POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH w REMESHOP EU Spółka z ograniczoną odpowiedzialnością

Rozdział 1

Postanowienia ogólne

§ 1.

Celem *Polityki bezpieczeństwa przetwarzania danych osobowych w REMESHOP EU Spółka z ograniczoną odpowiedzialnością*, zwanej dalej „Polityką bezpieczeństwa", w REMESHOP EU Spółka z ograniczoną odpowiedzialnością, zwanej dalej „Spółką", 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:

1) 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 (ogólne rozporządzenie o ochronie danych osobowych) (Dz. Urz. UE L 119 z 04.05.2016, s. 1);
2) ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000).

§ 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 działalności prowadzonej przez Spółkę

§ 4.

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Spółce 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

Administratorem danych osobowych przetwarzanych w Spółce jest Spółka, czyli REMESHOP EU SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOSCIĄ z siedzibą w Warszawie, przy ulicy Mazowieckiej nr 11, lok. 49, 00-052 Warszawa.

Rozdział 2

Definicje

§ 6.

Przez użyte w Polityce bezpieczeństwa określenia należy rozumieć:

1) **administrator danych osobowych –** osoba prawna, która samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
2) **ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000);

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 119 z 04.05.2016, s. 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 Spółce przetwarzane są dane osobowe 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 w Spółce.

§ 8.

Politykę bezpieczeństwa stosuje się w szczególności do:

1) danych osobowych przetwarzanych w systemie: *Microsoft Office* ,CMS Joomla , TorgsoftDB .

2) wszystkich informacji dotyczących danych Klientów sklepu internetowego prowadzonego przez Spółkę;

3) odbiorców danych osobowych, którym przekazano dane osobowe do przetwarzania w oparciu o umowy powierzenia (*np. biuro rachunkowe)*;

4) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych;

5) rejestru osób trzecich mających upoważnienia administratora danych osobowych do przetwarzania danych osobowych (*np. pracownicy)*;

6) innych dokumentów zawierających dane osobowe.

§ 9.

1. Zakresy ochrony danych osobowych określone przez Politykę bezpieczeństwa mają zastosowanie 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 dane osobowe podlegające ochronie;
   3) wszystkich pracowników Spółki i innych osób mających dostęp do danych osobowych podlegających ochronie.
2. Wszyscy pracownicy Spółki i inne osoby mające dostęp do danych osobowych podlegających ochronie zobowiązani są do stosowania zasad określonych przez Politykę bezpieczeństwa.

Rozdział 4

Wykaz zbiorów danych osobowych

§ 10.

Dane osobowe gromadzone są w zbiorach

1) Ewidencja osób upoważnionych do przetwarzania danych osobowych;
2) Umowy cywilno-prawne;
3) Umowy zawierane z kontrahentami;
4) Rejestr klientów;
5) Dokumenty archiwalne;
6) Akta osobowe pracowników;

§ 11.

W Spółce w sposób papierowy przetwarza się zbiory danych osobowych, o których mowa w § 10 pkt …, natomiast zbiory danych osobowych, o których mowa w § 10 pkt … gromadzi się i przetwarza przy użyciu systemu informatycznego

Rozdział 5
Środki organizacyjne i techniczne podjęte do ochrony danych osobowych podczas ich przetwarzania i zabezpieczania

§ 12.

1. Dane osobowe przetwarzane są w budynku, mieszczącym się w 3 Warszawa ,02-548 przy ulicy Grażyny 13/15 lok.310
2. W tym przepisie należy wskazać, gdzie przechowuje się dane osobowe (pomieszczenia, szafy, nośniki, segregatory itp.), osoby, stanowiska itp. które zajmują się porządkowaniem, przechowywaniem danych osobowych itp.

§ 13.

1. Zabezpieczenia organizacyjne:
   1) opracowano i wdrożono Politykę bezpieczeństwa przetwarzania danych osobowych;
   2) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych bądź osobę przez niego upoważnioną;
   3) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
   4) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
   5) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;

6) 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;

7) 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:
   1) wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą *hasłem*;
   2) stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową;
   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:
   1) urządzenia służące do przetwarzania danych osobowych umieszczone są w zamykanych pomieszczeniach;
   2) dokumenty i nośniki informacji zawierające dane osobowe przechowywane są w zamykanych na klucz szafach, do których dostęp posiadają jedynie upoważnieni pracownicy Spółki.

Rozdział 6

Zadania administratora danych osobowych

§ 14.

Do najważniejszych obowiązków administratora danych osobowych:

1) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami RODO i ustawy;
2) zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki bezpieczeństwa;
3) wydawanie pracownikom Spółki i anulowanie upoważnień do przetwarzania danych osobowych;

4) prowadzenie ewidencji pracowników Spółki upoważnionych do przetwarzania danych osobowych;

5) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych;

6) stały nadzór nad bezpieczeństwem danych osobowych.

Rozdział 7

Postanowienia końcowe

§ 20.

1. Każdego pracownika Spółki przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub ze zbiorami danych osobowych przetwarzanych w sposób papierowy należy poddać przeszkoleniu w zakresie ochrony danych osobowych gromadzonych i przetwarzanych w sposób elektroniczny i papierowy.
2. Za przeprowadzenie szkolenia odpowiada administrator danych osobowych.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy i jej aktów wykonawczych oraz z postanowieniami Polityką bezpieczeństwa.
4. Okoliczność odbycia szkolenia pracownik Spółki składa pisemne oświadczenie, w którym potwierdza odbycie szkolenia, i wskazuje datę szkolenia. Pracownik Spółki składa również pisemne oświadczenie, w którym zobowiązuje się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych w Spółce. Oświadczenia składane są następnie do akt osobowych pracownika Spółki.