Zespół Szkolno-Przedszkolny
w Przemiarowie
Przemiarowo 33, 06-100 Pułtusk
NIP 568 14 82 065
tel./fax: 23 691 09 52

Zarządzenie nr 1 a /2023/2024
Dyrektora Zespołu Szkolno-Przedszkolnego
w Przemiarowie
z dnia 25.08.2023r
w sprawie wprowadzenia
Regulaminu Ochrony Danych Osobowych

Na podstawie art. 24 ust. 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), publ. Dz. Urz. UE L Nr 119, s. 1, **zarządza się, co następuje:**

§ 1

Wprowadza się Regulamin Ochrony Danych Osobowych stanowiącą załącznik nr 1 do niniejszego Zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem wydania.

DYREKTOR ZESPOŁU
SZKOLNO-PRZEDSZKOLNEGO
mgr Bożena Kosek

Załącznik nr 1a z dn. 25.08.2023r.

do Zarządzenia nr 1a/2023/2024

ZSP w Przemiarowie

Zespół Szkolno-Przedszkolny
w Przemiarowie
Przemiarowo 33, 06-100 Pułtusk
Regon 130 454 223 / NIP 568 14 82 065
tel./fax: 23 691 09 52

Regulamin Ochrony Danych Osobowych

(Podstawowe zasady bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych oraz w sposób tradycyjny)

OPRACOWANY NA PODSTAWIE

- Rozporządzenia Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwanego „RODO",
- ustawy z dnia 10 maja 2018r. o ochronie danych osobowych, (t.j. Dz.U. z 2018 poz. 1000)
- ustawy z dnia 21 lutego 2019 r. (Dz.U.2019 poz. 730) o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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 (tzw. ustawa wdrażająca RODO)

UWAGA:

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO dla:

- Pracowników
- Nauczycieli
- Współpracowników
- Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora lub Podmiot przetwarzający w imieniu Administratora
- Użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Administratora lub Podmiot przetwarzający w imieniu Administratora
- Stażystów i Praktykantów

Każda z wymienionych osób powinna zapoznać się z poniższym regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych i podpisać oświadczenie o poufności.

WSTĘP

Po pierwsze należy zapytać co to jest RODO, czego dotyczy i po co ono jest?

„RODO", inaczej to zbiór przepisów, wytycznych dotyczących ochrony danych osobowych osób fizycznych, które zostało uchwalone przez Parlament Europejski i Radę (UE) w dniu 27 kwietnia 2016 r. uchylając w ten sposób dyrektywę 94/46/WE. Służy ono w głównej mierze unormowaniu i ujednoliceniu zbierania, przetwarzania i ochrony danych osobowych osób fizycznych, a zarazem ujednoliceniu praw tych osób w państwach Unii Europejskiej. W naszym kraju weszło w życie w dniu 25 maja 2018 r.

Co to są dane osobowe?

Są to dane za pomocą, których można zidentyfikować osobę bezpośrednio lub pośrednio za pomocą imienia i nazwiska, numeru identyfikacyjnego, identyfikatora internetowego, adresu, nr telefonu lub za pośrednictwem kilku szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową tożsamość osoby fizycznej.

Co rozumiemy przez przetwarzanie danych osobowych?

Przetwarzanie 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 przesyłanie, adresowanie, jak również udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Czy istnieje podział danych osobowych?

Tak, podział jest bardzo prosty wygląda to tak:

- dane osobowe zwane danymi zwykłymi i tu zaliczamy dane typu imię i nazwisko, numer identyfikacyjny, nr telefonu, adres zamieszkania, wizerunek;
- dane osobowe tzw. szczególnie chronione lub zwane też wrażliwymi, do nich zaliczamy dane genetyczne, dane biometryczne, dane dotyczące zdrowia lub dane dotyczące orientacji seksualnej, wyznania, przynależności partyjnej itp.;
- dane o wyrokach skazujących nałożonych i odbytych karach.

Należy pamiętać, że w procesie zbierania danych osobowych od osób fizycznych, zakres zbieranych danych był zgodny i adekwatny z celem do jakiego są zbierane i zgodny z prawem (czyli zbieramy dane osobowe tylko w takim zakresie by osiągnąć określony cel, najlepiej jest w stadium projektowania określić jakie minimalne dane są nam niezbędne do osiągnięcia określonego celu), natomiast w przypadku zbierania danych osobowych szczególnie chronionych należy posiadać twardą podstawę prawną w pełni wyczerpującą wymaganie zbierania takich danych od osoby fizycznej.
Przy ostatniej grupie danych osobowych mamy doczynienia z bardzo ograniczoną grupą, która może posiadać dostęp do takich danych, do tej grupy zaliczamy przede wszystkim sądy, prokuraturę i policję, w których to przetwarzanie odbywa się zgodnie z przepisami prawa.

Dopuszczalne jest przetwarzanie takich danych przez jednostki samorządu terytorialnego w uzasadnionych przypadkach pod ścisłym nadzorem organów wymiaru sprawiedliwości (np. prace społeczne nałożone jako kara).
Należy pamiętać, że przetwarzanie danych osobowych, nie dotyczy tylko osób, które zbierają dane osobowe w określonych celach, ale również dotyczy to osób od których są zbierane takie dane, by były w pełni świadome w jakim celu muszą swoje dane udostępnić i jaka jest podstawa prawna zbierania tych danych, zawsze obowiązek informacyjny stoi po stronie zbierającego dane osobowe.

Po wstępie, w którym dowiedzieliśmy się co to jest RODO oraz dane osobowe należy wspomnieć o przepisach prawnych wdrażających rozporządzenie w realia naszej rzeczywistości i obowiązujących podczas przetwarzania:

Rozporządzenie Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwanego „RODO",

W naszym Kraju weszło w życie dnia 25 maja 2018 r. Ustawą

ustawa z dnia 10 maja 2018r. o ochronie danych osobowych

Ustawa ostateczna wdrażająca RODO

ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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

Ustawy i przepisy krajowe

Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz. U. z 2018 r. poz. 996).
Ustawa z dnia 26 stycznia 1982 r. Karta Nauczyciela (Dz. U. z 2018 r. poz. 967).
Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 2018 r. poz. 1457).
Ustawa z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej (Dz. U. z 2017 r. poz. 2159).
Ustawa z dnia 27 października 2017 r. o finansowaniu zadań oświatowych (Dz.U. z 2017 poz. 2203, ze zm.)
Rozporządzenie Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z 2017 r. poz. 1646).

1 ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH.

1. **Należy pamiętać by zbierać dane osobowe zgodnie z wyznaczonym celem i w niezbędnym zakresie**, czyli zbieramy i przetwarzamy dane osobowe tylko niezbędne do osiągnięcia postawionego celu i zgodnie z obowiązującym prawem w sposób zapewniający odpowiednie bezpieczeństwo i ochronę (np. jeśli umawiamy się z klientem w jakimś określonym celu, że poinformujemy go telefonicznie o konkretnej sprawie to potrzebujemy tylko jego nr telefonu i nazwisko) – zgodność z art. 5 RODO;
2. Aby przystąpić do zbierania i przetwarzania danych osobowych należy uzyskać zgodę osoby na przetwarzanie jej danych w określonym celu lub określonych celach (art. 6 pkt. 1a), lub jeśli nie posiadamy takowej zgody, gdyż nie jest ona niezbędna do przetwarzania, albo przetwarzanie jest niezbędne do wykonania zawartej umowy z osobą fizyczną lub niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze możemy posiłkować się pozostałymi punktami zawartymi w pkt. 6 RODO, czyli podstawą do przetwarzania jest zgoda, a w pozostałych przypadkach muszą być spełnione ściśle określone warunki;
3. Jeżeli posiadamy indywidualną zgodę wyrażoną w pisemnym oświadczeniu, którą uzyskaliśmy od osoby w pełni świadomej zgodnie z art. 7 pkt. 2 RODO, to osoba, której dane dotyczą zgodnie z art. 7 pkt. 3 RODO została poinformowana o prawach związanych z możliwością jej cofnięcia. Należy pamiętać o obowiązku informacyjnym w postaci klauzuli informacyjnej zawierającej niezbędne informacje o ADO, celach i prawach osób, których dane są przetwarzane. Klauzule takie są umieszczone i widoczne w ogólnodostępnych miejscach w siedzibie organizacji.
4. Dzieci do lat 16 nie mogą osobiście wyrażać zgody na przetwarzanie danych osobowych, jednak w ich imieniu zgodę wyraża rodzic lub opiekun prawny – zgodność z art. 8 RODO;
5. Zgodnie z obowiązującymi przepisami prawa i wytycznymi zawartymi w RODO niedopuszczalne jest przetwarzanie danych osobowych tzw. wrażliwych (szczególnie chronionych) tj. ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia lub orientacji seksualnej tej osoby.

Powyższe traci moc w przypadku, gdy osoba (lub opiekun prawny), której dane dotyczą wyraziła wyraźną zgodę na przetwarzanie takich danych w konkretnym celu lub celach, a przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonania szczególnych praw nałożonych na Administratora w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to zgodne i dozwolone prawem Unii, lub przepisami i prawem państwa.

Ponadto Administrator może przetwarzać dane osobowe szczególnie chronione bez formalnej zgody w następujących przypadkach:

- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą;

- przetwarzane dane osobowe zostały upublicznione przez osobę, której dane dotyczą;

- przetwarzanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy, lub przetwarzanie jest niezbędne ze względów związanych z ważnych interesem publicznym;

- przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego;

- przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do badań naukowych lub historycznych, do celów statystycznych zgodnie z obowiązującymi przepisami prawa;

2 PRAWA OSOBY KTÓREJ DANE DOTYCZĄ

1. Każda osoba udzielająca zgody na przetwarzanie swoich danych osobowych ma wszelkie prawa dostępu do tych danych – zgodnie z art. 15, 16(*Prawo do sprostowania danych)*, 18(*Prawo do ograniczenia przetwarzania), przenoszenia danych)* RODO, a administrator lub osoba upoważniona musi dołożyć wszelkich starań by udzielić wszelkich informacji dotyczących danych tej osoby i tylko tej osobie – art. 12 RODO;
2. Jednocześnie należy wskazać, iż podczas przetwarzania danych osobowych przez szkołę osobie (uczniowie i rodzice), której dane są przetwarzane zgodnie z przepisami prawa krajowego nie przysługuje prawo do przenoszenia swoich danych oraz prawo do sprzeciwu i usunięcia przetwarzanych danych;
3. Na żądanie zainteresowanej osoby ADO ma obowiązek bez zbędnej zwłoki w ciągu miesiąca udzielić wszelkich informacji dotyczących przetwarzanych jej danych osobowych. Odpowiedź może być udzielona tradycyjnie lub elektronicznie z zachowaniem zabezpieczeń kryptograficznych;

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT zobowiązany jest do korzystania z niego w sposób bezpieczny i chronić przed zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i smartfony oraz inne urządzenia powierzone do przetwarzania danych przez Administratora Danych Osobowych.
   Każdy użytkownik systemu:
   - ma dostęp tylko do tych zasobów danych, do których został upoważniony przez administratora danych;
   - zapewnia ochronę ww. danych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem danych osobowych oraz ich utratą, zniszczeniem lub uszkodzeniem, jak również ma obowiązek zachować te informacje w tajemnicy oraz sposoby ich zabezpieczania (podpisuje stosowne oświadczenie, że jest świadomy obowiązku zabezpieczenia danych);
   - do realizacji zadań służbowych wykorzystuje **tylko służbowy sprzęt i służbowe zewnętrzne nośniki danych;**
   - monitoruje działanie systemu i sprzętu w czasie jego wykorzystywania, a każdy problem techniczny zgłasza administratorowi danych lub bezpośredniemu przełożonemu celem niezwłocznego podjęcia kroków zaradczych;
2. W przypadku zagubienia, utraty lub zniszczenia powierzonego Sprzętu IT użytkownik zobowiązany jest zgłosić ten fakt niezwłocznie Administratorowi Danych Osobowych.
3. Niedopuszczalne jest samowolne instalowanie, otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń przez ADO do sprzętu informatycznego.
4. Użytkownik sprzętu informatycznego jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów nie posiadających właściwych upoważnień) wglądu do danych wyświetlanych na monitorach komputerowych – **tzw. Polityka czystego ekranu**
5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem **wygaszacz ekranu (WINDOWS + L)** by wylogować się z systemu bądź z programu.
6. Po zakończeniu pracy, użytkownik zobowiązany jest:
   a. wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy
   b. zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne i optyczne na których znajdują się dane osobowe
7. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkownania komputerów) lub w odpowiedni sposób zabezpieczać kryptograficznie.
8. Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien TRWALE zniszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczenie płyt DVD i dokumentacji papierowej w niszczarce, zniszczenie mechaniczne twardego dysku, pendrive ale tylko i wyłącznie za zgodą ADMINISTRATORA DANYCH OSOBOWYCH).
9. Użytkownicy komputerów przenośnych na których znajdują się dane osobowe lub z dostępem do danych osobowych przez sieć publiczną, zobowiązani są do stosowania zasad bezpieczeństwa zawartych w Regulaminie użytkowania komputerów przenośnych.

4 ZARZĄDZANIE UPRAWNIENIAMI - PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. Każdy użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) musi mieć założone indywidualne konto systemowe, do którego ma dostęp poprzez własny indywidualny identyfikator (login) oraz hasło zgodne z polityką haseł.
2. Tworzenie kont użytkowników wraz z uprawnieniami (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) odbywa się na polecenie przełożonych a wykonywane przez Administratora systemów IT lub osobę upoważnioną.
3. Użytkownik nie może samodzielnie zmieniać swoich uprawnień (np. uzyskać uprawnienia administratora systemu operacyjnego na swoim komputerze)
4. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika
5. Zabrania się pracy wielu użytkowników na wspólnym koncie.
6. W przypadku systemów informatycznych służących do przetwarzania danych osobowych (np. program kadrowy, program płacowy, Płatnik itp.) każdy użytkownik, któremu nadano uprawnienia i dostęp do określonego systemu, powinien mieć nadany własny login i hasło dostępu do konta właściwego systemu.
7. Użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) rozpoczyna pracę poprzez zalogowanie do systemu z użyciem identyfikatora i hasła.
8. Użytkownik jest zobowiązany do powiadomienia Administratora systemów IT i Administratora Danych Osobowych o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje
9. W przypadku, gdy użytkownik podczas próby zalogowania doprowadzi do zablokowania sesji, zobowiązany jest powiadomić o tym Administratora systemów IT i Administratora Danych Osobowych (czas blokady konta musi wynosić minimum 30 minut)
10. Niedopuszczalne jest umożliwienie wglądu do danych wyświetlanych na ekranie klientom lub pracownikom innych działów nie posiadających właściwego upoważnienia do przetwarzania danych osobowych – należy wyłączyć monitor lub wylogować się z programu i/lub systemu.
11. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu. Jeżeli tego nie uczyni, po upływie 15 minut system automatycznie aktywuje wygaszacz
12. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została ona zweryfikowana jako pracownik firmy lub pracownik upoważniony przez Administratora Danych Osobowych. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
13. Po zakończeniu pracy, użytkownik zobowiązany jest:
    a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy
    b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe

5 POLITYKA HASEŁ

1. Hasła powinny składać się z minimum 8 znaków
2. Hasła powinny zawierać duże litery + małe oraz cyfry lub znaki specjalne
3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów ciągów znaków z klawiatury.
4. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie
5. W przypadku ujawnienia hasła – należy natychmiast je zmienić
6. Hasła muszą być zmieniane co - 30 do 60 dni
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła
8. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło
9. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności
10. Zabrania się używania w serwisach internetowych takich samych lub podobnych haseł jak w systemie komputerowym firmy
11. Zabrania się stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów.
12. Zabrania się definiowania haseł, w których jeden człon pozostaje niezmienny, a drugi zmienia się według przewidywalnego wzorca (np. Anna0001, Anna0002, Anna0003 itd.). Nie powinno się też stosować haseł, w których jeden z członów stanowi imię, nazwę lub numer miesiąca lub inny możliwy do odgadnięcia klucz.

6 ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „**Polityki czystego biurka**". Polega ona na zabezpieczaniu (zamykaniu) dokumentów oraz nośników np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych miejskich lub w lesie.

7 ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI POZA FIRMĘ

1. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Pracodawcy. Do

takich nośników zalicza się: wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu Flash

2. Nośniki wynoszone poza organizację, jeśli wymaga tego sytuacja muszą być zaszyfrowane, a pliki zabezpieczone hasłem.
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach
4. Należy korzystać ze sprawdzonych firm kurierskich
5. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą
6. Dane osobowe wynoszone poza obszar dokumentacji na nośnikach elektronicznych muszą być zaszyfrowane i posiadać zezwolenie Administratora Danych Osobowych.
7. W sytuacji przekazywania danych osobowych poza obszar organizacji na nośnikach elektronicznych można stosować następujące zasady bezpieczeństwa:
    a. adresat powinien zostać powiadomiony o przesyłce
    b. dane przed wysłaniem powinny zostać zaszyfrowane, a hasło podane adresatowi inną drogą
    c. stosować bezpieczne koperty depozytowe
    d. przesyłkę należy przesyłać przez kuriera

8 ZASADY KORZYSTANIA Z INTERNETU

1. Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT (np. ASI) i tylko w uzasadnionych przypadkach
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (w większości strony tego typu posiadają zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem)
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.
8. Zabrania się samowolnego podłączania do komputerów modemów, telefonów komórkowych i innych urządzeń dostępowych (np.: typu BlueConnect, iPlus, OrangeGo). Zabronione jest też łączenie się przy pomocy takich urządzeń z Internetem w chwili, gdy komputer użytkownika podłączony jest do sieci firmowej.

9 ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione i wyłącznie za pośrednictwem służbowych skrzynek pocztowych;
2. W przypadku przesyłania danych osobowych poza jednostkę należy wysyłać pliki zaszyfrowane/spakowane (np. programem 7 zip, winzipem, winrarem) i zabezpieczone hasłem, gdzie hasło powinno być przesłane do odbiorcy inną drogą np. telefonicznie lub SMS;
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym kanałem lub inną metodą, np. telefonicznie lub SMS-em;
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata
6. **UWAGA WAŻNE:** Nie otwierać załączników (.zip, .xlsm, .pdf, .exe) w mailach!!!!! Są to zwykle „wirusy", które infekują komputer oraz często pozostałe komputery w sieci. **WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH**
7. **UWAGA WAŻNE:** Nie wolno „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron z „wirusami". Użytkownik „klikając" na taki hiperlink infekuje komputer oraz inne komputery w sieci. **WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH**
8. Należy zgłaszać Administratorowi systemów IT przypadki podejrzanych e-maili
9. Użytkownicy nie powinni rozsyłać „niezawodowych" e-maili w formie „łańcuszków szczęścia",
10. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości"!
11. Użytkownicy powinni okresowo kasować niepotrzebne maile
12. Podczas realizacji zadań służbowych pracownik korzysta wyłącznie z konta pocztowego firmowego;
13. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych;
14. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób;
15. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum;
16. Zabrania się użytkownikom poczty elektronicznej konfigurowania swoich służbowych kont pocztowych do automatycznego przekierowania wiadomości na adres zewnętrzny;
17. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych;
18. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego;
19. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania;

20. Użytkownik bez zgody Pracodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, a całkowicie niedopuszczalne jest używanie do tego celu prywatnej elektronicznej skrzynki pocztowej

10 Ochrona antywirusowa

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe
3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany!, zainstaluj program antywirusowy", użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Administratora systemów IT lub osobę upoważnioną.

11 ZASADY KORZYSTANIA Z MONITORINGU

1. Jeśli organizacja posiada monitoring wizyjny, to należy przede wszystkim zwrócić uwagę na właściwą stronę informacyjną dotyczącą, iż obiekt lub teren wokół obiektu jest monitorowany, czyli w miejscu widocznym ogólnodostępnym powinny być zainstalowane tablice informujące o zainstalowanych kamerach monitoringu.
2. W każdym wejściu do budynku lub na teren organizacji powinna znaleźć się klauzula zawierająca niezbędne informacje o:
   - podstawie prawnej oraz celu przetwarzania – art. 6 ust. 1 lit. f RODO oraz art. 22^2 Kodeksu Pracy i inne;
   - Administratorze Ochrony Danych Osobowych i jego siedzibie;
   - zakresie i sposobie udostępniania zgromadzonych danych;
   - okresie przechowywania danych osobowych w postaci wizerunku;
   - prawach osób, których dane osobowe zebrano podczas procesu rejestracji;

12 Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Administratora Danych Osobowych w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych
2. Do sytuacji wymagających powiadomienia, należą:

Incydenty umyślne		
1	kradzież sprzętu	Zgłoszenie do administratora i do IOD
2	kradzież danych	Zgłoszenie do administratora i do IOD

3	ujawnienie danych osobom nieupoważnionym	Zgłoszenie do administratora i do IOD
4	świadome zniszczenie danych	Zgłoszenie do administratora i do IOD
5	włamanie do systemu informatycznego	Zgłoszenie do administratora i do IOD
6	włamanie do pomieszczeń	Zgłoszenie do administratora i do IOD
7	wyciek informacji	Zgłoszenie do administratora i do IOD
8	świadome zniszczenie danych	Zgłoszenie do administratora i do IOD
9	działanie wirusów i innego szkodliwego oprogramowania	Zgłoszenie do administratora
10	świadome nieuprawnione modyfikacje danych	Zgłoszenie do administratora i do IOD
zdarzenia losowe wewnętrzne		
1	awaria komputera	Zgłoszenie do administratora
2	awaria serwera	Zgłoszenie do administratora
3	awaria dysku twardego	Zgłoszenie do administratora
4	awaria oprogramowania	Zgłoszenie do administratora
5	awaria w wyniku pomyłki informatyków	Zgłoszenie do administratora
6	pomyłki użytkowników	Zgłoszenie do administratora
7	utrata danych	Zgłoszenie do administratora i do IOD
8	zagubienie danych	Zgłoszenie do administratora i do IOD
zdarzenia losowe zewnętrzne		
1	pożar	Zgłoszenie do administratora
2	zalanie wodą	Zgłoszenie do administratora
3	utrata zasilania	Zgłoszenie do administratora
4	utrata łączności	Zgłoszenie do administratora
5	atak terrorystyczny	Zgłoszenie do administratora
6	atak hackerski	Zgłoszenie do administratora

4. Okoliczności wskazujące na wystąpienie incydentu mogącego skutkować naruszeniem ochrony danych osobowych:

1	ślady na drzwiach, oknach i szafach wskazują na próbę włamania	Zgłoszenie do administratora
2	dokumentacja jest niszczona bez użycia niszczarki	Zgłoszenie do administratora
3	fizyczna obecność w budynku lub pomieszczeniach osób	Zgłoszenie do administratora

	zachowujących się podejrzanie	
4	nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych	Zgłoszenie do administratora i do IOD
5	stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.	Zgłoszenie do administratora i do IOD
6	wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia	Zgłoszenie do administratora i do IOD
7	udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej	Zgłoszenie do administratora i do IOD
8	stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji)	Zgłoszenie do administratora i do IOD
9	telefoniczne próby wyłudzenia danych osobowych	Zgłoszenie do administratora i do IOD
10	kradzież komputerów lub twardych dysków z danymi osobowymi	Zgłoszenie do administratora i do IOD
11	utrata kontroli nad kopią danych osobowych	Zgłoszenie do administratora i do IOD
12	maile zachęcające do ujawnienia identyfikatora i/lub hasła	Zgłoszenie do administratora
13	pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów	Zgłoszenie do administratora
14	istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki"	Zgłoszenie do administratora i do IOD
15	hasła do systemów przechowywane są w pobliżu komputera	Zgłoszenie do administratora i do IOD
16	zmiana danych bez zgody osoby, której dane dotyczą	Zgłoszenie do administratora i do IOD
17	wysłanie danych do niewłaściwej osoby (np. poprzez niewłaściwie zaadresowanie poczty elektronicznej)	Zgłoszenie do administratora i do IOD
18	utrata nośników danych (telefon, laptop, przenośnych nośników, teczki zawierające dane w wersji papierowej)	Zgłoszenie do administratora i do IOD
19	nieuprawnione udostępnienie danych (np. elektronicznie – przekazywanie danych przez zdalny dostęp np. VPN, często przydzielane bezterminowo - ale też np. telefonicznie (rozmówca podaje się za pracownika policji czy urzędu, próbując wyciągnąć informacje)	Zgłoszenie do administratora i do IOD

20	nieodpowiednie usuwanie danych (np. administrator postanawia pozbyć się starych komputerów. Przed sprzedażą usuwa jedynie pliki na pulpicie i opróżnia kosz ze starych plików. Nie usuwa jednak danych z dysku komputera	Zgłoszenie do administratora i do IOD
21	trwała utrata dostęp do danych osobowych w wyniku przerwy w dostawie prądu lub ataku	Zgłoszenie do administratora i do IOD
22	system informatyczny administratora został zainfekowany złośliwym oprogramowaniem	Zgłoszenie do administratora
23	nieostrożne usunięcie danych	Zgłoszenie do administratora
24	wyniesienie przez pomyłkę poza obszar chroniony teczki z niezabezpieczonymi danymi osobowymi, wśród których znajdują się również szczególne kategorie danych osobowych	Zgłoszenie do administratora i do IOD
25	niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów	Zgłoszenie do administratora
26	niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych	Zgłoszenie do administratora i do IOD
27	nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek	Zgłoszenie do administratora i do IOD
28	zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)	Zgłoszenie do administratora
29	otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe	Zgłoszenie do administratora i do IOD

13 OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Pracodawcę / Zleceniodawcę zadaniach
   b. zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem zadań powierzonych przez Pracodawcę / Zleceniodawcę
   c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Pracodawcę / Zleceniodawcę
   d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych
   e. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz ich przetwarzaniem
2. Każda osoba dopuszczona do przetwarzania zapoznaje się z zasadami ochrony danych osobowych lub odbywa szkolenie.

3. Osoby zapoznane z treścią niniejszego Regulaminu ODO zobowiązane są podpisać Oświadczenie o zrozumieniu obowiązujących przepisów i zachowaniu poufności dotyczących przetwarzania danych osobowych.
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego
5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych
6. Zabrania się ujawniania na grupach dyskusyjnych, forach internetowych, blogach itp. jakichkolwiek szczegółów dotyczących funkcjonowania organizacji, w tym informacji na temat sprzętu i oprogramowania, z jakiego korzysta firma, oraz informacji kontaktowych innych, niż ogólnodostępne w materiałach zewnętrznych.

14 POSTĘPOWANIE DYSCYPLINARNE

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Pracodawcę za naruszenie przepisów zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r. oraz Ustawy z dnia 10 maja 2018 r.

Konsekwencje nie przestrzegania zasad ochrony danych osobowych.

W przypadku, naruszenia ochrony danych osobowych, poprzez niewłaściwe zabezpieczenie podczas przesyłania pocztą elektroniczną, umyślne przekazanie informacji osobom trzecim lub też utrata lub zagubienie, lub przetwarzanie niezgodne jest z określonymi celami w organizacji, zastosowanie mają **przepisy karne**, a konkretniej art. 107 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000), penalizujący bezprawne przetwarzanie danych osobowych, zgodnie z którym: „1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, **podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch**". Natomiast jeśli przetwarzanie dotyczy tzw. danych „wrażliwych" (w tym danych dot. zdrowia, seksualności, danych genetycznych, ujawniających pochodzenie rasowe lub etniczne czy przekonania religijne) **ustawodawca zaostrzył karę pozbawienia wolności do lat trzech** (art. 107 ust. 2).

Dodatkowo należy pamiętać o podstawowej zasadzie, iż nałożona kara finansowa przez Urząd Ochrony Danych Osobowych na Administratora

Danych Osobowych w przypadku winy pracownika zostaje przeniesiona na drodze sądowej na winnego.

W interesie każdego pracownika i pracodawcy jest, aby żadna ze wskazanych wyżej form odpowiedzialności nigdy nie znalazła zastosowania. To, co leży po stronie pracownika to zapoznanie się z funkcjonującymi w danej organizacji rozwiązaniami i procedurami dot. ochrony danych osobowych, udział w zapewnianych przez pracodawcę szkoleniach z tego obszaru oraz dochowanie należytej staranności przy wykonywaniu działań na danych osobowych podczas codziennych obowiązków służbowych.

Opracował:

.....

.....

(Administrator Danych Osobowych)