Polityka bezpieczeństwa przetwarzania danych osobowych
w EVAPFLEX SP. Z O.O. w 41-800 ZABRZE UL. KNUROWSKA 8

Rozdział 1
Postanowienia ogólne

§ 1

Celem Polityki bezpieczeństwa przetwarzania danych osobowych w EVAPFLEX SP. Z O.O. zwanej dalej „Polityką bezpieczeństwa", jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe.

§ 2

Polityka bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w ustawie z 29 sierpnia 1997 r. o ochronie danych osobowych oraz rozporządzeniu ministra spraw wewnętrznych i administracji z 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.

§ 3

Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników.

§ 4

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w EVAPFLEX SP.Z O.O. rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   1) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
   2) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
   4) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
   5) dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
   6) 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 EVAPFLEX SP. Z O.O. jest Sylwester Ratuszny -Prezes Zarządu
2. Administrator danych osobowych powołuje administratora bezpieczeństwa informacji, którego zadania określa § 17.

Rozdział 2
Definicje

§ 6

Przez użyte w Polityce bezpieczeństwa określenia należy rozumieć:

1) **administrator danych osobowych –** rozumie się EVAPFLEX SP. Z O.O. w 41-800 ZABRZE UL. KNUROWSKA 8;
2) **administrator bezpieczeństwa informacji (także ABI)** – rozumie się przez to osobę wyznaczoną przez administratora danych osobowych, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
3) **ustawa** – rozumie się przez to ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz.U. z 2016 r. poz. 922);
4) **rozporządzenie** – rozporządzenie ministra spraw wewnętrznych i administracji z 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);
5) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
6) **zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
7) **przetwarzane danych –** rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
8) **system informatyczny –** rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
9) **system tradycyjny** – rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
10) **zabezpieczenie danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
11) **administrator systemu informatycznego** – rozumie się przez to osobę lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi;
12) **użytkownik** – rozumie się przez to upoważnionego przez administratora danych osobowych lub administratora bezpieczeństwa informacji (o ile został powołany), wyznaczonego do przetwarzania danych osobowych pracownika;
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 EVAPFLEX SP. Z .O. przetwarzane są w szczególności dane osobowe : IMIĘ I NAZWISKO, NUMER TELEFONU, E-MAIL zebrane w zbiorach danych osobowych.
2. Informacje te są przetwarzane zarówno w postaci dokumentacji tradycyjnej, jak i elektronicznej.
3. Polityka bezpieczeństwa zawiera dokumenty dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.
4.

§ 8

Politykę bezpieczeństwa stosuje się w szczególności do:

1) danych osobowych przetwarzanych w systemie: MICROSOFT OFFICE wszystkich informacji dotyczących danych IMIĘ I NAZWISKO, NUEMR TELEFONU, E-MAIL;
2) wszystkich danych IMIĘ I NAZWISKO, NUEMR TELEFONU, E-MAIL;
3) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych;
4) rejestru osób dopuszczonych do przetwarzania danych osobowych;
5) innych dokumentów zawierających dane osobowe.

§ 9

1. Zakresy ochrony danych osobowych określone przez dokumenty Polityki bezpieczeństwa mają zastosowanie do systemów informatycznych, w których są przetwarzane dane osobowe, a w szczególności 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, i innych osób mających dostęp do informacji podlegających ochronie.
2. Do stosowania zasad określonych przez dokumenty Polityki bezpieczeństwa zobowiązani są wszyscy pracownicy, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie.

Rozdział 4

Wykaz zbiorów danych osobowych

§ 10

1 . Dane osobowe gromadzone są w zbiorach (należy wymienić wszystkie zbiory danych osobowych przetwarzane w podmiocie, podane poniżej nazwy zbiorów są przykładowe):

1) *Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych;*
2) *Kontrola zarządcza – wyniki, opracowania, protokoły, notatki;*
3) *Akta osobowe pracowników;*
4) *Dokumentacja dotycząca polityki kadrowej – opiniowanie awansów, wyróżnień, odznaczeń, nagród, wnioski o odznaczenia, itp;*
5) *Notatki służbowe oraz postępowanie dyscyplinarne;*
6) *Zbiory informacji o pracownikach, oświadczenia na potrzeby ZFŚS;*
7) *Ewidencja zwolnień lekarskich;*
8) *Skierowania na badania okresowe, specjalistyczne;*
9) *Ewidencja urlopów, karty czasu pracy;*
10) *Kartoteki wydanej odzieży ochronnej i środków ochrony indywidualnej;*
11) *Rejestr delegacji służbowych;*
12) *Ewidencja osób korzystających z funduszu socjalnego i dokumentacja;*
13) *Listy płac pracowników;*
14) *Kartoteki zarobkowe pracowników, nakazy komornicze;*
15) *Deklaracje ubezpieczeniowe pracowników;*
16) *Deklaracje i kartoteki ZUS pracowników;*
17) *Deklaracje podatkowe pracowników;*
18) *Księga uczniów;*
19) *Arkusze ocen;*
20) *Karty zgłoszeń uczniów, podania o przyjęcie do szkoły;*
21) *Dzienniki zajęć obowiązkowych i dodatkowych;*
22) *Zaświadczenia z PPP i inne orzeczenia i opinie;*
23) *Ewidencje decyzji administracyjnych dyrektora szkoły – skreślenia z listy;*
24) *Deklaracje uczęszczania na religię, sprzeciw od zajęć z wychowania seksualnego;*
25) *Ewidencja decyzji – zwolnienia z obowiązkowych zajęć, odroczenia obowiązku szkolnego;*
26) *Rejestr zaświadczeń wydanych pracownikom szkoły;*
27) *Rejestr wypadków, ewidencja podejrzeń o chorobę zawodową, itp;*
28) *Księga druków ścisłego zarachowania;*
29) *Zbiór upoważnień;*
30) *Ewidencja osób przystępujących do egzaminów zewnętrznych – Hermes;*
31) *Umowy zawierane z osobami fizycznymi;*
32) *Protokoły rad pedagogicznych, księga uchwał;*
33) *Dokumenty archiwalne;*
34) *Teczki awansu zawodowego;*
35) *Arkusz organizacyjny placówki;*
36) *Pomoc społeczna – MOPS, stypendia, wyprawki, obiady;*
37) *……*
38) *……*

§ 11

Zbiory danych osobowych wymienione w § 10 ust. 1 pkt 1-36 podlegają przetwarzaniu w sposób tradycyjny oprócz zbiorów określonych w pkt 1-36., które gromadzone są i przetwarzane przy użyciu systemu informatycznego MICROSOFT OFFICE

Rozdział 5
Wykaz budynków, pomieszczeń i stref do przetwarzania danych osobowych

§ 12

1. Dane osobowe przetwarzane są w budynku, mieszczącym się w Katowicach przy ulicy Rymera 3/3 oraz Zabrzu przy ulicy Knurowskiej 8

1.	Wykaz pomieszczeń, w których przetwarzane są dane osobowe (wskazanie konkretnych nr pomieszczeń)	*pokój nr 53 oraz 49*
2.	Wykaz pomieszczeń, w których znajdują się komputery stanowiące element systemu informatycznego	*pokój nr 53 oraz 49*
3.	Wykaz pomieszczeń, 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)	*pokój nr 53 oraz 49*
4.	Wykaz pomieszczeń, w których składowane są uszkodzone komputerowe nośniki danych (taśmy, dyski, płyty CD, dyski przenośne, uszkodzone komputery)	*pokój 53 oraz 49*
5.	Wykaz pomieszczeń archiwum	*pokój 53 oraz 49*
6.	Wykaz programów, w których przetwarzane są dane osobowe	*Microsoft Office*
7.	Wykaz podmiotów zewnętrznych, które mają dostęp do danych osobowych lub je przetwarzają na podstawie podpisanych umów (np. informatyk) – nazwa firmy, imię, nazwisko, adres, funkcja.	
8.	Inne (proszę podać inne informacje dotyczące pomieszczeń, w których przetwarzane są dane osobowe oraz ich zabezpieczeń).	*pokoje zamykane na klucz, budynek chroniony, komputery z indywidualnymi hasłami*

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.	Dane osobowe	Evapflex Sp. Z o.o.	Microsoft Office	Pokój nr 53 oraz 49	Pokój nr 53 oraz 49
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 Evapflex Sp. Z o.o. przedstawia się w sposób następujący:

PRZYKŁADY

1. ***Program Kancelaryjny***

1) *Grupa,*
2) *Nazwa firmy,*
3) *Nr wpisu,*
4) *Imię,*
5) *Nazwisko,*
6) *Miejsce wykonywania czynności doradztwa podatkowego,*
7) *Miejscowość wykonywania czynności doradztwa podatkowego,*
8) *Województwo,*
9) *Zawieszenie od,*
10) *Zawieszenie do,*
11) *Miejsce zamieszkania,*
12) *Miejscowość zamieszkania,*
13) *Adres do korespondencji,*
14) *Tel,*
15) *Fax,*
16) *e-mail,*
17) *Tel komórkowy,*
18) *Data wpisu,*
19) *Data urodzenia,*
20) *Numer legitymacji,*
21) *Konto na składki,*

2. ***Program Comarch Optima Finanse I Księgowość***

Dla modułu Finanse i Księgowość systemu można wyróżnić następujące tabele i widoki (w schemacie bazy danych w przestrzeni nazw [FK]) służące przechowaniu danych ksiąg rachunkowych:

1) Okres,
2) Data okresu,
3) Opis,

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

§ 15

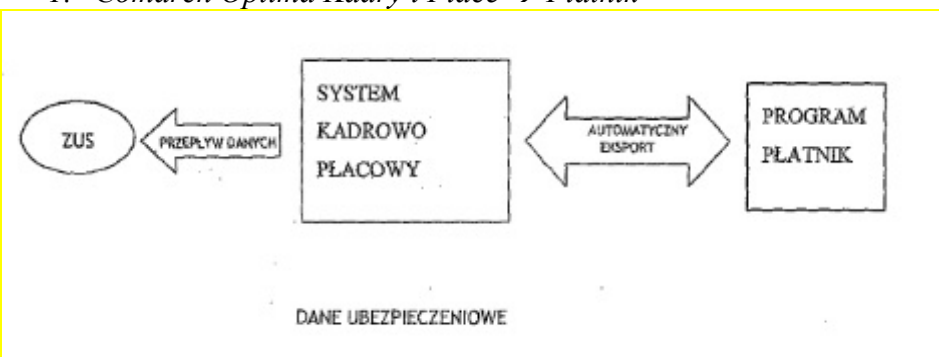
Przepływ danych pomiędzy poszczególnymi systemami

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

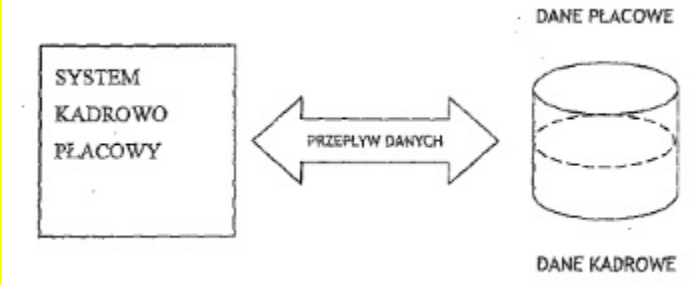
Można zapisać to też w formie graficznej

PRZYKŁADY

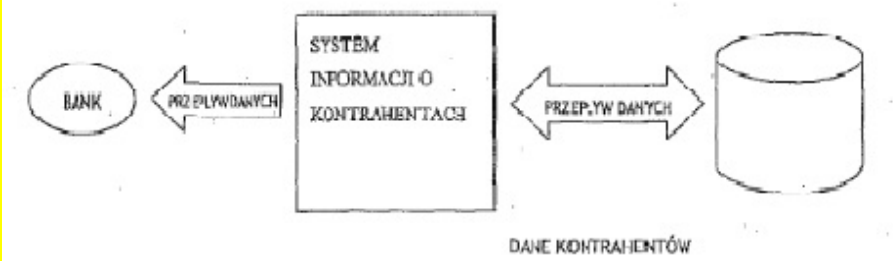
1. *Comarch Optima Kadry i Płace → Płatnik*



2. *Comarch Optima Kadry i Płace*



3. *Comarch Optima Finanse i Księgowość*



Rozdział 9
Środki techniczne i organizacyjne zabezpieczenia danych osobowych

§ 16

1. Zabezpieczenia organizacyjne
   1) sporządzono i wdrożono Politykę bezpieczeństwa;
   2) sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
   3) stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych;
   4) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
   5) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
   6) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
   7) 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;
   8) dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób.
2. Zabezpieczenia techniczne
   1) wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą Fire Wall stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową,

2) 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 umieszcza się w zamykanych pomieszczeniach.

Rozdział 10
Zadania administratora danych osobowych lub administratora bezpieczeństwa informacji
(w zależności czy ABI został powołany)

§ 17

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

1) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych,
2) zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki,
3) wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,
4) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
5) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych, prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
6) nadzór nad bezpieczeństwem danych osobowych,
7) kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
8) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

Rozdział 11
Zadania administratora systemu nformatycznego
(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 administratora bezpieczeństwa informacji ściśle określonych praw dostępu do informacji w danym systemie;
11) wnioskowanie do administratora danych osobowych lub administratora bezpieczeństwa informacji 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 ustawy o ochronie danych osobowych, rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 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 oraz Polityki bezpieczeństwa przez administratora danych lub administratora bezpieczeństwa informacji.

Rozdział 12
Szkolenia użytkowników

§ 19

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 ABI *(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 instrukcjami obowiązującymi u administratora danych osobowych, a także o zobowiązaniu się do ich przestrzegania.

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.
5. Dokument ten jest przechowywany w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

Rozdział 14
Postanowienia końcowe

§ 20

1. Administrator danych osobowych lub administrator bezpieczeństwa informacji *(o ile został powołany)* ma obowiązek zapoznać z treścią Polityki każdego użytkownika.
2. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
3. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.
4. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
5. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
6. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy oraz rozporządzenia.