POLITYKA BEZPIECZEŃSTWA

w

Przedszkolu Miejskim Nr 215 w Łodzi

Pieczęć firmowa:	Podpis Administratora Danych Osobowych:	Data:
		17.09.2018 r.

Wstęp

Realizując konstytucyjne prawo każdej osoby do ochrony życia prywatnego oraz postanowienia 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) w celu zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ww. rozporządzenia oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, wprowadza się następujący zestaw procedur w przedszkolu.

Rozdział 1

Podstawa prawna

1. Konstytucja Rzeczypospolitej Polskiej (art. 47 i 51 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. Dz.U. 1997 nr 78 poz. 483).

2. Ustawa o ochronie danych osobowych – rozumie się przez to Ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000),

3. Ogólne rozporządzenie o przetwarzaniu danych osobowych (w skrócie zwanym dalej RODO) – rozumie się przez to 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.

4. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. nr 100 poz. 1024 z późn. zm.).

5. Ustawa z dnia 26 czerwca 1974 r. – **Kodeks pracy** (Dz. U. 1974 nr 24 poz. 141 z późn. zm.).

6. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U. 2015, poz. 719);

7. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. 2015, poz. 745)

Definicje

§ 1

1) **Administrator-Przedszkole** – w tym dokumencie jest rozumiane jako Przedszkole Miejskie Nr 215 w Łodzi (ul. Budowlana 11/13, 93-356 Łódź);
2) **Polityka** – w tym dokumencie jest rozumiana jako „Polityka bezpieczeństwa" obowiązująca w Przedszkolu Miejskim Nr 215 w Łodzi;
3) **Instrukcja** – w tym dokumencie rozumiana jest jako „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Przedszkolu Miejskim Nr 215 w Łodzi;
4) **UODO –** Urząd Ochrony Danych Osobowych;
5) **dane osobowe** – rozumie się przez to 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;
6) **zbiór danych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie, zbiory danych określone są w załączniku nr 10;

7) **przetwarzanie danych** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich 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;
8) **system informatyczny** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
9) **zabezpieczenie danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
10) **administrator danych (ADO)** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
11) **administrator systemu informatycznego (ASI)** – osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych;
12) **inspektor ochrony danych (IOD) –** osoba wyznaczona przez administratora danych i zgłoszona do rejestru organu nadzorczego odpowiedzialna za bezpieczeństwo danych osobowych w formie papierowej oraz przetwarzania we wskazanych systemach informatycznych;
13) **osoba upoważniona –** osoba posiadająca upoważnienie wydane przez administratora danych osobowych (ADO) (lub osobę uprawnioną przez niego) i dopuszczona jako użytkownik do przetwarzania danych osobowych w formie elektronicznej (w systemie informatycznym) i papierowej w zakresie wskazanym w upoważnieniu;

14) **użytkownik systemu** – osoba upoważniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w szkole, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w szkole;
15) **zgoda osoby, której dane dotyczą** – oznacza to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
16) **odbiorca danych** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
17) **państwo trzecie** – rozumie się przez to państwo nie należące do Europejskiego Obszaru Gospodarczego;
18) **środki techniczne i organizacyjne** – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych;
19) **profilowanie** – oznacza to dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
20) **pseudonimizacja** – oznacza to przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

21) **teletransmisja** - przesyłanie informacji za pomocą sieci telekomunikacyjnej;
22) **podmiot przetwarzający** – oznacza to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
23) **naruszenie ochrony danych osobowych** – oznacza to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
24) **sieć publiczna** – sieć telekomunikacyjna, niebędącą siecią wewnętrzną służąca do świadczenia usług telekomunikacyjnych w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. 2017, poz. 1907 z późn. zm.);
25) **sieć telekomunikacyjna** – urządzenia telekomunikacyjne zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci za pomocą przewodów, fal radiowych, bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. 2017, poz. 1907 z późn. zm.).

Rozdział 2
Administrator danych

§ 2

Administratorem danych osobowych jest Przedszkole Miejskie Nr 215 w Łodzi reprezentowane przez Dyrektora.

§ 3

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator danych wdraża odpowiednie środki techniczne i organizacyjne, aby:
- przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane;
- zapewniały wymagane zaangażowanie pracowników w utrzymanie poziomu bezpieczeństwa informacji w tym ochrony danych osobowych, które przetwarza Administrator;

- określały kierunki rozwoju zarządzania bezpieczeństwem informacji w tym ochroną danych osobowych, przy jednoczesnym spełnieniu wszelkich wymogów obowiązującego prawa oraz zagwarantowaniu sprawnego funkcjonowania Administratora;
- identyfikowały i obniżały katalog ryzyk związanych z bezpieczeństwem informacji, w tym ochroną danych osobowych;

Przedszkole prowadzi rejestr czynności przetwarzania oraz wyznacza Inspektora Ochrony Danych (IOD).

Ochronie podlegają w szczególności:

a) dane osobowe przetwarzane przez Administratora, niezależnie od ich formy i nośnika,
b) sprzęt wykorzystywany do przetwarzania, przesyłania i przechowywania danych osobowych u Administratora,
c) pomieszczenia, w których znajduje się kluczowy sprzęt informatyczny zawierający dane osobowe,
d) dokumenty zawierające dane osobowe,
e) oprogramowanie wykorzystywane u Administratora,
f) wizerunek Administratora,
g) pozostałe mienie wykorzystywane przez Administratora lub będące jego własnością,
h) informacje, których właścicielem są kontrahenci lub jednostki zewnętrzne współpracujące z Administratorem – w ramach tej współpracy.

Rozdział 3
Cele i zasady funkcjonowania polityki bezpieczeństwa

Polityka bezpieczeństwa informacji w Przedszkolu ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tj.:

1. Naruszeń danych osobowych rozumianych jako prywatne dobro powierzone Przedszkolu;
2. Naruszeń przepisów prawa oraz innych regulacji;
3. Utraty lub obniżenia reputacji Przedszkola;
4. Strat finansowych ponoszonych w wyniku nałożonych kar;
5. Zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemów.

Procedurę związaną z naruszeniem danych osobowych określa treść niniejszej Polityki Bezpieczeństwa oraz załączniki nr 8, 9, 11, 12.

Administrator może wyznaczyć Administratora Systemów Informatycznych. ASI, jeśli został wyznaczony:

► zarządza bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa i dokumentami wewnętrznymi z zakresu ochrony danych osobowych obowiązującymi w Przedszkolu,

► doskonali i rozwija metody zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem,

► przydziela identyfikatory użytkownikom systemu informatycznego oraz zaznajamia ich z procedurami ustalania i zmiany haseł dostępu,

► nadzoruje prace związane z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu,

► zapewnia bezpieczeństwo wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych,

► prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne nośniki informacji zawierających dane osobowe,

► odpowiada za zapewnienie przestrzegania zasad ochrony danych osobowych przetwarzanych za pomocą systemów informatycznych.

ASI, jeśli został wyznaczony, podlega bezpośrednio kierownikowi jednostki organizacyjnej lub Administratorowi podczas wykonywania obowiązków z zakresu ochrony danych osobowych.

W przypadku nie wyznaczenia ASI za zapewnienie przestrzegania zasad ochrony danych osobowych przetwarzanych za pomocą systemów informatycznych odpowiada Administrator.

Dyrektor Przedszkola upoważniając pracownika zobowiązuje go do:

► ochrony prawa do prywatności osób fizycznych powierzających Przedszkolu swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w Polityce bezpieczeństwa Przedszkola,

► zapoznania się z zasadami określonymi w Polityce bezpieczeństwa Przedszkola i złożenia oświadczenie o znajomości tych przepisów.

Środki techniczne i organizacyjne

§ 4

1. Przetwarzanie danych osobowych może odbywać się wyłącznie w obszarach do tego celu przeznaczonych. Wykaz pomieszczeń, w których dopuszczalne jest przetwarzanie danych osobowych, stanowi załącznik nr 6.
2. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe lub przechowywane są kopie zapasowe baz danych zabezpieczony jest przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w tym obszarze jest możliwe tylko w obecności osoby upoważnionej do przetwarzania danych osobowych. Wejście do tego obszaru jest zabezpieczone.

§ 5

1. Przetwarzać dane osobowe może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych zgodnie z załącznikiem nr 5.
2. Wykaz osób upoważnionych do przetwarzania danych osobowych prowadzi administrator danych osobowych zgodnie z załącznikiem nr 7.
3. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
4. Identyfikator jest w sposób jednoznacznie przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora.
5. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.

§ 6

W celu ochrony danych osobowych stosuje się procedurę zarządzania kluczami i zasady dostępu:

a) Dyrektor wyznacza pracowników, którzy są upoważnieni do otwierania drzwi wejściowych oraz rozkodowywania systemu alarmowego przed rozpoczęciem pracy (załącznik nr 15).
b) Osobami wyznaczonymi są:

- nauczyciele;
- kucharki;
- intendent;
- pracownik sekretariatu.

c) Otwieranie Przedszkola w soboty, niedziele i święta możliwe jest jedynie za zgodą Dyrektora.

d) Pracownik, któremu powierzono klucze oraz kod cyfrowy do systemu alarmowego zobowiązany jest do:
- wykorzystania ich zgodnie z przeznaczeniem,
- nie kopiowania powierzonych kluczy bez zgody dyrektora oraz nie udostępniania osobom trzecim,
- nie udostępniania kodu cyfrowego do systemu alarmowego osobom trzecim.

e) Upoważnienie do zarządzania kluczami oraz kodem cyfrowym do systemu alarmowego Przedszkola pracownik potwierdza podpisem w rejestrze wydanych kluczy (załącznik nr 16).

f) Kluczami do gabinetu dyrektora dysponuje dyrektor oraz intendent. Pracownik sekretariatu oraz intendent dysponują kluczami do pomieszczeń w których wykonują swoje obowiązki pracownicze i ponoszą pełną odpowiedzialność za ich prawidłowe zabezpieczenie.

g) Po otwarciu pomieszczeń pracownicy sprawdzają stan zabezpieczeń sprzętu biurowego i komputerowego oraz dokumentacji i wyposażenia. W przypadku stwierdzenia nieprawidłowości lub naruszeń stanu zabezpieczeń pracownik, który to stwierdził natychmiast powiadamia Dyrektora Przedszkola.

h) Klucze do biurek, szafek oraz szaf drewnianych są w posiadaniu pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.

i) Zamknięcie dostępu zewnętrznego do całej strefy przetwarzania dokonuje się po wyznaczonych godzinach pracy;

j) Po opuszczeniu strefy przez wszystkich pracowników wyznaczony pracownik załącza system alarmowy w obiekcie i zamyka strefę;

k) Zabrania się pozostawiania kluczy w zamkach od drzwi podczas obecności i nieobecności pracownika w pomieszczeniu;

l) Zabrania się udostępniania kluczy osobom nieupoważnionym;

m) Zabrania się pozostawiania kluczy bez dozoru.

§ 7

1. W celu ochrony danych osobowych stosuje się politykę czystego biurka i czystego ekranu.
2. W przypadku dłuższej nieobecności przy stanowisku pracy lub po jej zakończeniu pracownik jest zobowiązany do umieszczenia wszelkich dokumentów i nośników zawierających dane osobowe w bezpiecznym miejscu np. zamykanej szafce. Nie należy również dokumentów i nośników pozostawiać w łatwo dostępnych miejscach.
3. W przypadku opuszczenia stanowiska pracy pracownik jest zobowiązany do wylogowania się z aplikacji lub zablokowania pulpitu stacji roboczej w celu uniemożliwienia dostępu do systemu lub aplikacji osoby nieupoważnionej zgodnie z procedurą wynikająca z Instrukcji Zarządzania Systemem Informatycznym – załącznik nr 13.

§ 8

W celu ochrony danych osobowych stosuje się następujące środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

a) komputery służące do przetwarzania danych osobowych nie są połączone z lokalną siecią komputerową;
b) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
c) stosuje się systemowe mechanizmy wymuszające okresową zmianę haseł;
d) stosuje się system rejestracji dostępu do systemu/zbioru danych osobowych;
e) dostęp do środków teletransmisji zabezpieczony jest za pomocą mechanizmów uwierzytelnienia;
f) stosuje się środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity;
g) używa się systemu Firewall do ochrony dostępu do sieci komputerowej;

§ 9

W celu ochrony danych osobowych stosuje się następujące środki ochrony w ramach narzędzi programowych i baz danych:

a) stosuje się środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych;
b) stosuje się środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych;
c) dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
d) stosuje się systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego;
e) stosuje się mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych;
f) zainstalowane są wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe;
g) stosuje się mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

Rozdział 4

Procedura DPIA

(Data Protection Impact Assessment)

§ 10

Ocenę skutków dla ochrony danych osobowych (DPIA) przeprowadza każdorazowy właściciel procesu wskazany przez administratora danych z wykorzystaniem załącznika nr 1.

§ 11

1. DPIA jest przeprowadzana przy każdorazowej istotnej zmianie procesu przetwarzania danych osobowych, np. zmiana dostawcy usług, zmiana sposobu przetwarzania danych, wymiana zasobów biorących udział w procesie.

2. DPIA jest przeprowadzana wraz z analizą ryzyka nie rzadziej niż raz w roku w stosunku do procesów, które w wyniku poprzednio przeprowadzonego DPIA wykazały wysokie ryzyko dla praw i wolności osób, których dane dotyczą.

Rozdział 5
Procedura analizy ryzyka i plan postępowania z ryzykiem

§ 12

Analizę ryzyka dla zasobów biorących udział w procesach przeprowadza każdorazowy właściciel procesu wskazany przez administratora danych lub administrator danych samodzielnie z wykorzystaniem załącznika nr 2.

§ 13

Analiza ryzyka jest przeprowadzana nie rzadziej niż raz w roku i stanowi podstawę do aktualizacji sposobu postępowania z ryzykiem.

§ 14

Na podstawie wyników przeprowadzonej analizy ryzyka, wskazani przez administratora danych właściciele procesów lub administrator danych samodzielnie wdrażają sposoby postępowania z ryzykiem.

§ 15

Każdorazowo administrator danych wybiera sposób postępowania z ryzykiem i określa, które ryzyka i w jakiej kolejności będą rozpatrywane jako pierwsze.

§ 16

Administrator danych nie może zlekceważyć ryzyk, których wartość przekracza 6 punktów zgodnie z załącznikiem nr 2 lub ryzyka w stosunku do zasobu, biorącego udział w procesie wysokiego ryzyka zgodnie z wynikiem DPIA zgodnie z załącznikiem nr 1.

Rozdział 6

Procedura współpracy z podmiotami zewnętrznymi

§ 17

Każdorazowe skorzystanie z usług podmiotu przetwarzającego jest poprzedzone zawarciem umowy powierzenia przetwarzania danych osobowych zgodnie z załącznikiem nr 3.

§ 18

Nie rzadziej niż raz w roku oraz każdorazowo przed zawarciem umowy powierzenia przetwarzania danych osobowych administrator danych weryfikuje zgodność z rozporządzeniem wszystkich podmiotów przetwarzających, z których usług korzysta lub ma zamiar skorzystać z wykorzystaniem listy kontrolnej.

Rozdział 7

Procedura domyślnej ochrony danych

§ 19

Administrator danych w przypadku zamiaru rozpoczęcia przetwarzania danych osobowych w nowym procesie przeprowadza DPIA w stosunku do tego procesu.

§ 20

W każdym przypadku tworzenia nowego produktu lub usług administrator danych uwzględnia prawa osób, których dane dotyczą, na każdym kluczowym etapie jego projektowania i wdrażania.

Rozdział 8

Procedura zarządzania incydentami

§ 21

W każdym przypadku naruszenia ochrony danych osobowych administrator danych weryfikuje, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych na podstawie procedury określonej jako Instrukcja postępowania w sytuacji naruszeń – załącznik nr 14.

§ 22

Administrator danych w przypadku stwierdzenia, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, zawiadamia niezwłocznie organ nadzorczy, jednak nie później niż w ciągu 72 godz. od identyfikacji naruszenia.

§ 23

Administrator danych zawiadamia osoby, których dane dotyczą, w przypadku wystąpienia wobec nich naruszeń skutkujących ryzykiem naruszenia ich praw lub wolności, chyba że zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka wystąpienia ww. naruszenia.

§ 24

Administrator danych dokumentuje naruszenia, które skutkują naruszeniem praw i wolności osób fizycznych i sporządza raport zgodnie z załącznikiem nr 8.
Administrator prowadzi również rejestr naruszeń bezpieczeństwa zgodnie z załącznikiem nr 9.

Rozdział 9
Procedura realizacji praw osób

§ 25

Każdy przypadek zgłoszenia przez osobę, której dane dotyczą, woli skorzystania z praw przewidzianych w rozporządzeniu administrator danych rozpatruje indywidualnie.

§ 26

Administrator danych niezwłocznie realizuje następujące prawa osób, których dane dotyczą:

a) prawo dostępu do danych,
b) prawo do sprostowania danych,
c) prawo do usunięcia danych,
d) prawo do przenoszenia danych,
e) prawo do sprzeciwu wobec przetwarzania danych,
f) prawo do nie podlegania decyzjom opartym wyłącznie na profilowaniu.

§ 27

W przypadku realizacji prawa do sprostowania, usunięcia i ograniczenia przetwarzania danych administrator danych niezwłocznie informuje odbiorców danych, którym udostępnił on przedmiotowe dane, chyba że jest to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

§ 28

Administrator danych odmawia realizacji praw osób, których dane dotyczą, jeżeli możliwość taka wynika z przepisów rozporządzenia, jednak każda odmowa realizacji praw osób, których dane dotyczą, wymaga uzasadnienia z podaniem podstawy prawnej wynikającej z rozporządzenia.

Rozdział 10
Procedura odbierania zgód oraz informowania osób

§ 29

W każdym przypadku pobierania danych bezpośrednio od osoby, której dane dotyczą, administrator danych informuje osobę, której dane dotyczą, zgodnie z załącznikiem nr 4.

§ 30

W każdym przypadku pobierania danych z innych źródeł niż osoba, której dane dotyczą, administrator danych informuje osobę, której dane dotyczą, niezwłocznie, jednak nie później niż przy pierwszym kontakcie z osobą, której dane dotyczą, zgodnie z załącznikiem nr 4.

§ 31

W każdym przypadku odbierania zgody od osoby, której dane dotyczą, korzysta się z klauzul zgody określonych w załączniku nr 4.

Rozdział 11

Postanowienia końcowe

§ 32

Wszelkie zasady opisane w niniejszym dokumencie są przestrzegane przez osoby upoważnione do przetwarzania danych osobowych ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą.

§ 33

Przed wprowadzeniem niniejszej polityki bezpieczeństwa sporządzono audyt dokumentujący dotychczasowy sposób przetwarzania danych osobowych.

§ 34

Dokument niniejszy obowiązuje od dnia jego zatwierdzenia przez administratora danych.

Załączniki:

- *Arkusz DPIA (załącznik nr 1),*
- *Arkusz analizy ryzyka (załącznik nr 2),*
- *Umowa powierzenia przetwarzania danych osobowych (załącznik nr 3),*
- *Przykładowe klauzule (załącznik nr 4),*
- *Wzór upoważnienia (załącznik nr 5),*
- *Wykaz pomieszczeń, w których dopuszczalne jest przetwarzania danych (załącznik nr 6),*
- *Rejestr osób upoważnionych (załącznik nr 7),*
- *Raport z naruszenia ochrony danych osobowych (załącznik nr 8),*
- *Rejestr naruszeń bezpieczeństwa (załącznik nr 9),*
- *Zbiory danych (załącznik nr 10),*
- *Zgłoszenie naruszenia do UODO (załącznik nr 11),*
- *Komunikat o naruszeniu (załącznik nr 12),*
- *Instrukcja Zarządzania Systemem Informatycznym (załącznik nr 13),*
- *Instrukcja postępowania w sytuacji naruszenia danych (załącznik nr 14),*

- *Upoważnienie do otwierania i zamykania budynku (załącznik nr 15),*
- *Rejestr wydanych kluczy (załącznik nr 16).*

Dokument Sporządzono: **Data: 17.09.2018 r.** **Miejsce: Łódź**	**Pełen podpis Administratora Danych**	**Pieczęć**