**POLITYKA BEZPIECZEŃSTWA**

**PRZETWARZANIA DANYCH OSOBOWYCH**

**ROZDZIAŁ I**

**POSTANOWIENIA OGÓLNE**

**§ 1**

Celem Polityki bezpieczeństwa przetwarzania danych osobowych, zwanej dalej „Polityką bezpieczeństwa” u **Katarzyny Kaźmierczak**, prowadzącej działalność gospodarczą pod nazwą : **Poznaj Duszę Katarzyna Kaźmierczak**, ul. Fabryczna 16A, 62-030 Luboń, zwaną dalej Przedsiębiorcą, 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/.

**§ 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 u Przedsiębiorcy 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 :
3. poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
4. integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
5. rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
6. integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej,
7. dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
8. 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**

Administratorem danych osobowych przetwarzanych u Przedsiębiorcy jest Katarzyna Kaźmierczak.

**ROZDZIAŁ II**

**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 III**

**ZAKRES ZASTOSOWANIA**

**§ 7**

1. U przedsiębiorcy przetwarzane są  dane klientów zebrane w zbiorach danych osobowych.
2. Informacje te są przetwarzane zarówno w postaci dokumentacji elektronicznej.
3. Polityka bezpieczeństwa zawiera uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.
4. Innymi dokumentami regulującymi ochronę danych osobowych u Przedsiębiorcy są:
   1. instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych u Przedsiębiorcy,
   2. instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych,
   3. regulamin ochrony przetwarzania danych osobowych.

**§ 8**

Politykę bezpieczeństwa stosuje się w szczególności do:

1. odbiorców danych osobowych, którym przekazano dane osobowe do przetwarzania w oparciu o umowy powierzenia*,*
2. informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
3. innych dokumentów zawierających dane osobowe.

**§ 9**

Zakresy ochrony danych osobowych określone przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty mają zastosowanie do wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych, w których przetwarzane są dane osobowe podlegające ochronie,

**ROZDZIAŁ IV**

**WYKAZ ZBIORÓW DANYCH OSOBOWYCH**

**§ 10**

1. Dane osobowe gromadzone są w zbiorach w szczególności :
   1. umów zawieranych z kontrahentami,
   2. rejestru klientów.

**§ 11**

Zbiory danych osobowych wymienione w §  10 podlegają przetwarzaniu przy użyciu systemu informatycznego.

**ROZDZIAŁ V**

**WYKAZ BUDYNKÓW, POMIESZCZEŃ, W KTÓRYCH WYKONYWANE SĄ OPERACJE PRZETWARZANIA DANYCH OSOBOWYCH**

**§ 12**

Dane osobowe przetwarzane urządzeniach informatycznych.

**ROZDZIAŁ VI**

**ŚRODKI ORGANIZACYJNE I TECHNICZNE ZABEZPIECZENIA DANYCH OSOBOWYCH**

**§ 13**

1. Zabezpieczenia organizacyjne :
2. opracowano i wdrożono Politykę bezpieczeństwa przetwarzania danych osobowych,
3. sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych u Przedsiębiorcy,
4. stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych,
5. przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
6. 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.
7. Zabezpieczenia techniczne :

|  |  |
| --- | --- |
| 1. **środki sprzętowe, informatyczne i telekomunikacyjne (nazwy zwyczajowo przyjęte albo symbole norm lub standardów technicznych)** |  |
| Pomieszczenie, w którym przetwarzane są dane osobowe zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego lub wolnostojącej gaśnicy. | TAK |
| Co najmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest z siecią publiczną (np. Internetem). | TAK |
| Zastosowano urządzenia typu UPS lub generator prądu lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed awarią zasilania. | TAK |
| Użyto system Firewall do ochrony dostępu do sieci komputerowej. | TAK |
| Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej. | TAK |
|  |  |
|  |  |
| 1. **środki ochrony w ramach oprogramowania systemów (nazwy zwyczajowo przyjęte albo symbole norm lub standardów technicznych)** |  |
| Dostęp do zbioru danych osobowych przetwarzanych za pomocą komputera zabezpieczony jest na tym komputerze za pomocą hasła BIOS. | TAK |
| Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. | TAK |
| Zastosowano oprogramowanie zabezpieczające przed nieuprawnionym dostępem do systemu informatycznego. | TAK |
|  |  |
|  |  |
| 1. **środki ochrony w ramach systemu użytkowego (nazwy zwyczajowo przyjęte albo symbole norm lub standardów technicznych)** |  |
| Stacja końcowa umożliwiająca dostęp do zbioru danych osobowych zabezpieczona jest identyfikatorem i hasłem dostępu. | TAK |
| Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe. | TAK |
| Zastosowano mechanizm blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika. | TAK |
|  |  |

**ROZDZIAŁ VII**

**ZADANIA ADMINISTRATORA DANYCH OSOBOWYCH**

**§ 14**

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.