## **Szczerców, 2018-07-26**

## **Klauzula informacyjna**

Na podstawie art. 13 ust. 1 i ust. 2, art. 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (dalej: RODO), informuję, że:

1. Administratorem Danych Osobowych jest Dyrektor Przedszkola Samorządowego w Szczercowie Agnieszka Grabowska, zwany dalej Administratorem.

Administrator prowadzi operacje przetwarzania Pani/Pana danych osobowych.

Inspektorem Danych Osobowych u Administratora jest Jakub Kuszmider, [kontakt@iszd.pl](mailto:kontakt@iszd.pl)

1. Administrator danych osobowych przetwarza Pani/Pana dane osobowe na podstawie obowiązujących przepisów prawa oświatowego i przepisów szczególnych.
2. Pani/Pana dane osobowe przetwarzane są w celu/celach:
3. realizacji zadań Przedszkola wynikajacych z przepisów prawa;
4. w pozostałych przypadkach Pani/Pana dane osobowe przetwarzane są wyłącznie na podstawie wcześniej udzielonej zgody w zakresie i celu określonym w treści zgody.
5. Posiada Pani/Pan prawo do:
6. żądania od Administratora dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych,
7. wniesienia sprzeciwu wobec takiego przetwarzania,
8. przenoszenia danych,
9. wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych,
10. prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, prawo do przenoszenia danych oraz prawo do wniesienia sprzeciwu wobec przetwarzania Pani/Pana danych osobowych, chyba, że ADO może przetwarzać dane na podstawie szczególnych przepisów prawa, tj.
11. przetwarzanie jest niezbędne do prowadzenia postępowania/ wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą,
12. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
13. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
14. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
15. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora.
16. Dane nie będą udostępniane podmiotom innym niż uprawnione na mocy przepisów prawa.
17. Pani/Pana dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu,
18. Pani/Pana dane osobowe będą przechowywane zgodnie ze szczególnymi przepisami.

**Klauzula Informacyjna – monitoring**

Obowiązek informacyjny

1. Informuje, iż Dyrektor Przedszkola Samorządowego w Szczercowie jest Administratorem prowadzonego monitoringu wizyjnego.
2. W celu należytej ochrony danych osobowych, Administrator powołał Inspektora Ochrony Danych, z którym można się skontaktować pod adresem e-mail: [kontakt@iszd.pl](mailto:kontakt@iszd.pl)
3. Monitoring wizyjny jest prowadzony wyłącznie w celu zapewnienia bezpieczeństwa wszystkich osób i mienia.

Podstawą prawną funkcjonowania monitoringu jest: Art. 108a. Ustawa z dnia 14 grudnia 2016 r. - Prawo oświatowe (Dz.U.2018.0.996 )

1. Monitoring wizyjny nie będzie przekazywany innym podmiotom z wyjątkiem tych, które są uprawnione do ich uzyskania na podstawie przepisów obowiązującego prawa.
2. Monitoring wizyjny będzie przechowywany przez okres 2 tygodni.

**Zmiany w zakresie Ochrony Danych Osobowych, w związku z wejściem   
w życie RODO po 25 maja 2018 r.**

Podstawy prawne ochrony danych osobowych

1. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, dalej jako RODO)
2. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (dalej jako Konstytucja)
3. Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. z 2018 r. poz. 1000)

**PODSTAWOWE POJĘCIA**

**dane osobowe -** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

**zbiór danych –** uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów , niezależnie od tego czy zestaw ten jest scentralizowany, zdecentralizowany, rozproszony funkcjonalnie lub rozproszony geograficznie.

**profilowanie –** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystywaniu danych osobowych do oceny, niektórych czynników osobowych osoby fizycznej, w szczególności do:

* analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej,
* jej sytuacji ekonomicznej,
* zdrowia,
* osobistych preferencji,
* zainteresowań,
* wiarygodności,
* zachowania,
* lokalizacji,
* przemieszczania się.

**pseudonimizacja –** oznacza przetworzenie danych osobowych w taki sposób, aby nie można było ich przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

**dane genetyczne —** dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej (art. 4 pkt 13 RODO);

**dane dotyczące zdrowia** — dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia (art. 4 pkt 15 RODO).

**dane biometryczne —** dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne (art. 4 pkt 14 RODO);

**szczególna kategoria danych osobowych (**kiedyś - dane wrażliwe) – dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne;

**zgoda – zgoda osoby, której dane dotyczą oznacza:**

* dobrowolne
* konkretne
* świadome
* jednoznaczne
* okazanie woli, którym osoba, której dane dotyczą, w formie:
* oświadczenia
* wyraźnego działania potwierdzającego

**przetwarzanie danych –** operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany

**PRZETWARZANIE DANYCH TO:**

**ZBIORY DANYCH OSOBOWYCH (U.O.D.O) A PROCESY PRZETWARZANIA DANYCH (RODO).**

|  |  |
| --- | --- |
| ZBIÓR DANYCH OSOBOWYCH | PROCES PRZETWARZANIA DANYCH OSOBOWYCH |
|  |  |
| ZBIÓR DANYCH OSOBOWYCH PRACOWNIKÓW | WYKONYWANIE UMÓW O PRACĘ |
| DOKUMENTACJA BHP | PROWADZENIE DOKUMENTACJI BHP |
| MONITORING WIZYJNY | PROWADZENIE MONITORINGU WIZYJNEGO |
| DOKUMENTACJA FINANSOWO-KSIĘGOWA | PROWADZANIE DOKUMENTACJI FINANSOWO - KSIĘGOWEJ |
| WNIOSKI O UDOSTĘPNIENIE INFORMACJI PUBLICZNEJ | OBSŁUGA OSÓB SKŁADAJĄCYCH WNIOSKI O UDZIELENIE INFORMACJI PUBLICZNEJ. |
| REJESTR KORESPONDENCJI PRZYCHODZĄCEJ I WYCHODZĄCEJ | KORESPONDENCJA |
| ZBIÓR DANYCH OSOBOWYCH KANDYDATÓW NA PRACOWNIKÓW | REKRUTACJA PRACOWNIKÓW |

**ZASADY PRZETWARZANIA DANYCH OSOBOWYCH (ART. 5 RODO)**

**zgodność z prawem, rzetelność i przejrzystość**

**ograniczenie celu**

**minimalizacja danych**

**prawidłowość**

**ograniczenie przechowywania**

**integralność i poufność**

**rozliczalność**

**Zasada zgodności z prawem, rzetelności i przejrzystości** – oznacza przetwarzanie danych wyłącznie w przypadku spełnienia jednego ze wskazanych w RODO warunków (art. 6 i 9) oraz przekazanie osobie, której dane są pozyskiwane informacji określonych w art. 13 i 14.

**Zasada ograniczenia celu –** oznacza, że dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;

**Zasada minimalizacji danych –** oznacza, że dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;

**Zasada prawidłowości –** oznacza, że dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;

**Zasada ograniczenia przetwarzania –** oznacza, że dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą;

**Zasada integralności i poufności –** oznacza przetwarzanie w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych;

**Rozliczalność -** Administrator jest odpowiedzialny za przestrzeganie przepisów i musi być w stanie wykazać ich przestrzeganie.

**Zgodność przetwarzania z prawem (art. 6 RODO)**

1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - spełniony jest co najmniej jeden z poniższych warunków:
   1. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
   2. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
   3. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
   4. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
   5. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
   6. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem.
2. Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

**Przetwarzanie szczególnych kategorii danych osobowych (art. 9 RODO)**

1.Zabrania się przetwarzania danych osobowych 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, seksualności lub orientacji seksualnej tej osoby.

2.Ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:

* 1. osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;
  2. przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
  3. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
  4. przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
  5. przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
  6. przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
  7. przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
  8. przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;
  9. przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
  10. przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

**Prawa osób, których dane dotyczą**

**OBOWIĄZKI ADMINISTRATORA**

**Inspektor Ochrony Danych**

**ZADANIA IOD**

**Artykuł 38.i 39 RODO - Status inspektora ochrony danych.**

**Administrator oraz podmiot przetwarzający zapewniają**:

* by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
* wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań
* dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
* by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań.

Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.

Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.

Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego.

**Zgodnie z art 39. Zadania inspektora ochrony danych.**

1. Inspektor ochrony danych ma następujące zadania:

a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;

d) współpraca z organem nadzorczym;

e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa

**Powierzenie przetwarzania danych osobowych**

powierzenie przetwarzania danych osobowych – zlecenie wykonania czynności przetwarzania danych osobowych przez podmiot przetwarzający na rzecz Administratora na podstawie stosownego zapisu w umowie zapewniającego warunki bezpieczeństwa danych osobowych zgodnie z przepisami Rozporządzenia lub na podstawie odrębnej pisemnej umowy powierzenia przetwarzania danych osobowych zawartej zgodnie z  art. 28 Rozporządzenia

**Zagrożenia przy korzystaniu z systemu informatycznego podczas pełnionych obowiązków służbowych**

* E-maile nakłaniające do wykonania określonych operacji
* Zamieszczanie nieznanych linków na stronach internetowych
* Korzystanie z form komunikacji internetowej tj. portale społecznościowe czy komunikatory.
* Zasady postępowania pocztą elektroniczną i innymi źródłami informacji
* Używaj programów antywirusowych,
* Zawsze uważnie sprawdzaj zawartość wiadomości e-mail,
* Nie uruchamiaj załączników do poczty elektronicznej, gdy nie masz pewności, że jest to załącznik bezpieczny,
* Używaj przeglądarek internetowych, które mają wysokie lokaty w testach bezpieczeństwa,
* Nie wysyłaj za pośrednictwem poczty e-mail żadnych danych osobistych,
* Przed podaniem swoich poufnych danych upewnij się do kogo należy strona www,

**Uzupełniaj swoją wiedzę na temat zagrożeń w sieci np. informacje na serwisach dotyczących zagrożeń w sieci,**

**Naruszenie bezpieczeństwa danych osobowych**

naruszeniem bezpieczeństwa danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawniania danych osobowych, udostępniania lub umożliwiania dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego

**Co zrobić w przypadku naruszenia bezpieczeństwa danych osobowych?**

**ZASADY OCHRONY DANYCH OSOBOWYCH**

1. Pracujesz na danych, które są niezbędne do wykonywania obowiązków na Twoim stanowisku, tylko i wyłącznie w celu relacji swoich zadań
2. Jesteś odpowiedzialny za przetwarzane i powierzone Tobie informacje oraz jesteś zobowiązany do przestrzegania ustanowionych procedur wewnętrznych związanych z ochroną danych osobowych,
3. Nie zostawiaj osób postronnych samych w pomieszczeniu pod Twoją nieobecność. Bezwzględnie zamykaj pomieszczenia na klucz przy ich opuszczaniu i nie pozostawiaj kluczy w zamkach.
4. Zasada czystego biurka - nie zostawiaj bez nadzoru dokumentów papierowych oraz nośników danych na biurku,
5. Zasada czystego kosza – dokumenty papierowa z wyjątkiem materiałów promocyjnych powinny być niszczone w niszczarkach,
6. Blokuj komputer przy każdym opuszczeniu pomieszczenia. W przypadku dłuższej nieobecności w pomieszczeniu koniecznie wyloguj się z systemu,
7. Komputery i urządzania mobile powinny zawierać hasła,
8. Rekomenduje się zmianę hasła, co pewien ustalony okres czasu
9. Wygaszacz komputera powinien uruchamiać się, gdy nie pracujesz przez pewien okres czasu, rekomendujemy, aby ekran wygaszał się po 10 min, jeśli nie pracujesz na komputerze
10. Nie korzystaj z komputera służbowego w celach prywatnych
11. Monitor komputera powinien być tak ustawiony, aby uniemożliwić wgląd osobom postronnym w przetwarzane dane osobowe,
12. Na pulpicie komputera miej zapisane jedynie ikony standardowego oprogramowania i aplikacji służbowych oraz skróty do folderów, pod warunkiem, że w nazwie nie zawierają informacji, które mogą zostać w sposób niekontrolowany ujawnione np. podczas prezentacji.
13. Jesteś zobowiązany do pracy w systemach informatycznych na przypisanych Tobie kontach. Zabronione jest udostępnianie kont osobom trzecim.
14. Nie udzielaj informacji telefonicznie, jeśli nie jesteś w stanie zidentyfikować osoby, z którą rozmawiasz,
15. Nie otwieraj wiadomości e-mail, wobec których masz podejrzenia,
16. Gdy wysyłasz dane osobowe e-mailem pamiętaj, aby zawsze zabezpieczyć je w należyty sposób np. szyfrując za pomocą odpowiednich licencjonowanych programów
17. Zabrania się samodzielnego instalowania oprogramowania, w tym w szczególności przechowywania na komputerze treści naruszających prawa autorskie oraz innych nielegalnych danych.
18. Zamykaj szafy z dokumentami na klucz
19. Nigdy nie zostawiaj samych osób, które nie mają upoważnienia to przetwarzania danych
20. Zwracaj uwagę na osoby, które mogą wzbudzić uzasadnione podejrzenie niecelowości przebywania w jednostce

**Procedura postępowania w przypadku uzasadnionego podejrzenia naruszenia danych osobowych lub naruszenie ochrony danych osobowych.**

**Zgodnie z art. 33 i 34 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) z dnia 27 kwietnia 2016 r. (Dz.Urz.UE.L Nr 119, str. 1)**

**§1**

Celem procedury jest określenie sposobu postępowania w przypadku uzasadnionego podejrzenia naruszenia danych osobowych lub naruszenia ochrony danych.

**§2**

Naruszenie bezpieczeństwa przetwarzanych danych osobowych, określone jest jako przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

**§3**

1. W każdym przypadku, kiedy pracownik jednostki ma uzasadnione podejrzenie, iż mogło dojść do naruszenia ochronę danych osobowych lub doszło do naruszenia ochrony danych zobowiązany jest niezwłocznie, najpóźniej w ciągu 24 godzin po stwierdzeniu naruszenia lub uzasadnionego podejrzenia, iż doszło do naruszenia ochrony danych osobowych zawiadomić Inspektora Ochrony Danych lub Administratora Danych Osobowych.
2. Jeżeli mimo uzasadnionego podejrzenia, iż mogło dojść do naruszenia ochrony danych osobowych lub naruszenia ochrony danych osobowych, pracownik jednostki nie zgłosi Administratorowi Danych Osobowych lub Inspektorowi Ochrony Danych tego faktu, to zobowiązany jest do wyjaśnienia przyczyny opóźnienia na piśmie w ciągu 24 godzin.
3. Wyjaśnienie na piśmie przedkłada Administratorowi Danych Osobowych lub Inspektorowi Ochrony Danych.
4. Niewywiązanie się ze zobowiązań w zakresie ochrony danych osobowych skutkuje nałożeniem na pracownika odpowiedzialności zgodnie z obowiązującymi przepisami prawa w szczególności Kodeksem Pracy.

§4

Zgłoszenia o uzasadnionym podejrzeniu naruszenia ochrony danych, naruszeniu ochrony danych nie dokonuje się jeśli jest mało prawdopodobne, by takie naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, jednak decyzję o tym podejmuje Administrator Danych Osobowych w porozumieniu z Inspektorem Ochrony Danych.

**§5**

Sposób reagowania na naruszenia przez pracowników, którzy je ujawnili.

1. Należy niezwłocznie poinformować o zdarzeniu osobę nadzorującą, Administratora Danych Osobowych, Inspektora Ochrony Danych.
2. Miejsce zdarzenia powinno się pozostawić w stanie nienaruszonym do czasu przybycia inspektora ochrony danych lub innej osoby nadzorującej,
3. Zebrane materiały powinno się przedstawić administratorowi danych, który z pomocą inspektora ochrony danych, w terminie i na podstawie przesłanek określonych w ogólnym rozporządzeniu o ochronie danych powinien ocenić, czy zaistniałe naruszenie podlega obowiązkowi zgłoszenia organowi nadzorczemu oraz powiadomieniu osoby, której dane dotyczą.

**§6**

W przypadku naruszenia ochrony danych osobowych w organizacji, Administrator Danych lub Inspektor Ochrony Danych bez zbędnej zwłoki, w terminie 72 godzin po stwierdzeniu naruszenia, jest zobowiązany zgłosić takie naruszenie organowi nadzorczemu – Prezesa Urzędu Ochrony Danych Osobowych.

§7

W przypadku gdy naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych należy również poinformować osobę, której dane dotyczą**.**

**§7**

Zgłoszenie naruszenia do Prezesa Urzędu Ochrony Danych Osobowych powinno zgodnie z art. 33 ust.3