Polityka bezpieczeństwa przetwarzania danych osobowych „RODO”

w Zakładzie Produkcyjno-Usługowo-Handlowym „STOL-BUD” Zbigniew Witkowski ul. Lubawska 25, 13-220 Rybno

Rozdział 1

Postanowienia ogólne

§ 1

Celem Polityki bezpieczeństwa przetwarzania danych osobowych, zwanej dalej „Polityką bezpieczeństwa” w Zakładzie Produkcyjno-Usługowo-Handlowym „STOL-BUD” Zbigniew Witkowski ul. Lubawska 25, 13-220 Rybno, zwanej dalej „Firmą”, 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/,
- Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. 2016 r. poz. 922) (uodo).
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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. Nr 100, poz. 1024).
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 roku w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz.U., poz. 1934).
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U., poz. 745).
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U., poz. 719).
- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2016 r., poz. 113).

§ 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 Firmie 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:

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 ZPUH „STOL-BUD” Zbigniew Witkowski jest Zbigniew Witkowski – właściciel.
2. Administrator danych osobowych nie powołał inspektora ochrony danych, zgodnie art. 37 RODO. Zadania inspektora ochrony danych zawarte w art. 39 RODO są realizowane przez Administratora Danych Osobowych.

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 Firmie przetwarzane są dane osobowe 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. Załącznikami do Polityki bezpieczeństwa są :

- Wykaz zbiorów danych osobowych.
- Wykaz budynków
- Oświadczenie o przestrzeganiu zasad i przepisów ochrony danych osobowych i o zachowaniu tajemnicy danych osobowych.
- Karta szkolenia wstępnego z zakresu ochrony danych osobowych.
- Upoważnienie do przetwarzania danych osobowych.
- Wykaz udostępnień danych osobowych innym podmiotom
- Wykaz podmiotów zewnętrznych, którym powierzono dane do przetwarzania.
- Rejestr działań zapobiegawczych i korygujących.
- Analiza organizacyjna środków bezpieczeństwa informacji.
- Raport z naruszenia ochrony danych.
- Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu.
- Ewidencja osób upoważnionych do przetwarzania danych osobowych.
- Rejestr czynności przetwarzania danych osobowych
- Klauzule informacyjne dla poszczególnych zbiorów danych osobowych
- Wzór umowy powierzenia przetwarzania danych osobowych
- Wykaz programów informatycznych wykorzystywanych w ZPUH „STOL-BUD" Zbigniew Witkowski

4. Innymi dokumentami regulującymi ochronę danych osobowych w Firmie są:

ZASADY UŻYTKOWANIA ZASOBÓW KOMPUTEROWYCH I SIECI KOMUNIKACYJNEJ

§ 8

Politykę bezpieczeństwa stosuje się w szczególności do:

1. danych osobowych przetwarzanych w systemie: Fakt, Microsoft Office, Płatnik System Obsługi Dofinansowań PFRON, Bankowość elektroniczna, poczta elektroniczna
2. wszystkich informacji dotyczących danych : pracowników, kandydatów do pracy, kontrahentów, klientów
3. odbiorców danych osobowych, którym przekazano dane osobowe do przetwarzania w oparciu o umowy powierzenia : specjalistyczna przychodnia lekarska (lekarz medycyny pracy)
4. informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
5. rejestru osób trzecich *(pracowników)* 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:

1.1 wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie,
1.2 wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
1.3 wszystkich pracowników, stażystów i innych osób mających dostęp do informacji podlegających ochronie.
1.4 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

1. ***Ewidencja osób upoważnionych do przetwarzania danych osobowych,***
2. ***Akta osobowe pracowników,***
3. ***Zbiór kandydatów do pracy***
4. ***Zbiór zwolnień lekarskich,***
5. ***Ewidencja urlopów, czasu pracy,***
6. ***Kartoteki wydanej odzieży ochronnej i środków ochrony indywidualnej,***
7. ***Listy płac pracowników,***
8. ***Deklaracje ubezpieczeniowe pracowników,***
9. ***Deklaracje i kartoteki ZUS pracowników,***
10. ***Deklaracje podatkowe pracowników,***
11. ***Rejestr wypadków,***
12. ***Umowy cywilno-prawne,***
13. ***Umowy zawierane z kontrahentami,***
14. ***Rejestr klientów,***
15. ***Rejestr pracowników zgłoszonych do ubezpieczenia grupowego***
16. ***Dokumenty archiwalne,***
17. ***Zbiór dokumentów księgowych – zakupu***
18. ***Zbiór dokumentów księgowych – sprzedaży***
19. ***Zbiór zamówień od klientów***

§ 11

Zbiory danych osobowych wymienione w § 10 ust. 1 pkt 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 podlegają przetwarzaniu w sposób tradycyjny, a zbiory określone w pkt 4, 5, 7, 8, 9, 10, 12, 14, 15, 16, 17, 18, 19 gromadzone są i przetwarzane przy użyciu systemu informatycznego wykazanego w § 8 pkt. 1.

Rozdział 5

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

§ 12

1. Dane osobowe przetwarzane są w budynku, mieszczącym się w Rybnie przy ulicy Lubawskiej 25.

1.	pomieszczenia, w których przetwarzane są dane osobowe	Pomieszczenia sekretariatu, księgowości i archiwum
2.	pomieszczenia, w których znajdują się komputery stanowiące element systemu informatycznego	Pomieszczenia sekretariatu i księgowości
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)	Pomieszczenia sekretariatu, księgowości i archiwum
4.	pomieszczenia, w których składowane są uszkodzone komputerowe nośniki danych (taśmy, dyski, płyty CD, dyski przenośne, uszkodzone komputery)	Pomieszczenia sekretariatu, księgowości i archiwum
5.	pomieszczenia archiwum	Pomieszczenie archiwum

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.	***Ewidencja osób upoważnionych do przetwarzania danych osobowych,***	Dział księgowości	Forma papierowa		Pomieszczenia księgowości
2.	***Akta osobowe pracowników***	Dział księgowości	Forma papierowa		Pomieszczenia księgowości
3.	***Zbiór kandydatów do pracy***	Dział księgowości	Forma papierowa		Pomieszczenia księgowości

4,	***Zbiór zwolnień lekarskich***	Dział księgowości	Forma papierowa, Pue ZUS		Pomieszczenia księgowości
5.	***Ewidencja urlopów, czasu pracy***	Dział księgowości	FAKT, Forma papierowa		Pomieszczenia księgowości
6.	***Kartoteki wydanej odzieży ochronnej i środków ochrony indywidualnej***	Dział BHP	Forma papierowa		Pomieszczenia księgowości
7.	***Listy płac pracowników***	Dział księgowości	Fakt, forma papierowa		Pomieszczenia księgowości
8.	***Deklaracje ubezpieczeniowe pracowników***	Dział księgowości	Płatnik, forma papierowa		Pomieszczenia księgowości
9.	***Deklaracje i kartoteki ZUS pracowników***	Dział księgowości	Płatnik, forma papierowa		Pomieszczenia księgowości
10.	***Deklaracje podatkowe pracowników***	Dział księgowości	Fakt, forma papierowa		Pomieszczenia księgowości
11.	***Rejestr wypadków***	Dział BHP	forma papierowa		Pomieszczenia księgowości
12.	***Umowy cywilno-prawne***	Dział księgowości	Fakt, forma papierowa		Pomieszczenia księgowości
13.	***Umowy zawierane z kontrahentami,***	Dział księgowości	forma papierowa		Pomieszczenia księgowości
14.	***Rejestr klientów***	Dział sprzedaży, Dział księgowości	Exel, Fakt, forma papierowa		Pomieszczenia księgowości, pomieszczenia sekretariatu
15.	***Rejestr pracowników zgłoszonych do ubezpieczenia grupowego***	Dział księgowości	Płatnik, forma papierowa		Pomieszczenia księgowości
16.	***Dokumenty archiwalne***	Archiwum, Dział księgowości	Fakt, Płatnik, Office, forma papierowa		Pomieszczenia księgowości

17.	***Zbiór dokumentów księgowych – zakupu***	Dział księgowości	Fakt, forma papierowa, platforma Ministerstwa Finansów		Pomieszczenia księgowości
18.	***Zbiór dokumentów księgowych – sprzedaży***	Dział księgowości	Fakt, forma papierowa, platforma Ministerstwa Finansów		Pomieszczenia księgowości
19.	***Zbiór zamówień od klientów***	Dział sprzedaży	Exel, poczta elektroniczna, forma papierowa		Pomieszczenia sekretariatu

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 Firmie przedstawia się w sposób następujący:

1. *Program Płatnik:* Imię i nazwisko, adres zamieszkania, adres do korespondencji, data urodzenia, PESEL, płeć, stopień niepełnosprawności
2. *Program FAKT:* Imię i nazwisko, adres zamieszkania, adres do korespondencji, data urodzenia, PESEL, płeć, stopień niepełnosprawności; Nazwa firmy, NIP, REGON, siedziba firmy, nr r-ku bankowego
3. *Microsoft Office:* Imię i nazwisko, adres zamieszkania, adres do korespondencji, data urodzenia, PESEL, płeć, stopień niepełnosprawności; Nazwa firmy, NIP, REGON, siedziba firmy
4. *System Obsługi Dofinansowań PFRON:* Imię i nazwisko, adres zamieszkania, adres do korespondencji, data urodzenia, PESEL, płeć, stopień niepełnosprawności
5. *Bankowość elektroniczna:* Imię i nazwisko, adres zamieszkania, Nazwa firmy, siedziba firmy, nr r-ku bankowego
6. *Poczta elektroniczna:* Nazwa firmy, NIP, REGON, siedziba firmy, nr r-ku bankowego, imię i nazwisko, nr telefonu, adres poczty elektronicznej

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	Poczta elektroniczna	Office	Zamówienia klientów przesyłane pomiędzy pracownikami firmy
Fakt – dane z modułu moduł sprzedaży	Poczta elektroniczna	Fakt – zaimportowanie faktur sprzedaży do programu księgowego	Faktury sprzedaży wystawione dla klientów
Fakt	Bramka Ministerstwa Finansów	Platforma Ministerstwa Finansów	Deklaracje podatkowe, pliki JPK
Płatnik	Serwer systemu Płatnik ZUS	System Płatnik - ZUS	Deklaracje ZUA, ZZA, ZCNA, ZWUS, ZIUA, DRA, RCA i RSA
System Obsługi Dofinansowań PFRON	Serwer PFRON	System PFRON	Miesięczne raporty zatr. osób niepełnosprawnych
Bankowość elektroniczna	Serwer Banku	Bankowość elektroniczna	Dane zawarte w przelewach

Rozdział 9

Środki organizacyjne i techniczne zabezpieczenia danych osobowych

§ 16

1. Zabezpieczenia organizacyjne:

1.1 opracowano i wdrożono Politykę bezpieczeństwa przetwarzania danych osobowych,
1.2 sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Firmie,
1.3 stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych,
1.4 opracowano i bieżąco prowadzi się rejestr czynności przetwarzania
1.5 do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych bądź osobę przez niego upoważnioną,
1.6 osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego,
1.7 osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,
1.8 przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,

1.9 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,
1.10 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:

2.1 wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą – hasło dostępu do sieci
2.2 stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową,
2.3 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:

3.1 urządzenia służące do przetwarzania danych osobowych umieszczone są w zamykanych pomieszczeniach,
3.2 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 pełni Administrator Danych Osobowych

§ 18

1. Administrator Danych Osobowych odpowiedzialny jest za :

   1.1 bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
   1.2 optymalizację wydajności systemu informatycznego, instalacje i konfiguracje sprzętu sieciowego i serwerowego,
   1.3 instalacje i konfiguracje oprogramowania systemowego, sieciowego,
   1.4 konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem,
   1.5 nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
   1.6 współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
   1.7 zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
   1.8 zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
   1.9 przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
   1.10 przyznawanie przez administratora danych osobowych lub inspektora ochrony danych ściśle określonych praw dostępu do informacji w danym systemie,
   1.11 zarządzanie licencjami, procedurami ich dotyczącymi,
   1.12 prowadzenie profilaktyki antywirusowej.

Rozdział 12

Sprawozdanie roczne z funkcjonowania systemu ochrony danych osobowych

§ 19

1. Corocznie do dnia 30 czerwca każdego roku Administrator Danych Osobowych przygotowuje sprawozdanie roczne z funkcjonowania systemu ochrony 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
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.

Właściciel

Zbigniew Witkowski