Polityka bezpieczeństwa przetwarzania danych osobowych
w

Rozdział 1
Postanowienia ogólne

§ 1
Celem Polityki bezpieczeństwa przetwarzania danych osobowych, zwanej dalej „Polityką bezpieczeństwa" w ……., zwanej dalej „Organizacją", jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe.

§ 2
Polityka bezpieczeństwa została opracowana w oparciu o wymagania zawarte w:

- Rozporządzeniu 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 /Dz. Urz. UE.L nr 119, str.1/,
- Ustawie z dnia 29 sierpnia 2017 r. o ochronie danych osobowych /Dz. U. z 2002 r.,Nr 101, poz.926 i Nr 153, poz. 1271 oraz z 2014 r. Nr 25, poz. 219 i Nr 33, poz. 285./,

§ 3
Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników proporcjonalne i adekwatne do ryzyka naruszenia bezpieczeństwa danych osobowych przetwarzanych w ramach prowadzonej działalności.

§ 4

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Organizacji rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest akceptowalna wielkość ryzyka związanego z ochroną danych osobowych.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

a) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
b) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
c) rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
d) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
e) dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
f) zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

§ 5

1. Administratorem danych osobowych przetwarzanych w ..... jest ……..

Rozdział 2
Definicje

§ 6
Przez użyte w Polityce bezpieczeństwa określenia należy rozumieć:

1. **administrator danych osobowych –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,
2. **inspektor ochrony danych** – osoba wyznaczona przez administratora danych osobowych, nadzorująca przestrzeganie zasad i wymogów ochrony danych osobowych określonych w RODO i przepisach krajowych,
3. **RODO** – rozporządzenie Parlamentu Europejskiego i Rady /UE/ 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str. 1/,
4. **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,
5. **zbiór danych osobowych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów,
6. **przetwarzane danych –** operacja lub zestaw operacji wykonywanych na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, łączenie, przesyłanie, zmienianie, udostępnianie i usuwanie, niszczenie, itd.,
7. **system informatyczny –** zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych,
8. **system tradycyjny** – zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych osobowych na papierze,
9. **zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
10. **administrator systemu informatycznego** – osoba lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi,
11. **odbiorca –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m. in. o umowę powierzenia,
12. **strona trzecia –** osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, które z upoważnienia administratora danych osobowych mogą przetwarzać dane osobowe,
13. **identyfikator użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
14. **hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Rozdział 3
Zakres stosowania

§ 7

1. W Organizacji przetwarzane są dane osobowe …… */ np. pracowników, pracowników młodocianych, kandydatów do pracy, klientów/* zebrane w zbiorach danych osobowych.
2. *Informacje te są przetwarzane zarówno w postaci dokumentacji tradycyjnej, jak i elektronicznej.* */*/*
3. Polityka bezpieczeństwa zawiera uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

4. *Innymi dokumentami regulującymi ochronę danych osobowych w Organizacji są:* [*/]

1) rejestr czynności przetwarzania danych osobowych,
2) procedura alarmowa w przypadku naruszenia ochrony danych osobowych,
3) .....

§ 8
Politykę bezpieczeństwa stosuje się w szczególności do:

1. danych osobowych przetwarzanych w systemie: ……..(*należy wskazać wszystkie systemy w których przetwarzane są dane osobowe np. Symfonia, Płatnik, Microsoft Office itp*.),
2. wszystkich informacji dotyczących danych …… */wymienić wszystkie podmioty, których dane są przetwarzane np. pracownicy, klienci, członkowie/,*
3. odbiorców danych osobowych, którym przekazano dane osobowe do przetwarzania w oparciu o umowy powierzenia */np. biuro rachunkowe, specjalistyczna przychodnia lekarska/,*
4. informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
5. rejestru osób trzecich */np. pracownicy/* mających upoważnienia administratora danych osobowych do przetwarzania danych osobowych,
6. innych dokumentów zawierających dane osobowe.

§ 9

1. Zakresy ochrony danych osobowych określone przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty mają zastosowanie do:

1. wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie,
2. wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
3. wszystkich pracowników, stażystów, …….. i innych osób mających dostęp do informacji podlegających ochronie.

2. Do stosowania zasad określonych przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty zobowiązani są wszyscy pracownicy, stażyści, ... oraz inne osoby mające dostęp do danych osobowych podlegających ochronie.

Rozdział 4
Wykaz zbiorów danych osobowych

§ 10
1. Dane osobowe gromadzone są w zbiorach *(należy wymienić wszystkie zbiory danych osobowych przetwarzane w Organizacji, podane poniżej nazwy zbiorów i ich podział są przykładowe):*

1. *Ewidencja osób upoważnionych do przetwarzania danych osobowych,*
2. *Akta osobowe pracowników,*
3. *Zbiory informacji o pracownikach, oświadczenia na potrzeby ZFŚS,*
4. *Ewidencja zwolnień lekarskich,*
5. *Skierowania na badania okresowe, specjalistyczne,*
6. *Ewidencja urlopów, czasu pracy, wyjść,*
7. *Kartoteki wydanej odzieży ochronnej i środków ochrony indywidualnej,*
8. *Rejestr delegacji służbowych,*
9. *Listy płac pracowników,*
10. *Deklaracje ubezpieczeniowe pracowników,*

11. *Deklaracje i kartoteki ZUS pracowników,*
12. *Deklaracje podatkowe pracowników,*
13. *Rejestr wypadków,*
14. *Umowy cywilno-prawne,*
15. *Umowy zawierane z kontrahentami,*
16. *Rejestr klientów,*
17. *Dokumenty archiwalne,* */*/*
18. *……*
19. *……*

§ 11
Zbiory danych osobowych wymienione w § 10 ust. 1 pkt …… podlegają przetwarzaniu w sposób tradycyjny, a zbiory określone w pkt ……..... gromadzone są i przetwarzane przy użyciu systemu informatycznego ……..

Rozdział 5
Wykaz budynków, pomieszczeń, w których wykonywane są operacje przetwarzania danych osobowych

§ 12
1. Dane osobowe przetwarzane są w budynku, mieszczącym się w ..... przy ulicy .....

1.	pomieszczenia, w których przetwarzane są dane osobowe (wskazanie konkretnych nr pomieszczeń)	*np. pokój nr 1, 2, 3, 4 sekretariat*
2.	pomieszczenia, w których znajdują się komputery stanowiące element systemu informatycznego	*np. pokój nr 1, 2*
3.	Pomieszczenia, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe)	*np. pokój nr 1, 2, 3*
4.	pomieszczenia, w których składowane są uszkodzone komputerowe nośniki danych (taśmy, dyski, płyty CD, dyski przenośne, uszkodzone komputery)	*np. pokój 3*
5.	pomieszczenia archiwum	*np. pokój 4*

Rozdział 6 */*/*
Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

§ 13

Lp.	Zbiór danych	Dział/ jednostka organizacyjna	Program	Lokalizacja bazy danych	Miejsce przetwarzania danych
1.					
2.					
3.					
4.					
5.					
6.					

Rozdział 7 */*/*
Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych

§ 14
Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych dla programów i systemów stosowanych w Organizacji przedstawia się w sposób następujący:

PRZYKŁAD

1. *Program Kancelaryjny*

1. *Nazwa firmy,*
2. *Nr wpisu,*
3. *Imię,*
4. *Nazwisko,*
5. *Województwo,*
6. *Miejsce zamieszkania,*
7. *Miejscowość zamieszkania,*
8. *Adres do korespondencji,*
9. *Tel,*
10. *Fax,*
11. *e-mail,*
12. *Tel komórkowy,*
13. *Data wpisu,*
14. *Data urodzenia,*
15. *Numer legitymacji służbowej.*

Rozdział 8 */*/*
Sposób przepływu danych między poszczególnymi systemami, współpracy systemów informatycznych ze zbiorami danych

§ 15
Przepływ danych pomiędzy poszczególnymi systemami

Program 1	Przepływ	Program 2	Przepływ danych
Office	<->	……	brak
Office	<->	……	brak
Office	<->	……	brak
……	<->	……	brak
……	<->	……	brak
……	<->	……	brak

/Można zapisać te przepływy również w formie graficznej/

Rozdział 9
Środki organizacyjne i techniczne zabezpieczenia danych osobowych

§ 16

1. Zabezpieczenia organizacyjne

1. opracowano i wdrożono Politykę bezpieczeństwa przetwarzania danych osobowych,
2. sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Organizacji,
3. stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych,
4. **opracowano i bieżąco prowadzi się rejestr czynności przetwarzania** */*/*
5. ..... */wymienić inne dokumenty jeśli je wdrożono/*
6. **wyznaczono inspektora ochrony danych,** */*/*
7. do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych bądź osobę przez niego upoważnioną,
8. osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego,
9. osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,
10. przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
11. przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych,
12. dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonuje się takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści.

2. Zabezpieczenia techniczne

1. wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą ……..*(proszę wskazać rozwiązania zapewniające bezpieczeństwo np. wykorzystanie urządzenia stanowiącego bramę DNS, FireWall itp.),*
2. stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową,
3. komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanie zmiany hasła,

3. Środki ochrony fizycznej:

1. obszar, na którym przetwarzane są dane osobowe, poza godzinami pracy, chroniony jest alarmem,
2. obszar, na którym przetwarzane są dane osobowe objęty jest całodobowym monitoringiem,
3. urządzenia służące do przetwarzania danych osobowych umieszczone są w zamykanych pomieszczeniach,
4. dokumenty i nośniki informacji zawierające dane osobowe przechowywane są w zamykanych na klucz szafach.

Rozdział 10
Zadania administratora danych osobowych lub inspektora ochrony danych (jeśli *został powołany)*

§ 17
Do najważniejszych obowiązków administratora danych osobowych lub administratora bezpieczeństwa informacji należy:

1. organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami RODO i ustawy o ochronie danych osobowych,

2. zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki bezpieczeństwa i innymi dokumentami wewnętrznymi,
3. przeprowadzenie oceny skutków planowanej operacji przetwarzania dla ochrony danych osobowych – w przypadku, gdy organizacja wprowadza nowy rodzaj przetwarzania danych osobowych,
4. wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,
5. prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
6. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
7. nadzór nad bezpieczeństwem danych osobowych,
8. kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
9. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

Rozdział 11 */*/*
Zadania administratora systemu informatycznego *(o ile został powołany/zatrudniony np. informatyk)*

§ 18

1. Administrator systemu informatycznego odpowiedzialny jest za:

1. bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
2. optymalizację wydajności systemu informatycznego, instalacje i konfiguracje sprzętu sieciowego i serwerowego,
3. instalacje i konfiguracje oprogramowania systemowego, sieciowego,
4. konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem,
5. nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
6. współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
7. zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
8. zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
9. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
10. przyznawanie na wniosek administratora danych osobowych lub inspektora ochrony danych ściśle określonych praw dostępu do informacji w danym systemie,
11. wnioskowanie do administratora danych osobowych lub inspektora ochrony danych w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń,
12. zarządzanie licencjami, procedurami ich dotyczącymi,
13. prowadzenie profilaktyki antywirusowej.

2. Praca administratora systemu informatycznego jest nadzorowana pod względem przestrzegania RODO, ustawy o ochronie danych osobowych, ... oraz Polityki bezpieczeństwa Organizacji przez administratora danych lub inspektora ochrony danych.

Rozdział 12 */*/*
Sprawozdanie roczne z funkcjonowania systemu ochrony danych osobowych
§ 19

1. Corocznie do dnia …… inspektor ochrony danych */jeśli został powołany/* przygotowuje sprawozdanie roczne z funkcjonowania systemu ochrony danych osobowych i przekazuje do administratora danych osobowych.
2. Sprawozdanie przygotowywane jest w formie pisemnej.

Rozdział 13
Postanowienia końcowe

§ 20

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada administrator danych osobowych lub inspektor ochrony danych*(o ile został powołany)*.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz Polityką bezpieczeństwa i innymi związanymi z nią dokumentami obowiązującymi u administratora danych osobowych,
4. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.