



**POLITYKA BEZPIECZEŃSTWA OCHRONY
I
PRZETWARZANIA DANYCH OSOBOWYCH
W**

Niepubliczne Przedszkole i Żłobek „Niezapominajka”

Monika Gorgosz

ul. Podgórna 26, ul. Sportowa 1, 63-300 Pleszew

Pieczęć firmowa:	Podpis Administratora Danych Osobowych:	Data:
NIEPUBLICZNE PRZEDSZKOLE I ŻŁOBEK "NIEZAPOMINAJKA" Monika Gorgosz ul. Podgórna 26, 63-300 Pleszew NIP:6172062125 R-n:362090480	Monika Gorgosz	23 maja 2018

Wstęp

Realizując konstytucyjne prawo każdej osoby do ochrony życia prywatnego oraz postanowienia rozporządzenia Parlamentu Europejskiego i Rady (UE) 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) 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, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ww. rozporządzenia oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, wprowadza się następujący zestaw procedur.

Powyższy wstęp określa założenia ustawodawcy przewidziane w art. 47 oraz art. 51 Konstytucji RP jak również treść art. 32 rozporządzenia ogólnego o ochronie danych osobowych, który nakazuje każdemu administratorowi danych wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający zidentyfikowanemu ryzyku.

Rozdział 1

Postanowienia ogólne

§ 1. Ilekroć w dokumencie jest mowa o:

- 1) **rozporządzeniu** – rozumie się przez to rozporządzenie Parlamentu Europejskiego i Rady (UE) 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);
- 2) **danych osobowych** – 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;
- 3) **zbiorze 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;
 - 4) **przetwarzaniu 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;
 - 5) **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
 - 6) **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
 - 7) **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
 - 8) **administratorze danych** – 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;
 - 9) **zgodzie 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;

- 10) **odbiorcy 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;
- 11) **państwie trzecim** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego;
- 12) **środkach technicznych i organizacyjnych** – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych;
- 13) **ograniczeniu przetwarzania** – należy przez to rozumieć oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
- 14) **profilowaniu** – 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;
- 15) **pseudonimizacji** – 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;
- 16) **podmiocie przetwarzającym** – oznacza to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

17) **naruszeniu 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.

Powyżej określono katalog definicji wynikający z art. 4 rozporządzenia

Rozdział 2

Administrator danych

§ 2. Administrator danych w szczególności:

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, 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.
2. Jeżeli obowiązek ten ma zastosowanie – prowadzi rejestr czynności przetwarzania.
3. Jeżeli obowiązek ten ma zastosowanie – wyznacza Inspektora Ochrony Danych (IOD).

Zgodnie z art. 24 rozporządzenia.

Rozdział 3

Obszar przetwarzania danych osobowych

Obszarem przetwarzania danych osobowych w Niepublicznym Przedszkolu i Żłobku „Niezapominajka” są pomieszczenia w budynku posadowionym przy ul. Sportowej 1 w Pleszewie oraz pomieszczenia w budynku posadowionym przy ul. Podgórnej 26, wykazane w niżej zamieszczonej tabeli.

Lp.	Adres – budynek	Pomieszczenia
1.	ul. Sportowa 1, 63-300 Pleszew	gabinet dyrektora, sekretariat, księgowość, pokój nauczycielski, sale zajęć, składnica akt

2.	ul. Podgórna 26, 63-300 Pleszew	Wyznaczone pomieszczenie biurowe
----	---------------------------------	----------------------------------

Rozdział 4

Zbiory danych przetwarzanych w Jednostce

1. Zbiory danych osobowych przetwarzanych tradycyjnie w formie papierowej

Nr zbioru	NAZWA ZBIORU	STRUKTURA ZBIORU
1	Akta osobowe	PESEL/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/płeć/adres stały/ numer telefonu/ e-mail/ dowód osobisty (seria i nr, wydany przez, data wydania)/ imię ojca/ imię matki/ stan cywilny i rodzinny /stosunek do służby wojskowej (dokument wojskowy, seria i numer, stopień wojskowy)/ numer legitymacji służbowej/ posiada gospodarstwo rolne/ emeryt/rencista/obywatelstwo obce/ osoba kontaktowa/ wykształcenie/ nazwa szkoły i rok ukończenia/ warunki zatrudnienia/ staż pracy/ historia pracy, kary, nagrody/tytuł zawodowy/zawód wyuczony i wykonywany/ uzyskane kwalifikacje/ nieobecności w pracy
2	Ewidencja akt osobowych	imię i nazwisko
3	Orzeczenia lekarskie	PESEL/ imię i nazwisko/ adres stały/ informacje o stanie zdrowia
4	Karty zasiłkowe	PESEL/NIP/imię i nazwisko/ data urodzenia/okresy niezdolności do pracy/wysokość zasiłków
5	Kartoteka zarobkowa	imię i nazwisko/wysokość zarobków
6	Informacje o zarobkach (PIT- y)	PESEL/NIP/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ adres stały/wysokość

		zarobków
7	Zaświadczenia	PESEL/NIP/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ adres stały/wysokość zarobków/ nr dowodu osobistego
8	Dokumentacja ubezpieczeniowa	PESEL/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ adres stały/ informacje o stanie zdrowia
9	Arkusz organizacyjny	PESEL/imię i nazwisko/ staż pracy/ tytuł zawodowy/ ukończone kursy/ uzyskane kwalifikacje/ zawód wyuczony i zawód wykonywany/ warunki zatrudnienia/ nieobecności w pracy
10	Dokumentacja awansów zawodowych nauczycieli	imię i nazwisko/ data i miejsce urodzenia/ adres stały/ wykształcenie/ historia pracy/ uzyskane kwalifikacje
11	Dokumentacja dzieci i ich rodziców – prawnych opiekunów	PESEL/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/płeć /adres stały /numer telefonu/ e-mail/ dowód osobisty (seria, nr i rodzaj, wydany przez, data wydania)/ imię i nazwiska rodziców (opiekunów prawnych), adresy rodziców (opiekunów prawnych)/ stan cywilny/numer obywatelstwo obce/osoba kontaktowa/ wykształcenie/ historia nauki/ nazwa szkoły i rok ukończenia/ numer konta/ wyznanie/ informacje o stanie zdrowia
12	Ewidencja dzieci	PESEL/imię i nazwisko/ data i miejsce urodzenia/adres stały imię, nazwiska i adresy rodziców (opiekunów prawnych)
13	Dzienniki przebiegu zajęć	PESEL/imię i nazwisko/ data i miejsce urodzenia/płeć /adres stały (miejscowość, ulica, numer domu, numer mieszkania/ imię i nazwiska rodziców (opiekunów prawnych), adresy i numer

	POLITYKA BEZPIECZEŃSTWA OCHRONY I PRZETWARZANIA DANYCH OSOBOWYCH
	<i>Niepubliczne Przedszkole i Żłobek "Niezapominajka" Monika Gorgosz Pleszew</i>

		telefonu rodziców (opiekunów prawnych)/ nieobecności /uzyskane wyniki
14	Karta zdrowia ucznia	PESEL/imię i nazwisko/ data i miejsce urodzenia/ adres/ imiona rodziców/ informacje o stanie zdrowia
15	Orzeczenie o niepełnosprawności	imię i nazwisko/data i miejsce urodzenia/PESEL/ rodzaj i nr dokumentu tożsamości/adres zamieszkania/ stopień i symbol niepełnosprawności/wskazania/ uzasadnienie
16	Orzeczenie o potrzebie kształcenia specjalnego	imię i nazwisko wnioskodawcy oraz ucznia/data i miejsce urodzenia ucznia/adres zamieszkania/klasa/ imiona i nazwiska rodziców(opiekunów prawnych) oraz ich adres zamieszkania stopień upośledzenia/ diagnoza/zalecenia/uzasadnienie
17	Zaświadczenie lekarskie	imię i nazwisko/data urodzenia/PESEL/dziecka/ informacja o stanie zdrowia

2. Zbiory danych osobowych przetwarzanych w systemie informatycznym

Administrator danych posiada następujące systemy informatyczne:

Nr zbioru	NAZWA ZBIORU - PROGRAMU INFORMATYCZNE GO	STRUKTURA ZBIORU
18	Program do rozliczania ZUS	PESEL/ NIP/ imię (imiona) i nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ płeć/adres stały/ numer telefonu/ e-mail/ dowód osobisty (seria i nr, wydany przez, data wydania)/ imię ojca/ imię matki/ stan cywilny i rodzinny/ numer legitymacji służbowej/ posiada gospodarstwo rolne/ emeryt/ rencista/

		obywatelstwo obce/ dane osoby kontaktowej/ wykształcenie/ nazwa szkoły i rok ukończenia/ staż pracy/ historia pracy/ warunki zatrudnienia/ wysokość wynagrodzenia /ukończone kursy/ kary i nagrody/ nieobecności w pracy/ informacja o karalności/ informacje o stanie zdrowia
19	PŁATNIK	PESEL/ NIP/ imię/nazwisko/ adres/ data i miejsce urodzenia
20	Mała Księgowość RP	PESEL/ NIP/ imię/nazwisko/ adres/ data i miejsce urodzenia/ numer konta bankowego
21	SIO	PESEL/płeć/wykształcenie/ nazwa szkoły i rok ukończenia/ warunki zatrudnienia/ staż pracy/ historia pracy, kary, nagrody/ tytuł zawodowy/ zawód wyuczony i wykonywany/ uzyskane kwalifikacje/ nieobecności w pracy
22	OPTIVUM - Sekretariat	PESEL/imię i nazwisko/ data i miejsce urodzenia/ płeć/adres stały /numer telefonu/e-mail/ dowód osobisty (seria, numer i rodzaj, wydany przez, data wydania)/ imiona, nazwiska i adresy rodziców (opiekunów prawnych)/ stan cywilny/
23	OBIEG	PESEL/ imię (imiona) i nazwisko/ imiona rodziców/ adres/ data i miejsce urodzenia
24	OPTIVUM - Rekrutacja	PESEL/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ płeć/adres stały (miejscowość, ulica, numer domu, numer mieszkania)/ imię, nazwiska i adresy rodziców (opiekunów prawnych)/uzyskane oceny

Rozdział 5

Środki techniczne i organizacyjne

§ 3. W celu ochrony danych spełniono wymogi, o których mowa w rozporządzeniu, w szczególności:

- a) przeprowadzono ocenę skutków dla ochrony danych,
- b) przeprowadzono analizę ryzyka w stosunku do zasobów biorących udział w poszczególnych procesach,
- c) do przetwarzania danych zostały dopuszczone wyłącznie osoby upoważnione przez administratora danych;
- d) zawarto umowy powierzenia przetwarzania danych,
- e) została opracowana i wdrożona niniejsza polityka bezpieczeństwa.

§ 4. W celu ochrony danych osobowych stosuje się następujące środki ochrony fizycznej danych osobowych:

- a) zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi,
- b) zbiory danych osobowych przechowywane są w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat;
- c) pomieszczenia, w których przetwarzane są zbiory danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy;
- d) dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych, jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony;
- e) dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych, przez całą dobę jest nadzorowany przez służbę ochrony;
- f) zbiory danych osobowych w formie papierowej przechowywane są w zamkniętej niemetalowej szafie;
- g) kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętej niemetalowej szafie;
- h) pomieszczenia, w których przetwarzane są zbiory danych osobowych, zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i wolnostojącej gaśnicy;

- i) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

§ 5. 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) zastosowano urządzenia typu UPS, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania;
- c) dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej/komputerze przenośnym, zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła;
- d) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
- e) zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych;
- f) zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych;
- g) zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity;

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

- a) wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych;
- b) zastosowano 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) zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego;

§ 7. W celu ochrony danych osobowych stosuje się następujące środki organizacyjne:

- a) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych;
- b) przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego;
- c) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
- d) monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane;

Rozdział 6

Procedura DPIA

(Data Protection Impact Assessment)

§ 8. Ocenę skutków dla ochrony danych osobowych (DPIA) przeprowadza każdorazowy właściciel procesu wskazany przez administratora danych;

§ 9. 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.

§ 10. 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 7

Procedura analizy ryzyka i plan postępowania z ryzykiem

§ 11. Analizę ryzyka dla zasobów biorących udział w procesach przeprowadza każdorazowy właściciel procesu wskazany przez administratora danych lub administrator danych samodzielnie z wykorzystaniem odpowiednich narzędzi;

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

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

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

§ 15. Administrator danych nie może zlekceważyć ryzyk, których wartość przekracza ryzyko w stosunku do zasobu, biorącego udział w procesie wysokiego ryzyka zgodnie z wynikiem DPIA zgodnie z narzędziem pracy.

Analiza ryzyka związanego z przetwarzaniem danych osobowych

FORMA PRZETWARZANIA DANYCH	ZAGROŻENIA
dane przetwarzane w sposób tradycyjny	- oszustwo, kradzież, sabotaż; - zdarzenia losowe (powódź, pożar); - zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej); - niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; - pokonanie zabezpieczeń fizycznych; - podsłuchy, podglądy; - brak rejestrowania udostępniania danych; - niewłaściwe miejsce i sposób przechowywania dokumentacji;
dane przetwarzane w systemach informatycznych	- niewłaściwa administracja systemem; - niewłaściwa konfiguracja systemu; - zniszczenie (sfalszowanie) kont użytkowników; - kradzież danych kont; - pokonanie zabezpieczeń programowych; - zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej); - niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; - zdarzenia losowe (powódź, pożar); - niekontrolowane wytwarzanie i wpływ danych poza obszar przetwarzania z pomocą nośników informacji i

	komputerów przenośnych; - naprawy i konserwacje systemu lub sieci teleinformatycznej wykonywane przez osoby nieuprawnione; - przypadkowe bądź celowe uszkodzenie systemów i aplikacji informatycznych lub sieci; - przypadkowe bądź celowe modyfikowanie systemów i aplikacji informatycznych lub sieci; - przypadkowe bądź celowe wprowadzenie zmian do chronionych danych osobowych
--	---

Rozdział 8

Procedura współpracy z podmiotami zewnętrznymi

§ 16. Każdorazowe skorzystanie z usług podmiotu przetwarzającego jest poprzedzone zawarciem umowy powierzenia przetwarzania danych osobowych;

§ 17. 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 9

Procedura domyślnej ochrony danych

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

§ 19. 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 10

Procedura zarządzania incydentami

§ 20. W każdym przypadku naruszenia ochrony danych osobowych administrator danych weryfikuje, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

§ 21. 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.

§ 22. 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.

§ 23. Administrator danych dokumentuje naruszenia, które skutkują naruszeniem praw i wolności osób fizycznych.

Rozdział 11

Procedura realizacji praw osób

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

§ 25. 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 niepodlegania decyzjom oparte wyłącznie na profilowaniu.

§ 26. 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.

§ 27. 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 12

Procedura odbierania zgód oraz informowania osób

§ 28. W każdym przypadku pobierania danych bezpośrednio od osoby, której dane dotyczą, administrator danych informuje osobę, której dane dotyczą.

§ 29. 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.

§ 30. W każdym przypadku odbierania zgody od osoby, której dane dotyczą, korzysta się z klauzul zgody.

Rozdział 13

Postanowienia końcowe

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

§ 32. Dokument niniejszy obowiązuje od dnia jego zatwierdzenia przez administratora danych.

Załączniki do polityki:

1. Lista kontrolna zgodności RODO,
2. Rejestr czynności przetwarzania danych osobowych,
3. Analiza przetwarzania danych osobowych,
4. Arkusz inwentaryzacji zasobów,
5. Dokumentacja dotycząca ochrony danych osobowych i ich przetwarzania.