Pracownia Rozwoju Osobistego
Organizacja Pożytku Publicznego
ul. Plac Oleandrów 8
45-220 Opole

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W STOWARZYSZENIU PRACOWNIA ROZWOJU OSOBISTEGO

Pracownia Rozwoju Osobistego
Organizacja Pożytku Publicznego
ul. Plac Oleandrów 8
45-220 Opole

ROZDZIAŁ I
Postanowienia ogólne

§ 1.

1. Polityka bezpieczeństwa przetwarzania danych osobowych w Stowarzyszeniu Pracownia Rozwoju Osobistego zwana dalej „Polityką bezpieczeństwa", określa podstawowe zasady dotyczące zapewnienia bezpieczeństwa w zakresie danych osobowych przetwarzanych w zbiorach danych:

a) tradycyjnych, w szczególności aktach osobowych, wykazach, zbiorach ewidencyjnych; dokumentacji rekrutacyjno-zgłoszeniowej, dokumentacji realizowanych usług,

b) w systemach informatycznych, w szczególności deklaracje ZUS, ewidencje płacowe, informacje skarbowe, ewidencje statystyczne, ewidencje i dokumentacja realizowanych usług.

2. Ilekroć w Polityce Bezpieczeństwa jest mowa o:

a) ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych z dnia 29 sierpnia 1997r. (tekst jedn. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.);

b) stowarzyszeniu – rozumie się Stowarzyszenie Pracownia Rozwoju Osobistego

c) Administratorze danych osobowych – rozumie się Prezesa Stowarzyszenia Pracownia Rozwoju Osobistego

d) Administratorze systemu – rozumie się osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych, służących do przetwarzania danych osobowych;

e) nośniki danych osobowych – płyty CD lub DVD, pamięć flash, dyski twarde lub inne urządzenia/materiały służące do przechowywania plików z danymi;

f) osoba upoważniona (użytkownik) – osoba posiadająca upoważnienie wydane przez Administratora danych osobowych ;

g) Administrator Bezpieczeństwa Informacji – osoba powołana zarządzeniem Administratora danych osobowych, której zadaniem jest nadzorowanie i koordynowanie w Stowarzyszeniu Pracownia Rozwoju Osobistego zasad postępowania przy przetwarzaniu danych osobowych

h) dane osobowe - w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

i) przetwarzanie 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;

j) zbiór danych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów;

k) system informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

l) identyfikator użytkownika (login) - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

m) hasło - ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

n) uwierzytelnianie — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

o) poufności danych — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

§ 2.

1. Administrator danych osobowych realizując politykę bezpieczeństwa dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

a) przetwarzane zgodnie z prawem;
b) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane przetwarzaniu niezgodnemu z tymi celami;
c) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą.

2. Administrator danych osobowych dąży do systematycznego unowocześniania stosowanych w firmie informatycznych, technicznych i organizacyjnych środków ochrony tych danych w celu zabezpieczenia danych osobowych przed ich udostępnianiem osobom nieupoważnionym, przetwarzaniem z naruszeniem przepisów o ochronie danych osobowych, nieautoryzowaną zmianą, uszkodzeniem lub zniszczeniem.

ROZDZIAŁ II
Wykaz zbiorów danych osobowych

§ 3.

Dane osobowe gromadzone są w zbiorach. Wykaz zbiorów danych osobowych stanowi załącznik nr 1.

§ 4.

Zbiory danych osobowych wymienione w załączniku nr 1 podlegają przetwarzaniu w sposób tradycyjny oprócz zbiorów Nr 2, 3, 4 i 7, które gromadzone są i przetwarzane przy użyciu systemów informatycznych.

ROZDZIAŁ III
Wykaz pomieszczeń, w których przetwarzane są dane osobowe.

§ 5.

1. Dane osobowe gromadzone i przetwarzane są z użyciem sprzętu komputerowego oraz metodą tradycyjną w siedzibie firmy w pomieszczeniach wskazane w załączniku nr 2.
2. Zabrania się przetwarzania danych poza obszarami wskazanymi określonym w załączniku nr 2.
3. Przebywanie osób, nieuprawnionych w obszarach wskazanych w załączniku nr 2 w czasie przetwarzania danych osobowych jest dopuszczalne za zgodą Administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych – za jego zgodą.

ROZDZIAŁ IV
Ewidencja osób upoważnionych do przetwarzania danych osobowych

§ 6.

1. Ewidencja osób, które mają dostęp do zbiorów danych osobowych prowadzona jest w formie Rejestru upoważnień do przetwarzania danych osobowych, który stanowi załącznik nr 3.
2. Ewidencja zawiera: imię i nazwisko osoby upoważnionej, datę nadania i ustania uprawnień.
3. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie. Wzór upoważnienia stanowi załącznik nr 4.
4. Unieważnienie upoważnienia następuje na piśmie, wg wzoru stanowiącego załącznik nr 5.
5. Każdy upoważniony do przetwarzania danych potwierdza pisemnie fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa. Wzór potwierdzenia stanowi załącznik nr 6.

ROZDZIAŁ V
Opis zdarzeń naruszających ochronę danych osobowych

§ 7.

Rodzaje zagrożeń naruszających ochronę danych osobowych:

1. Zagrożenia losowe:

a) zewnętrzne np. klęski żywiołowe, przerwy w zasilaniu – ich wystąpienie może prowadzić do utraty integralności danych lub ich zniszczenia lub uszkodzenia infrastruktury technicznej systemu: ciągłość zostaje naruszona, jednak nie dochodzi do naruszenia danych osobowych;

b) wewnętrzne np. niezamierzone pomyłki operatorów, awarie sprzętowe, błędy oprogramowania – w wyniku ich wystąpienia może dojść do zniszczenia danych, może nastąpić zakłócenie ciągłości pracy systemu i naruszenia poufności danych.

2. Zagrożenia zamierzone (świadome i celowe naruszenia poufności danych) – w wyniku ich wystąpienia zazwyczaj nie występuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy. W ramach tej kategorii zagrożeń wystąpić mogą:

a) nieuprawniony dostęp do systemu z zewnątrz;
b) nieuprawniony dostęp do systemu z wewnątrz;
c) nieuprawnione przekazanie danych;
d) bezpośrednie zagrożenie materialnych składników np. kradzież, zniszczenie.

3. Okoliczności zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to w szczególności:

a) sytuacje losowe lub nieprzewidywalne oddziaływanie czynników zewnętrznych na zasoby systemu np. wybuch gazu, pożar, zalanie pomieszczeń, uszkodzenia wskutek prowadzonych prac remontowych;

b) niewłaściwe parametry środowiska np. nadmierna wilgotność, temperatura, wstrząsy, oddziaływania pola elektromagnetycznego, przeciążenia napięcia;

c) awarie sprzętu lub oprogramowania, które są celowym działaniem na potrzeby naruszenia ochrony danych osobowych;

d) pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub niepożądaną modyfikację w systemie;

e) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;

f) modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia;

g) ujawnienie osobom nieuprawnionym danych osobowych lub objętych tajemnicą procedur ochrony ich przetwarzania;
h) podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub skasowanie bądź skopiowanie w sposób niedozwolony danych osobowych;
i) rażące naruszenie obowiązków w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowywanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce lub kserokopiarce, niewykonanie kopii zapasowych, prace na danych osobowych w celach prywatnych itp.);
j) nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych, znajdujących się na dyskach, płytach CD, kartach pamięci oraz wydrukach komputerowych w formie niezabezpieczonej (otwarte szafy, biurka, regały, archiwum).

4. W przypadku stwierdzenia naruszenia zasad bezpieczeństwa danych osobowych sporządza się raport oraz przedstawia się go Administratorowi danych.

ROZDZIAŁ VI
Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych

§ 8.

1. Formy zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe:

a) wszystkie pomieszczenia, w których przetwarzane są dane osobowe zamykane są na klucz, w przypadku opuszczenia przez ostatnia osobę upoważnioną do przetwarzania danych osobowych – także w godzinach pracy;
b) dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (pamięć flash, płyty CD, DVD, dyskietki) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, a tam, gdzie jest to możliwe w szafach pancernych lub metalowych;
c) nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarkach;
d) budynki, w którym są przetwarzane dane jest chroniony systemem alarmowym z telefonicznym powiadamianiem.

§ 9.

1. Formy zabezpieczeń przed nieautoryzowanym dostępem do danych osobowych:

a) podłączenie urządzenia końcowego (komputera, drukarki) do sieci firmy dokonywane jest przez Administratora systemu;
b) udostępnianie użytkownikowi zasobów sieci zawierających dane osobowe przez Administratora systemu następuje na podstawie upoważnienia do przetwarzania danych osobowych;
c) identyfikacja użytkownika w systemie następuje poprzez zastosowanie uwierzytelniania (login, hasło; dot. danych przetwarzanych przy użyciu systemu informatycznego);
d) udostępnianie kluczy do pomieszczeń, w których przetwarzane są dane osobowe tylko osobom upoważnionym;
e) ustawienie monitorów na stanowiskach pracy w sposób uniemożliwiający wgląd w dane osobowe (dot. danych przetwarzanych przy użyciu systemu informatycznego).

f) miejsce użytkowania komputerów przenośnych na których przetwarzane są dane osobowe ogranicza się tylko i wyłącznie do pomieszczeń wskazanych w załączniku nr 2 do „Polityki bezpieczeństwa".

§ 10.

1. Formy zabezpieczeń przed utratą danych osobowych w wyniku awarii:

a) odrębne zasilanie sprzętu komputerowego – do przetwarzania danych osobowych używane są komputery przenośne standardowo wyposażone w baterię/akumulator;

b) zastosowanie ochrony antywirusowej

§ 11.

1. Organizację ochrony danych osobowych realizuje się poprzez:

a) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych

b) przed dopuszczeniem do pracy;

c) kontrolowanie pomieszczeń budynku;

d) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;

e) wyznaczenie Administratora Bezpieczeństwa Informacji.

ZAŁĄCZNIKI:

1. *Wykaz zbiorów danych osobowych przetwarzanych w Stowarzyszeniu Pracownia Rozwoju Osobistego*
2. *Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym są przetwarzane dane osobowe w Stowarzyszeniu Pracownia Rozwoju Osobistego*
3. *Rejestr upoważnień do przetwarzania danych osobowych w Stowarzyszeniu Pracownia Rozwoju Osobistego*
4. *Wzór upoważnienia do przetwarzania danych osobowych Stowarzyszenia Pracownia Rozwoju Osobistego*
5. *Wzór odwołania upoważnienia do przetwarzania danych osobowych Stowarzyszenia Pracownia Rozwoju Osobistego*
6. *Oświadczenia pracowników Stowarzyszenia Pracownia Rozwoju Osobistego o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych*
7. *Instrukcja bezpieczeństwa przetwarzania danych osobowych w Stowarzyszeniu Pracownia Rozwoju Osobistego.*