Polityka bezpieczeństwa przetwarzania danych osobowych „RODO”
w „STOL-BUD” Marcin Witkowski ul. Lubawska 25a, 13-220 Rybno

Rozdział 1
Postanowienia ogólne

§ 1

Celem Polityki bezpieczeństwa przetwarzania danych osobowych, zwanej dalej „Polityką bezpieczeństwa” w „STOL-BUD” Marcin Witkowski ul. Lubawska 25a, 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 „STOL-BUD” Marcin Witkowski jest Marcin 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 „STOL-BUD”
Marcin 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 25a. 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