia ich bezpieczeństwa.

Potwierdzam odbiór 1 egz. Niniejszego oświadczenia.

Warszawa, .....

.....

(podpis)

ORE Ośrodek Rozwoju Edukacji

# Załącznik nr 10 do Polityki Bezpieczeństwa Informacji

# Spis systemów teleinformatycznych ORE

**Spis systemów teleinformatycznych**

**za rok .....**

**Ośrodek Rozwoju Edukacji w Warszawie**

| L. p. | Nazwa aktywu | Typ aktywu | Lokalizacja | Właściciel aktywu | Użytkownicy aktywu | Wymogi poufności, integralności i dostępności | | | Ważność aktywu | Kategoria informacji |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | P | D | I | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | | | 8 | 9 |
| 1 | | | | | | | | | | |
| 2 | | | | | | | | | | |
| 3 | | | | | | | | | | |

**Legenda:**

**Kolumna 2** 'Nazwa aktywu' - nazwa aktywów zidentyfikowanych w komórce organizacyjnej

**Kolumna 3** 'Typ aktywu' - należy zakwalifikować dane aktywa do jednego z poniższych typów:

Aktywa główne:

1. Procesy wytwarzania, przetwarzania, przesyłania i przechowywania informacji
2. Informacje.

Aktywa wspomagające:

1. Sprzęt;
2. Oprogramowanie;
3. Sieć;
4. Personel;
5. Siedziba;
6. Struktura organizacyjna.

**Kolumna 4** 'Lokalizacja' - miejsce przechowywania aktywów; należy określić, gdzie aktywa są przechowywane; w przypadku aktywów materialnych: budynek/pomieszczenie, w przypadku aktywów niematerialnych: miejsce udostępnienia, wytworzenia, przechowywania, miejsce ich nośnika tj. serwera, płyty CD, itp.; w przypadku aktywu lub zasobu rozproszonego, należy wymienić wszystkie lokalizacje kluczowych elementów zasobu; w przypadku braku możliwości określenia lokalizacji, np. ludzie, wartości niematerialne, sprzęt mobilny kolumny się nie wypełnia.

**Kolumna 5** 'Właściciel aktywu' - przełożony komórki organizacyjnej, w której gromadzi się i przechowuje dane aktywo/zasób; osoba odpowiedzialna za bezpieczeństwo aktywa, jego prawidłowe wykorzystanie

**Kolumna 6** 'Użytkownicy aktywu' - komórki organizacyjne wykorzystujące aktywo do wykonywania obowiązków służbowych

**Kolumna 7** 'Wymogi poufności, integralności i dostępności' - określenie wrażliwości aktywu na utratę jednego z trzech atrybutów bezpieczeństwa; ocena w skali 1-3

**Kolumna 8** 'Ważność aktywu' - ogólna ocena ważności aktywu: P+D+I; wartości: 3-9

**Kolumna 9** 'Kategoria informacji' - Ogólnodostępne/Wewnętrzne/Chronione

Ośrodek Rozwoju Edukacji

# Załącznik nr 11 do Polityki Bezpieczeństwa Informacji

# Wzór Rejestru czynności przetwarzania danych osobowych

## Ośrodek Rozwoju Edukacji

# Rejestr czynności przetwarzania

| Nazwa i dane kontaktowe administratora | |
|---|---|
| **Nazwa** | Ośrodek Rozwoju Edukacji |
| **Adres** | Al. Ujazdowskie28, 00-478 Warszawa |
| **Email** | sekretariat@ore.edu.pl |
| **Telefon** | 22 345 37 00 |

| Inspektor Ochrony Danych | |
|---|---|
| **Nazwa** | Jacek Kaczyński |
| **Adres** | Al. Ujazdowskie28, 00-478 Warszawa, |
| **Email** | iod@ore.edu.pl |
| **Telefon** | 22 345 37 00 |

| Przedstawiciel (jeśli wyznaczono) | |
|---|---|
| **Nazwa** | nie dotyczy |
| **Adres** | nie dotyczy |
| **Email** | nie dotyczy |
| **Telefon** | nie dotyczy |

*Kolorem niebieskim oznaczono informacje wymagane w rejestrze przez art. 30 i art.. 32 RODO

| LP. | Nazwa czynności przetwarzania | Jednostka organizacyjna (departament, dział itp.) | Cel przetwarzania | Kategorie osób | Kategorie danych | Planowany termin usunięcia kategorii danych *(jeżeli jest to możliwe)* | Nazwa współadministratora i dane kontaktowe *(jeśli dotyczy)* | Nazwa podmiotu przetwarzającego i dane kontakowe *(jeśli dotyczy)* | Kategorie odbiorców *(innych niż podmiot przetwarzający)* | Ogólny opis technicznych i organizacyjnych srodków bezpieczeństwa zgodnie z art. 32 ust. 1 *(jeżeli jest to możliwe)* | Transfer do kraju trzeciego lub org. międzynarodowej | | Podstawa prawna | Dodatkowe dane do rejestru czynności w przypadku przetwarzania danych przez procesora | | | Uwagi |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu) | Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń | | Dane procesora | Dane Administratora Danych Osobowych | Formy przetwarzania (przechowywanie, modyfikowania, usuwanie) | |
| | | | Art. 30 ust. 1 pkt b | Art. 30 ust. 1 pkt c | Art. 30 ust. 1 pkt c | Art. 30 ust. 1 pkt f | Art. 30 ust. 1 pkt a | Art. 30 ust. 1 pkt d | Art. 30 ust. 1 pkt d | Art. 30 ust. 1 pkt g | Art. 30 ust. 1 pkt e | Art. 30 ust. 1 pkt e | | | | | |
| 1 | | | | | | | | | | | | | | | | | |
| 2 | | | | | | | | | | | | | | | | | |

ORE Ośrodek Rozwoju Edukacji

# Załącznik nr 12 do Polityki Bezpieczeństwa Informacji

## Wzór klauzuli informacyjnej i zgody na przetwarzanie danych osobowych

ORE Ośrodek Rozwoju Edukacji
Aleje Ujazdowskie 28
00-478 Warszawa
tel. 22 345 37 00
fax 22 345 37 70
www.ore.edu.pl

## 1. Zgoda na przetwarzanie danych osobowych

Wyrażam zgodę na przetwarzanie przez Ośrodek Rozwoju Edukacji (ORE) z siedzibą przy ul. Aleje Ujazdowskie 28,00-478 Warszawa, moich danych osobowych w zakresie ..... podanych w związku z .....

.....
Podpis osoby, której dane dotyczą
(imię i nazwisko)

**INFORMACJA O PRZETWARZANIU DANYCH OSOBOWYCH:**

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016 r.), dalej „RODO", Ośrodek Rozwoju Edukacji w Warszawie informuje, że:

1. Administratorem Pani/Pana danych osobowych jest Ośrodek Rozwoju Edukacji z siedzibą w Warszawie (00-478), Aleje Ujazdowskie 28, e-mail: sekretariat@ore.edu.pl, tel. 22 345 37 00;
2. W sprawach dotyczących przetwarzania danych osobowych można się skontaktować z Inspektorem Ochrony Danych poprzez e-mail: iod@ore.edu.pl;
3. Pani/Pana dane osobowe będą przetwarzane przez Ośrodek Rozwoju Edukacji w Warszawie na podstawie wyrażonej przez Panią/Pana zgody w celu.....;
4. Odbiorcami Pani/Pana danych osobowych mogą być podmioty uprawnione do ich otrzymania na podstawie przepisów prawa, podmioty świadczące usługi na rzecz Administratora, na podstawie zawartych z nim umów oraz .....;
5. Pani/Pana dane osobowe będą przechowywane, przez okres niezbędny do realizacji celów określonych w pkt 3, a po tym czasie przez okres, oraz w zakresie wymaganym przez przepisy powszechnie obowiązującego prawa;
6. Pani/Pana dane osobowe nie będą podlegały zautomatyzowanemu podejmowaniu decyzji w tym również profilowaniu;
7. Dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej;
8. Podanie dotyczących Pani/Pana danych osobowych oraz wyrażenie zgody jest dobrowolne ale jest warunkiem niezbędnym do realizacji celu przetwarzania określonego w pkt. 3. Zgoda może zostać cofnięta w każdej chwili bez podawania przyczyny lecz bez wpływu na zgodność z prawem przetwarzania do którego doszło przed jej cofnięciem;
9. W związku z przetwarzaniem Pani/Pana danych osobowych, przysługują Pani/Panu następujące uprawnienia: prawo dostępu do swoich danych osobowych, prawo żądania ich sprostowania, prawo żądania od administratora ograniczenia przetwarzania lub ich usunięcia, prawo do cofnięcia wyrażonej zgody, z tym, że oraz prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

ORE Ośrodek Rozwoju Edukacji
Aleje Ujazdowskie 28
00-478 Warszawa
tel. 22 345 37 00
fax 22 345 37 70
www.ore.edu.pl

## 2. Zgoda na przetwarzanie danych osobowych wraz z dodatkową klauzulą zgody na publikację danych w sieci Internet

Wyrażam zgodę na przetwarzanie i publikację przez Ośrodek Rozwoju Edukacji (ORE) z siedzibą przy ul. Aleje Ujazdowskie 28,00-478 Warszawa, moich danych osobowych w zakresie ..... podanych w związku z .....

.....
Podpis osoby, której dane dotyczą
(imię i nazwisko)

.....
Podpis osoby której dane dotyczą

Wyrażam zgodę na umieszczenie moich danych osobowych w zakresie: ..... w internetowej bazie danych .....(opcjonalnie nazwa bazy), prowadzonej przez Ośrodek Rozwoju Edukacji (ORE) z siedzibą w Warszawie (00-478), Aleje Ujazdowskie 28. Dane umieszone w bazie danych są publicznie dostępne na stronach internetowych.

Zgoda na umieszczenie danych osobowych w internetowej bazie danych jest dobrowolna. Przysługuje Pani/Panu prawo do dostępu i poprawiania swoich danych, a także wycofania niniejszej zgody.

.....
Podpis osoby której dane dotyczą

**INFORMACJA O PRZETWARZANIU DANYCH OSOBOWYCH:**

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016 r.), dalej „RODO", Ośrodek Rozwoju Edukacji w Warszawie informuje, że:

1. Administratorem Pani/Pana danych osobowych jest Ośrodek Rozwoju Edukacji z siedzibą w Warszawie (00-478), Aleje Ujazdowskie 28, e-mail: sekretariat@ore.edu.pl, tel. 22 345 37 00;
2. W sprawach dotyczących przetwarzania danych osobowych można się skontaktować z Inspektorem Ochrony Danych poprzez e-mail: iod@ore.edu.pl;
3. Pani/Pana dane osobowe będą przetwarzane przez Ośrodek Rozwoju Edukacji w Warszawie na podstawie wyrażonej przez Panią/Pana zgody w celu udostępnienia ich ..... (np. na stronie internetowej www.ore.edu.pl);
4. Odbiorcami Pani/Pana danych osobowych mogą być osoby odwiedzające stronę internetową Ośrodka Rozwoju Edukacji, odbiorcy uprawnieni do ich otrzymania na podstawie przepisów prawa, oraz podmioty świadczące usługi na rzecz Administratora, na podstawie zawartych z nim umów;
5. Pani/Pana dane osobowe będą przechowywane, przez okres niezbędny do realizacji celów określonych w pkt 3, a po tym czasie przez okres, oraz w zakresie wymaganym przez przepisy powszechnie obowiązującego prawa;
6. Pani/Pana dane osobowe nie będą podlegały zautomatyzowanemu podejmowaniu decyzji w tym również profilowaniu;
7. Dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej;
8. Podanie dotyczących Pani/Pana danych osobowych oraz wyrażenie zgody jest dobrowolne ale jest warunkiem niezbędnym do realizacji celu przetwarzania określonego w pkt. 3. Zgoda może zostać cofnięta

Aleje Ujazdowskie 28
00-478 Warszawa
tel. 22 345 37 00
fax 22 345 37 70
www.ore.edu.pl

w każdej chwili bez podawania przyczyny lecz bez wpływu na zgodność z prawem przetwarzania do którego doszło przed jej cofnięciem;

9. W związku z przetwarzaniem Pani/Pana danych osobowych, przysługują Pani/Panu następujące uprawnienia: prawo dostępu do swoich danych osobowych, prawo żądania ich sprostowania, prawo żądania od administratora ograniczenia przetwarzania lub ich usunięcia prawo do cofnięcia wyrażonej zgody oraz prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

.....

Podpis osoby której dane dotyczą

ORE Ośrodek Rozwoju Edukacji

# Załącznik nr 13 do Polityki Bezpieczeństwa Informacji

## Klauzule umowne w umowach powierzenia przetwarzania danych osobowych

## Ośrodek Rozwoju Edukacji

ORE Ośrodek Rozwoju Edukacji
Aleje Ujazdowskie 28
00-478 Warszawa
tel. 22 345 37 00
fax 22 345 37 70
www.ore.edu.pl

**1. Klauzule w odrębnej umowie o powierzeniu danych osobowych (lub aneks/ustęp w istniejących umowach)**

**§ 1**
**Przedmiot umowy**

1. Ośrodek Rozwoju Edukacji w Warszawie oświadcza, że realizuje obowiązki Administratora określone w art. 4 pkt. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (Dz. U. UE. L. z 2016 r. Nr 119) zwanego w niniejszej Umowie również jako „RODO" lub „Rozporządzenie".
2. Administrator powierza Podmiotowi Przetwarzającemu przetwarzanie danych osobowych, na zasadach określonych w Umowie oraz we właściwych przepisach regulujących przetwarzanie danych osobowych, w szczególności w RODO.
3. Rodzaj danych osobowych, kategorie osób, których dotyczą dane osobowe, jak również przedmiot, czas trwania, charakter i cel przetwarzania danych osobowych są wskazane w **załączniku nr 1** do umowy.
4. Strony zobowiązują się wykonywać zobowiązania wynikające z umowy z najwyższą starannością, w celu prawidłowego zabezpieczenia prawnego, organizacyjnego i technicznego interesów Stron oraz osób, których dane osobowe dotyczą, w zakresie przetwarzania danych osobowych.

*) niepotrzebne skreślić

**§ 2**

**Oświadczenie Podmiotu Przetwarzającego**

1. Podmiot Przetwarzający oświadcza, że:
   a) wdrożył środki techniczne i organizacyjne gwarantujące przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami, w sposób zapewniający ochronę praw osób, których dotyczą dane osobowe;
   b) dysponuje środkami, doświadczeniem, wiedzą oraz odpowiednio wyszkolonym personelem, umożliwiającymi prawidłowe przetwarzanie danych osobowych w zakresie i w celu określonych w umowie.

**§ 3**

**Przetwarzanie danych osobowych**

1. Z zastrzeżeniem ust. 2, przetwarzanie danych osobowych przez Podmiot Przetwarzający może następować wyłącznie w przypadkach wynikających z Umowy lub na podstawie odrębnych zleceń Administratora, wyrażonych w formie pisemnej (papierowej lub cyfrowej, w tym za pośrednictwem poczty elektronicznej).
2. Podmiot Przetwarzający ma prawo przetwarzać dane osobowe, jeżeli obowiązek taki nakłada na niego prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Podmiot Przetwarzający. W takim przypadku Podmiot Przetwarzający jest zobowiązany poinformować Administratora o stosującym się do niego obowiązku prawnym co najmniej na 24 godziny przed rozpoczęciem przetwarzania, chyba że wiążące go przepisy zabraniają mu udzielania takiej informacji, z uwagi na ważny interes publiczny.
3. Przetwarzanie danych osobowych przez Podmiot Przetwarzający jest ograniczone do celu i zakresu wskazanych w **załączniku nr 1** do umowy.
4. Podmiot Przetwarzający prowadzi rejestr czynności przetwarzania danych osobowych, zawierający informacje wymagane przez obowiązujące przepisy, chyba że zgodnie z obowiązującymi przepisami nie ma obowiązku prowadzenia takiego rejestru.
5. Podmiot Przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora zgodnie z art. 30 ust. 2 RODO, chyba że zgodnie z obowiązującymi przepisami nie ma obowiązku prowadzenia takiego rejestru.
6. Wszelkie zlecane przez Administratora operacje przetwarzania danych osobowych Podmiot Przetwarzający wykonuje niezwłocznie, w szczególności jeśli chodzi o usunięcie danych osobowych na żądanie osoby, której dotyczą.
7. Biorąc pod uwagę charakter przetwarzania danych osobowych, Podmiot Przetwarzający ma obowiązek współdziałania z Administratorem w celu wywiązania się z obowiązku odpowiadania na żądania osoby, której dane osobowe dotyczą, w zakresie wykonywania jej praw określonych w obowiązujących przepisach, wdrażając odpowiednie środki techniczne i organizacyjne.
8. Podmiot Przetwarzający zapewni, że osoby, które będą zaangażowane w czynności przetwarzania danych osobowych w ramach jego organizacji:
   a) otrzymają pisemne upoważnienia do przetwarzania danych osobowych;

*) niepotrzebne skreślić

b) będą zaznajomione z obowiązującymi przepisami o ochronie danych osobowych (z uwzględnieniem ich ewentualnych zmian) oraz z odpowiedzialnością za ich nieprzestrzeganie;
c) będą dokonywały czynności przetwarzania danych osobowych wyłącznie na polecenie Administratora, z zastrzeżeniem ust. 2;
d) zobowiążą się do bezterminowego zachowania w tajemnicy danych osobowych oraz stosowanych przez Podmiot Przetwarzający sposobów ich zabezpieczenia, o ile taki obowiązek nie wynika dla nich z odpowiednich przepisów.

9. Podmiot Przetwarzający prowadzi ewidencję udzielonych upoważnień do przetwarzania danych osobowych, o których mowa w ust. 8 lit. a).

**§ 4**
**Dalsze powierzenia przetwarzania**

1. Podmiot Przetwarzający ma prawo korzystać z podwykonawców przy przetwarzaniu danych osobowych (dalsze powierzenie przetwarzania), pod warunkiem, że przed powierzeniem podwykonawcy przetwarzania danych osobowych:
   a) zawrze z podwykonawcą umowę powierzenia przetwarzania danych osobowych na warunkach nie gorszych niż warunki umowy;
   b) upewni się, że podwykonawca zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom obowiązujących przepisów;
   c) poinformuje Administratora w formie dokumentowej (papierowej lub cyfrowej, w tym za pośrednictwem poczty elektronicznej) o zawarciu umowy;
2. Jeżeli podwykonawca nie wywiąże się ze spoczywających na nim obowiązków ochrony danych osobowych, Podmiot Przetwarzający ponosi pełną odpowiedzialność wobec Administratora za wypełnienie obowiązków podwykonawcy.
3. Wykaz podwykonawców, z których Podmiot Przetwarzający korzysta w dniu zawarcia umowy, i co do których Administrator wyraża zgodę na dalsze powierzenie przetwarzania danych osobowych, stanowi załącznik nr 2 do umowy.

**§ 5**
**Bezpieczeństwo danych osobowych**

1. Podmiot Przetwarzający stosuje środki techniczne i organizacyjne, odpowiednie do zagrożeń oraz charakteru, zakresu, kontekstu i celu przetwarzania danych osobowych, zapewniające bezpieczeństwo danych osobowych, w szczególności przed ich przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem.
2. Podmiot Przetwarzający zobowiązuje się stale monitorować stan stosowanych zabezpieczeń danych osobowych oraz występujących zagrożeń bezpieczeństwa, i w razie potrzeby aktualizuje stosowane środki techniczne i organizacyjne, tak, żeby zapewnić najwyższy osiągalny poziom ochrony danych osobowych.

*) niepotrzebne skreślić

3. Podmiot Przetwarzający, uwzględniając charakter przetwarzania danych osobowych oraz dostępne mu informacje, ma obowiązek współdziałania z Administratorem w wywiązaniu się z obowiązków określonych w art. 32–36 RODO.
4. Podmiot Przetwarzający niezwłocznie zawiadamia Administratora, przed podjęciem jakichkolwiek działań, o każdym przypadku:
   a) wystąpienia jakiegokolwiek organu z żądaniem udostępnienia danych osobowych, chyba że zakaz ujawnienia tej informacji wynika z obowiązujących przepisów;
   b) wystąpienia przez osobę, której dane osobowe dotyczą, z żądaniem dotyczącym przetwarzania danych osobowych lub ich treści.
5. Podmiot Przetwarzający niezwłocznie – w każdym wypadku nie później niż w ciągu 24 godzin od wykrycia – informuje Administratora o wszelkich wykrytych naruszeniach bezpieczeństwa danych osobowych, przekazując Administratorowi wszelkie dostępne Podmiotowi Przetwarzającemu informacje na temat naruszenia, w szczególności:
   a) charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane osobowe dotyczą, oraz kategorie i przybliżoną liczbę wpisów, których dotyczy naruszenie;
   b) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   c) możliwe konsekwencje naruszenia ochrony danych osobowych;
   d) środki zastosowane lub proponowane przez Podmiot Przetwarzający w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
6. Podmiot Przetwarzający współdziała z Administratorem przy ustalaniu szczegółów związanych ze zgłoszonym Administratorowi naruszeniem, w szczególności przyczyn i skutków jego wystąpienia oraz wdraża zalecane przez Administratora środki mające na celu złagodzenie ewentualnych niekorzystnych skutków naruszenia danych osobowych oraz środki naprawcze.
7. Podmiot Przetwarzający niezwłocznie informuje Administratora, jeśli jego zdaniem wydane mu przez Administratora polecenie dotyczące przetwarzania danych osobowych stanowi naruszenie obowiązujących przepisów.

**§ 6**
**Prawo do kontroli**

1. Administrator ma prawo kontrolowania sposobu wypełniania przez Podmiot Przetwarzający jego obowiązków określonych w umowie lub w obowiązujących przepisach. W szczególności Administrator może żądać udostępnienia określonych informacji lub dokumentów oraz może przeprowadzać – samodzielnie lub przez upoważnionego przez Administratora pracownika lub współpracownika – audyty, w tym inspekcje w miejscu przetwarzania danych osobowych przez Podmiot Przetwarzający.
2. Podmiot Przetwarzający ma obowiązek współpracować z Administratorem lub upoważnionym przez Administratora pracownikiem lub współpracownikiem w czasie przeprowadzanej kontroli, w sposób

*) niepotrzebne skreślić

umożliwiający Administratorowi weryfikację prawidłowej realizacji obowiązków Podmiotu Przetwarzającego.

**§ 7**
**Rozwiązanie umowy**

1. Umowa wchodzi w życie z dniem podpisania i zostaje zawarta na czas określony do dnia rozwiązania lub wygaśnięcia ostatniej z umów łączących Strony, z których wynika konieczność przetwarzania danych osobowych przez Podmiot Przetwarzający.
2. W przypadku stwierdzenia naruszenia przez Podmiot Przetwarzający obowiązków wynikających z umowy, Administrator ma prawo rozwiązać wszystkie umowy zawarte z Podmiotem Przetwarzającym, z których wynika konieczność przetwarzania danych osobowych przez Podmiot Przetwarzający, ze skutkiem natychmiastowym.
3. Najpóźniej w dniu rozwiązania umowy Podmiot Przetwarzający ma obowiązek:
   a) usunąć wszelkie dane osobowe; albo
   b) zwrócić Administratorowi wszelkie nośniki zawierające dane osobowe oraz usunąć wszelkie istniejące kopie danych osobowych, chyba że obowiązujące przepisy wymagają od niego dalszego przechowywania części lub całości danych osobowych,

   zależnie od wyboru Administratora, zakomunikowanego Podmiotowi Przetwarzającemu w formie dokumentowej (papierowej lub cyfrowej, w tym za pośrednictwem poczty elektronicznej) co najmniej na 7 dni przed terminem rozwiązania Umowy.
4. W przypadku rozwiązania Umowy w trybie ust. 2 wybór Administratora będzie zakomunikowany Podmiotowi Przetwarzającemu w oświadczeniu o rozwiązaniu umowy ze skutkiem natychmiastowym.
5. Czynności wskazane w ust. 3 zostaną wykazane w pisemnym protokole, podpisanym przez przedstawiciela Podmiotu Przetwarzającego i dostarczonym Administratorowi w terminie 7 dni od dokonania wskazanych w nim czynności.

**§ 8**
**Postanowienia końcowe**

1. Podmiotowi Przetwarzającemu nie przysługuje wynagrodzenie za wykonywanie Umowy.
2. Umowa stanowi całość porozumienia pomiędzy Stronami i zastępuje w całości uprzednie lub równoczesne uzgodnienia poczynione przez Strony (w formie pisemnej lub ustnej) w przedmiocie regulowanym postanowieniami niniejszej Umowy.
3. Załączniki do Umowy stanowią jej integralną część.
4. Wszelkie spory między Stronami będą rozwiązywane na zasadzie polubownych negocjacji. W przypadku nieosiągnięcia przez Strony porozumienia, spór zostanie przekazany do rozstrzygnięcia sądowi powszechnemu właściwemu dla siedziby Administratora.
5. Wszelkie zmiany umowy wymagają formy pisemnej pod rygorem nieważności.
6. Umowa została sporządzona w dwóch egzemplarzach, po jednym dla każdej ze Stron.

Administrator: Podmiot Przetwarzający:

*) niepotrzebne skreślić

ORE Ośrodek Rozwoju Edukacji
Aleje Ujazdowskie 28
00-478 Warszawa
tel. 22 345 37 00
fax 22 345 37 70
www.ore.edu.pl

Załączniki:

1. **Załącznik nr 1** do umowy powierzenia przetwarzania danych osobowych z dnia ..... - Dane osobowe;
2. **Załącznik nr 2** do umowy powierzenia przetwarzania danych osobowych z dnia ..... – Podwykonawcy zatwierdzeni przez Administratora

*) niepotrzebne skreślić

ORE Ośrodek Rozwoju Edukacji
Aleje Ujazdowskie 28
00-478 Warszawa
tel. 22 345 37 00
fax 22 345 37 70
www.ore.edu.pl

**Załącznik nr 1 do umowy powierzenia przetwarzania danych osobowych z dnia .....**

**Dane osobowe**

| | |
|---|---|
| **Rodzaje danych osobowych**<br><br>(np. imię, nazwisko, adres, numer PESEL, numer telefonu, e-mail, adres IP, dane o stanie zdrowia) | |
| **Kategorie osób, których dane osobowe dotyczą**<br><br>(np. pracownicy, dostawcy, pacjenci, kontrahenci, klienci) | |
| **Zakres przetwarzania danych osobowych**<br><br>(czynności dokonywane na powierzonych danych osobowych, np.: zbieranie, utrwalanie, organizowanie, porządkowanie, adaptowanie, przechowywanie, modyfikowanie, pobieranie, przeglądanie, udostępnianie, zmienianie, usuwanie | |
| **Charakter przetwarzania**<br><br>(np. systematyczny/sporadyczny) | |
| **Cel przetwarzania**<br><br>(np. wykonanie umowy z dnia...) | |
| **Czas przetwarzania**<br><br>(np. *okres obowiązywania umowy z dnia...)* | |

*) niepotrzebne skreślić

ORE Ośrodek Rozwoju Edukacji
Aleje Ujazdowskie 28
00-478 Warszawa
tel. 22 345 37 00
fax 22 345 37 70
www.ore.edu.pl

**Załącznik nr 2 do umowy powierzenia przetwarzania danych osobowych z dnia .....**

**Podwykonawcy zatwierdzeni przez Administratora**

| Lp. | Nazwa | Adres | NIP |
|---|---|---|---|
| 1. | | | |
| 2. | | | |
| 3. | | | |

*) niepotrzebne skreślić