Polityka bezpieczeństwa przetwarzania danych osobowych

Polityka bezpieczeństwa zawiera zasady dotyczące zabezpieczeń zapewniających ochronę przetwarzanych danych osobowych przez Piotra Sareckiego prowadzącego działalność gospodarczą pod firmą „Trisar”, ul. Lipowa 3/21, 30-704 Kraków, NIP: 6371973496, REGON: 122225380.

§ 1

Definicje

Przez użyte w niniejszej polityce bezpieczeństwa określenia należy rozumieć:

1. **administrator danych osobowych –** Piotr Sarecki prowadzący działalność gospodarczą pod firmą „Trisar”, ul. Lipowa 3/21, 30-704 Kraków, NIP: 6371973496, REGON: 122225380,
2. **ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz.U. z 2016 r. poz. 922),
3. **rozporządzenie** – rozporządzenie ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. 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. z 2004 r. nr 100, poz. 1024),
4. **RODO** – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,
5. **dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określa jących fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,
6. **zbiór danych osobowych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie,
7. **przetwarzanie danych –** operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie

poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,

8. **system informatyczny –** zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych,
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. **użytkownik** – upoważniony przez administratora danych osobowych pracownik, zleceniobiorca, wykonawca umowy o dzieło, wykonawca umowy o świadczenie usług, praktykant lub stażysta wyznaczony do przetwarzania danych osobowych; użytkownikiem może być również administrator danych osobowych,
12. **identyfikator użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
13. **hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

§ 2

Postanowienia ogólne

1. Celem niniejszej polityki bezpieczeństwa jest zapewnienie, aby informacje zawierające dane osobowe były przetwarzane zgodnie z wymogami obowiązujących aktów prawnych.
2. Polityka dotyczy zabezpieczenia danych przetwarzanych we wszystkich systemach informatycznych, zarówno używanych obecnie jak i przyszłych we wszystkich lokalizacjach, w których przetwarzane są dane osobowe.
3. Ochrona danych osobowych realizowana jest poprzez odpowiednie zabezpieczenia, m.in.: fizyczne, organizacyjne, wybrane oprogramowanie, aplikacje oraz użytkowników.
4. Oprócz niniejszej polityki wdrożono także instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych. Określa ona sposób zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w szczególności, aby zapewnić ich bezpieczeństwo.

5. Do stosowania zasad określonych przez Politykę bezpieczeństwa zobowiązani są wszyscy mający dostęp do informacji podlegających ochronie.
6. Polityka bezpieczeństwa nie dotyczy podmiotów zewnętrznych, które przetwarzają dane osobowe powierzone im do przetwarzania przez administratora danych osobowych na podstawie stosownych umów powierzenia. Podmioty te stosują własne procedury i środki bezpieczeństwa związane z ochroną danych osobowych wymagane przez przepisy prawa, do czego zobowiązały się w ramach zawartych umów powierzenia przetwarzania danych osobowych.

§ 3

Administrowanie danymi osobowymi

1. Administratorem danych osobowych jest Piotr Sarecki prowadzący działalność gospodarczą pod firmą „Trisar”, ul. Lipowa 3/21, 30-704 Kraków, NIP: 6371973496, REGON: 122225380.
2. Administrator danych osobowych wykonuje także czynności inspektora ochrony danych osobowych oraz administratora systemów informatycznych.
3. Administrator danych osobowych zapewnia bezpieczeństwo, nadzór i ochronę danych osobowych zgodnie z wymogami obowiązujących przepisów prawa oraz przetwarzanie ich zgodnie z uregulowaniami niniejszej Polityki.
4. Wydaje i anuluje upoważnienia dla osób przetwarzających dane osobowe oraz prowadzi ich rejestr.
5. Administrator danych osobowych prowadzi postępowanie wyjaśniające w przypadku naruszenia ochrony danych osobowych i zgłasza fakt naruszenia organowi nadzorczemu oraz zawiadomienie o tym osobę, której dane dotyczą.
6. Każdy użytkownik, za wyjątkiem administratora danych osobowych, 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.
7. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z obowiązującymi przepisami prawa w zakresie ochrony danych osobowych oraz z instrukcjami obowiązującymi u administratora danych osobowych.

8. Administrator danych osobowych prowadzi stronę https://solvbot.pl w związku z czym dochodzi do przetwarzania danych osobowych zarówno w formie elektronicznej jak i papierowej.
9. Dane osobowe w formie elektronicznej mogą być przetwarzane z dowolnego miejsca i w dowolnym czasie z wykorzystaniem komputerów oraz innych urządzeń przenośnych. Przetwarzanie odbywa się w ramach systemów informatycznych, do których dostęp następuje on-line, a systemy te nie są zainstalowane lokalnie na komputerach. W związku z tym użytkownicy tych systemów stosują odpowiednie procedury zabezpieczające dane osobowe. Dane mogą być także przechowywane na dyskach komputerów.
10. Dane osobowe w formie papierowej przetwarzane są w obrębie siedziby administratora danych osobowych podanej w ust. 1 niniejszego paragrafu.
11. Administrator danych osobowych powierza przetwarzanie niektórych danych osobowych podmiotom trzecim, które zobowiązały się do stosowania odpowiednich środków ochrony i bezpieczeństwa danych osobowych wymaganych przez przepisy prawa.
12. Dane osobowe przetwarzane są przez administratora danych osobowych w ramach następujących zbiorów opisanych w załączniku nr 1:

    1) zbiór „Newsletter”,
    2) zbiór „Faktury”,
    3) zbiór „Umowy”,
    4) zbiór „Korespondencja”,
    5) zbiór „Kontakty”,
    6) zbiór „Komentarze”,
    7) zbiór „Social Media”,

§ 4

Administrator systemu informatycznego

1. Administratora systemu informatycznego powołuje administrator danych osobowych w formie pisemnej. Administrator danych osobowych nadzoruje prace administratora systemu informatycznego. Jeżeli administrator systemu informatycznego nie zostanie powołany, jego zadania wykonuje administrator danych osobowych.

2. Administrator systemu informatycznego odpowiedzialny jest za:

- bieżący monitoring i zapewnienie ciągłości działania komputerów i innych urządzeń wykorzystywanych do przetwarzania danych osobowych oraz systemów operacyjnych,
- optymalizację wydajności komputerów i innych urządzeń wykorzystywanych do przetwarzania danych osobowych oraz systemów operacyjnych,
- instalację i konfiguracje sprzętu sieciowego i serwerowego,
- instalację i konfigurację oprogramowania systemowego, sieciowego,
- konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem,
- nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
- współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego,
- zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
- zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
- przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
- przyznawanie na wniosek administratora danych osobowych ściśle określonych praw dostępu do informacji w danym systemie,
- wnioskowanie do administratora danych osobowych w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń,
- zarządzanie licencjami, procedurami ich dotyczącymi,
- prowadzenie profilaktyki antywirusowej.

§ 5

Zabezpieczenie danych osobowych

1. Przez bezpieczeństwo przetwarzanych danych osobowych rozumie się zapewnienie ich:
    - Poufności - dane nie są udostępniane nieupoważnionym osobom,
    - Rozliczalności - działania osoby może być przypisana w sposób jednoznaczny tylko tej osobie
    - Integralności – dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany
    - Dostępności – osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne

2. System przetwarzania danych jest integralny, co oznacza, że nie jest możliwa żadna manipulacja nim, także zewnętrzna,
3. Wdrożono także zarządzanie ryzykiem poprzez proces identyfikowania, minimalizowania oraz eliminowania ryzyka dotyczącego bezpieczeństwa danych osobowych w systemach zarządzania.
4. W celu zabezpieczenia danych osobowych wdrożono politykę bezpieczeństwa i instrukcję zarządzania systemami informatycznymi.
5. Dane osobowe są przetwarzane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.
6. Wszystkie osoby mające do czynienia z przetwarzaniem danych osobowych zostały zobowiązane do zachowania ich w tajemnicy, a także przeszkolono je w zakresie wymogów prawnych i systemów informatycznych w zakresie zachowania ich bezpieczeństwa.
7. Dokumenty papierowe zawierające dane osobowe przechowywane są w….
8. Zastosowano system Firewall do ochrony dostępu do sieci komputerowej oraz oprogramowanie antywirusowe, a także wygaszacze ekranów.
9. Zastosowano uwierzytelnienie poprzez identyfikator użytkownika oraz hasło przy starcie systemu operacyjnego komputera oraz dostępie do zbioru danych.
10. Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych oraz rejestrujące zmiany dokonywane na elementach zbiorów danych osobowych.
11. Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
12. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych oraz do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.

§ 6

Zgłaszanie i zawiadamianie o naruszeniu ochrony danych osobowych

1. Administrator danych osobowych dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia, jego skutki oraz podjęte środki zaradcze. Dokumentacja odbywa się z wykorzystaniem zestawienia incydentów naruszenia ochrony danych osobowych.
2. Każde naruszenie ochrony danych osobowych powinno być niezwłocznie zgłaszane przez użytkowników administratorowi danych osobowych.
3. Szczegóły w zakresie postępowania w związku ze stwierdzonym naruszeniem ochrony danych osobowych przy korzystaniu z systemów informatycznych opisane zostały w Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.
4. W przypadku naruszenia ochrony danych osobowych na administratorze danych osobowych ciąży obowiązek zgłoszenia tego faktu do organu nadzorczego zgodnie z postanowieniami art. 33 RODO oraz zawiadomienia osoby, której dane dotyczą, zgodnie z postanowieniami art. 34 RODO.

§ 7

Postanowienia końcowe

1. Administrator danych osobowych ma obowiązek zapoznać z treścią Polityki każdego użytkownika.
2. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.
3. Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością karną.

Załącznik nr 1 – opis zbiorów danych osobowych

Zbiór nr 1 – „**Newsletter**”

1. W ramach tego zbioru przetwarzane są dane osobowe osób (adres e-mail, imię), które zapisały się do newslettera.
2. Informacje trafiają do zbioru w wyniku zapisania się do newslettera. Zapis do newslettera odbywa się za pośrednictwem strony internetowej administratora danych osobowych poprzez przesłanie specjalnego formularza zapisu do newslettera. Przesłanie formularza skutkuje zapisaniem danych w bazie.
3. Administrator zawarł z dostawcą systemu mailingowego umowę świadczenia usług mailingowych oraz umowę powierzenia przetwarzania danych osobowych. Dane te przetwarzane są w formie elektronicznej, w ramach systemu mailingowego MailChimp. Dane przechowywane są na serwerze zapewnianym przez dostawcę systemu, tj. Rocket Science Group // 675 Ponce de Leon Ave NE, Suite 5000, Atlanta, GA 30308. Dostawca systemu mailingowego deklaruje spełnienie wszystkich wymogów nakładanych przez RODO, w tym przystąpienie do programu Privacy Shield celem zagwarantowania odpowiedniego poziomu ochrony i bezpieczeństwa danych osobowych zgodnego ze standardami europejskimi.
4. Dostawca systemu mailingowego dane tylko przechowuje, nie modyfikując ich, ale zapewniając do nich dostęp administratorowi. Dane zostaną usunięte w razie podjęcia decyzja o zamknięciu newslettera jak również w razie rezygnacji przez użytkownika z otrzymywania newslettera, co spowoduje usunięcie danych z bazy.
5. Dostęp do systemu mailingowego wymaga zalogowania się z wykorzystaniem identyfikatora użytkownika oraz hasła zdefiniowanych przez administratora. Administrator tworzy oddzielne konta dla wszystkich użytkowników upoważnionych do przetwarzania danych osobowych. Użytkownicy mogą uzyskać dostęp wyłącznie do systemu mailingowego, ale nie są w stanie uzyskać dostępu bezpośrednio do serwera, na którym przechowywane są dane zapisane w systemie.

Zbiór nr 2 – „**Faktury”**

1. W ramach zbioru Faktury przetwarzane są dane osób, dla których została wystawiona faktura.

W zbiorze przetwarzane są następujące informacje

1) imię i nazwisko,
2) adres zamieszkania,
3) firma, numer NIP, adres miejsca wykonywania działalności gospodarczej lub adres siedziby – jeżeli faktura została wystawiona dla przedsiębiorcy.

2. Dane trafiają do zbioru automatycznie w wyniku wyrażenia w trakcie składania zamówienia chęci otrzymania faktury. Dane wprowadzane są również do zbioru manualnie w razie konieczności wystawienia faktury niezwiązanej ze sprzedażą on-line.

3. Dane zostaną usunięte w razie zakończenia prowadzenia działalności gospodarczej przez administratora danych osobowych. Jeżeli użytkownik zażąda usunięcia jego danych osobowych, a usunięcie nie będzie stało w sprzeczności z uzasadnionym celem przetwarzania danych przez administratora, dane również zostaną usunięte z bazy.

4. Jeżeli chodzi o faktury przechowywane w dokumentacji księgowej administratora, to będą one przechowywane przez okres wymagany przez aktualnie obowiązujące przepisy prawa.

Nr 3 - zbiór „**Umowy**”

1. Zbiór Umowy obejmujące dane osób, z którymi administrator zawiera umowy inne niż umowy z współpracownikami oraz inne niż umowy zawierane w ramach sprzedaży on-line.

Dane trafiają do zbioru w wyniku zawarcia umowy z administratorem.

Dane gromadzone, przechowywane i przetwarzane są w formie zbioru umów. Zbiór umów przechowywany jest w siedzibie administratora.

W zbiorze przetwarzane są następujące dane:

1) imię i nazwisko,
2) adres zamieszkania,
3) firma,
4) adres miejsca prowadzenia działalności gospodarczej,
5) numer NIP,
6) numer PESEL,
7) adres e-mail,
8) numer telefonu,
9) numer rachunku bankowego.

2. Umowy są również w formie elektronicznej przechowywane na dysku komputera administratora danych osobowych.
3. Umowy mogą być również kopiowane do chmury Google Drive w ramach automatycznej synchronizacji. Regulamin usługi zawiera postanowienia dotyczące ochrony danych osobowych.

Nr 4 - zbiór „**Komentarze**”,

1. W ramach zbioru Komentarze przetwarzane są dane osób, które dodały komentarz na blogu administratora.

   W zbiorze przetwarzane są następujące informacje:

   1) imię i nazwisko,
   2) adres e-mail,
   3) adres strony internetowej,
   4) adres IP.

2. Informacje trafiają do zbioru w wyniku dodania komentarza. Dodanie komentarza odbywa się za pośrednictwem bloga administratora danych osobowych poprzez przesłanie specjalnego formularza w ramach systemu Disqus. Przesłanie formularza skutkuje zapisaniem danych w bazie.
3. Dane przetwarzane są w formie elektronicznej, w ramach systemu komentarzy Disqus. Ponieważ użytkownik korzysta z systemu Disqus na podstawie umowy o świadczenie usług drogą elektroniczną zawieraną z Disqus Inc., Disqus Inc. jest niezależnym administratorem danych osobowych w stosunku do administratora.
4. Dane przetwarzane są również w systemie Wordpress i przechowywane na serwerze zapewnianym przez koi.pl Z podmiotem tym administrator zawarł umowę powierzenia przetwarzania danych osobowych. Podmiot ten zobowiązał się do utrzymywania w trakcie trwania powierzenia odpowiednich środków ochrony i bezpieczeństwa danych osobowych wymaganych przez aktualnie obowiązujące przepisy prawa.
5. Dostęp do systemu Disqus oraz Wordpress wymaga zalogowania się z wykorzystaniem identyfikatora użytkownika oraz hasła zdefiniowanych przez administratora. Administrator tworzy oddzielne konta dla wszystkich użytkowników upoważnionych do przetwarzania danych osobowych. Użytkownicy mogą uzyskać dostęp wyłącznie do systemu Disqus, ale nie są w stanie uzyskać dostępu bezpośrednio do serwera, na którym przechowywane są dane zapisane w tym systemie. W odniesieniu do systemu Wordpress, Użytkownicy mogą uzyskać dostęp zarówno do systemu, jak i do serwera, na którym przechowywane są dane zapisane w systemie, przy czym odczytanie danych bezpośrednio z serwera nie jest możliwe, ponieważ zapisane są one w systemie plików odczytywanym przez system Wordpress.
6. Dane zostaną usunięte w razie zakończenia funkcjonowania bloga.

Nr 5 – zbiór „**Media społecznościowe**”

1. W ramach zbioru Media społecznościowe przetwarzane są dane osób, które obserwują administratora w mediach społecznościowych; Facebook, Instagram, inne.

   W zbiorze przetwarzane są następujące informacje:

1) imię i nazwisko,
2) wizerunek (zdjęcie profilowe)

2. Dostęp do danych wymaga zalogowania się na konto administratora w serwisach społecznościowych. Zalogowanie wymagania podania nazwy użytkownika oraz hasła.
3. Dane osobowe przechowywane są w bazach podmiotów trzecich, nad którymi administrator nie ma kontroli.
4. Administrator utraci dostęp do danych w ramach listy, gdy dana osoba przestanie go obserwować itp. lub gdy zadecyduje o zamknięciu danego profilu społecznościowego.

Nr 6 - zbiór „**Kontakty**”

1. W ramach zbioru „Kontakty” przetwarzane są dane osób zapisanych jako kontakty w książkach adresowych. Dane te są przetwarzane w związku z kontaktami realizowanymi za pomocą środków porozumiewania się na odległość.
2. Książki adresowe mogą mieć formę elektroniczną lub pisemną. Te w formie elektronicznej przechowywane są na dysku komputera lub w innych urządzeniach wykorzystywanych do przetwarzania danych osobowych.
3. W zbiorze przetwarzane są następujące dane:

a)imię i nazwisko,
b)adres e-mail,
c)numer telefonu.

4. Kontakty mogą być usuwane z książek adresowych na bieżąco, lub być przechowywane przez dłuższy czas niemożliwy do określenia z góry.

Pozostałe przypadki przetwarzania danych osobowych

1. Administrator dołożył najwyższej staranności, by zidentyfikować wszystkie procesy przetwarzania danych osobowych funkcjonujące w ramach jego organizacji, wyodrębniając jednocześnie zbiory danych osobowych, w ramach których dane są przetwarzane. Dane osobowe mogą być jednak przetwarzane incydentalnie również poza zbiorami, w szczególności w następujących sytuacjach:

   1) Korzystanie ze skrzynki pocztowej e-mail

2) Korzystanie z systemu Mailchimp

3) Korzystanie z systemu Microsoft Ofiice

4) Korzystanie z systemu Google: docs, gmail

5) Drukowanie dokumentów zawierających dane osobowe

2. W każdym przypadku incydentalnego przetwarzania danych osobowych, zachowana jest szczególna ostrożność przy postępowaniu z danymi osobowymi mająca na celu ochronę tych danych, w szczególności przed ujawnieniem tych danych osobom nieuprawnionym.