POLITYKA BEZPIECZEŃSTWA

obowiązująca u przedsiębiorcy Marcina Chmieleckiego
prowadzącego działalność gospodarczą pod firmą
"CHILI WEB APPLICATIONS" MARCIN CHMIELECKI
z siedzibą w Łodzi przy ul. Traktorowej 126 lok. 104, 91-204 Łódź
NIP: 7261647595, REGON: 472964034

- wersja obowiązująca od dnia 25 maja 2018 roku

SPIS TREŚCI

I.	Postanowienia ogólne	3
II.	Obowiązki Przedsiębiorcy jako ADO i Procesora	5
III.	Zasady przetwarzania danych osobowych	6
IV.	Osoby upoważnione do przetwarzania danych osobowych	10
V.	Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe	11
VI.	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych wraz z opisem struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	11
VII.	Sposób przepływu danych pomiędzy poszczególnymi systemami	11
VIII.	Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	12
IX.	Procedura postępowania w przypadku naruszenia bezpieczeństwa danych osobowych	13
X.	Przeglądy Polityki Bezpieczeństwa	15
XI.	Postanowienia końcowe	15
XII.	Wykaz załączników	15

I. POSTANOWIENIA OGÓLNE

1. Niniejszym wprowadza się niniejszą Politykę Bezpieczeństwa.

2. Jeśli w niniejszej Polityce Bezpieczeństwa mowa o:
   a) **Administratorze Danych Osobowych (ADO) –** rozumie się przez to podmiot decydujący o celach i środkach przetwarzania danych osobowych**;**
   b) **Administratorze Systemów Informatycznych (ASI)** – rozumie się przez to osobę fizyczną nadzorującą bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych;
   c) **danych sensytywnych** - rozumie się przez to dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby;
   d) **Ewidencji Upoważnień** – rozumie się przez to ewidencję udzielonych upoważnień do przetwarzania danych osobowych;
   e) **Instrukcji** – rozumie się przez to instrukcję zarządzania systemem informatycznym sporządzoną i wdrożoną przez Przedsiębiorcę;
   f) **integralności danych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   g) **odbiorcy danych -** rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią, z wyłączeniem organów administracji publicznej, które mogą otrzymywać dane osobowe w ramach konkretnego prowadzonego przez nie postępowanie;
   h) **poufności danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
   i) **Procesorze** – rozumie się przez to Przedsiębiorcę działającego jako podmiot, któremu właściwy ADO powierzył w drodze umowy przetwarzanie danych osobowych;
   j) **Przedsiębiorcy** – rozumie się przez to Marcina Chmieleckiego prowadzącego działalność gospodarczą pod firmą "CHILI WEB APPLICATIONS" MARCIN CHMIELECKI z siedzibą w Łodzi przy ul. Traktorowej 126 lok. 104, 91-204 Łódź, NIP: 7261647595, REGON: 472964034, który pełni rolę Administratora Danych Osobowych lub Procesora;
   k) **przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
   l) **RODO** - rozumie się przez to 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 (ogólne rozporządzenie o ochronie danych);
   m) **rozliczalności** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

n) **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
o) **usłudze społeczeństwa informacyjnego** - rozumie się przez to każdą usługę normalnie świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług;
p) **zbiorze danych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

3. Polityka Bezpieczeństwa reguluje całościowo dopuszczalny prawem sposób zarządzania i ochrony danych osobowych oraz prawa osób, których dane osobowe są przetwarzane przez Przedsiębiorcę.

4. Polityka odnosi się do wszelkich danych osobowych przetwarzanych przez Przedsiębiorcę, w zbiorach danych lub poza nimi.

5. Celem Polityki Bezpieczeństwa jest:
   a) wskazanie działań, jakie należy podjąć, formy tych działań oraz sposób ich przeprowadzania, niezbędnych do zadośćuczynienia obowiązkom ciążącym na Przedsiębiorcy jako ADO lub Procesorze;
   b) stworzenie podstaw organizacyjnych dla wdrożenia systemu zarządzania bezpieczeństwem danych osobowych przez Przedsiębiorcę;
   c) określenie podstawowych zasad i wymagań organizacyjno-technicznych oraz prawnych dla zapewnienia właściwej ochrony bezpieczeństwa danych osobowych;
   d) właściwe udokumentowanie przypadków naruszenia bezpieczeństwa oraz zapewnienie właściwego trybu działania w celu przywrócenia bezpieczeństwa danych.

6. Przedsiębiorca w zakresie przetwarzania danych osobowych działa przede wszystkim jako Procesor na podstawie umów o powierzenie przetwarzania danych osobowych zawartymi z kontrahentami, którzy są w takich przypadkach Administratorami Danych Osobowych. Ponadto przedsiębiorca przetwarza dane osobowe swoich pracowników oraz klientów sklepu internetowego www.goodssl.pl .

7. Przedsiębiorca deklaruje podejmowanie wszelkich możliwych działań koniecznych do zapobiegania wszelkim zagrożeniom bezpieczeństwa danych osobowych.

8. Przedsiębiorca nie należy do podmiotów, o których mowa w art. 38 RODO. Ze względu na niewielką ilość zatrudnionych przez Przedsiębiorcę osób i podział ról w zakładzie pracy wystarczające jest, aby wykonywał on samodzielnie obowiązki, które zostałyby przekazane inspektorowi ochrony danych osobowych, gdyby został powołany. Przedsiębiorca nie jest podmiotem publicznym, ewentualne przetwarzanie przez niego danych sensytywnych jest sporadyczne, a jego działalność nie polega na operacjach przetwarzania danych, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą.

II. OBOWIĄZKI PRZEDSIĘBIORCY JAKO ADO I PROCESORA

1. Przedsiębiorca realizuje zadania w zakresie ochrony danych osobowych zmierzające do zapewnienia przestrzegania o ochronie danych osobowych, w szczególności:
    a) nadzoruje opracowanie i aktualizację Polityki Bezpieczeństwa i Instrukcji;
    b) nadzoruje przestrzeganie zasad określonych w Polityce Bezpieczeństwa i Instrukcji;
    c) zapewnia środki techniczne i organizacyjne zapewniające ochronę danych osobowych;
    d) zapewnia, że dostęp do danych osobowych mają jedynie osoby upoważnione;
    e) zabezpiecza dane osobowe przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez podmiot nieuprawniony, zmianą, utratą, uszkodzeniem lub zniszczeniem;
    f) zapewnia legalność przetwarzania danych osobowych na zasadach określonych w stosownych przepisach;
    g) zapewnia zgodne z przepisami prawa udostępnianie i powierzanie danych osobowych;
    h) podejmuje odpowiednie działania w przypadku zagrożenia bezpieczeństwa przetwarzania danych osobowych.

2. Przedsiębiorca samodzielnie wykonuje zadania ASI, w szczególności:
    a) zapewnia prawidłowe użytkowanie systemu informatycznego;
    b) przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego, ustawia i modyfikuje uprawnienia, wyrejestrowuje oraz usuwa konta użytkowników;
    c) wyjaśnia wszystkie zgłoszone nieprawidłowości i incydenty dotyczące przetwarzania danych z wykorzystaniem środków informatycznych.

3. Przedsiębiorca realizuje prawo osoby, której dane dotyczą, do:
    a) uzyskania informacji o administratorze danych osobowych, celu, zakresie i sposobie przetwarzania danych, kategoriach odnośnych danych, planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe - kryteriach ustalania tego okresu; źródle, z którego dane pochodzą oraz sposobie udostępniania danych oraz ich odbiorcach lub ich kategoriach;
    b) żądania uzupełnienia, uaktualnienia, sprostowania danych
    c) ograniczenia przetwarzania danych osobowych na zasadach określonych w art. 18 RODO;
    d) wniesienia umotywowanego wniosku do zaprzestania przetwarzania danych;
    e) wycofania zgody na przetwarzanie danych osobowych;
    f) otrzymania kopii danych osobowych podlegających przetwarzaniu - jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną (e-mail) i jeżeli nie zaznaczy inaczej, informacji udziela się tą samą drogą;
    g) otrzymania ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych, które dostarczyła ADO;
    h) żądania przesłania danych tej osoby innemu ADO, o ile jest to technicznie możliwe.

4. Jeżeli Przedsiębiorca ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

5. Jeżeli Przedsiębiorstwo przetwarza dane osobowe wspólnie z innym podmiotem, zwłaszcza w sytuacji, kiedy przetwarza dane jako Procesor, Przedsiębiorca z innymi podmiotami – ADO lub innym procesorem - w przejrzysty sposób określą zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności do udzielania informacji, o których mowa w rozdziale III ust. 8 i 13 niniejszej Polityki Bezpieczeństwa.

III. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. Dane osobowe Przedsiębiorca przetwarza w systemach informatycznych oraz w formie papierowej.

2. Przetwarzanie danych osobowych może nastąpić:
   a) za zgodą osoby, której dane dotyczą,
   b) w zakresie, w jakim pozwala na to Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną,
   c) w zakresie, w jakim Przedsiębiorcy powierzono przetwarzanie danych na podstawie umowy z właściwym ADO.

3. Zgoda osoby, której dane dotyczą, oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

4. Zgoda osoby, której dane dotyczą, nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Przedsiębiorca dąży do tego, aby zgoda na przetwarzanie danych osobowych była utrwalona w systemie informatycznym.

5. Zgoda może być wycofana w każdym czasie. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

6. W przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat. Jeżeli dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody.

7. Podczas pozyskiwania danych osobowych przekazuje się osobie, której dane dotyczą, następujące informacje:
   a) dane ADO, w szczególności nazwę oraz adres siedziby;
   b) dane wszystkich podmiotów, którym powierzono przetwarzanie danych osobowych, w szczególności nazwę oraz adres siedziby;

c) cele przetwarzania danych osobowych, oraz podstawę prawną ich przetwarzania;
d) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
e) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe - kryteria ustalania tego okresu;
f) informacje o prawie do żądania od ADO lub Procesora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
g) informację o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
h) informację o prawie wniesienia skargi do organu nadzorczego na podstawie RODO;
i) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych.

8. W przypadku świadczenia usług drogą elektroniczną przez Przedsiębiorcę, przekazuje on osobie, której dane dotyczą (usługobiorcy) również informacje o:
   a) możliwości korzystania z usługi świadczonej drogą elektroniczną anonimowo lub z wykorzystaniem pseudonimu, o ile jest to dopuszczalne;
   b) udostępnianych przez Przedsiębiorcę środkach technicznych zapobiegających pozyskiwaniu i modyfikowaniu przez osoby nieuprawnione danych osobowych przesyłanych drogą elektroniczną,
   c) podmiocie, któremu powierza przetwarzanie danych, ich zakresie i zamierzonym terminie przekazania.

9. Informacje, o których mowa w Rozdziale III ust. 8 niniejszej Polityki Bezpieczeństwa, Przedsiębiorca podaje rozsądnym terminie, najpóźniej w ciągu miesiąca, przy pierwszej komunikacji z osobą, której dane dotyczą – w chwili ich wprowadzania przez tę osobę do systemu informatycznego.

10. Zgoda osoby, której dane dotyczą, może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania.

11. Obowiązek uzyskania zgody osoby, której dane dotyczą, ciąży na ADO.

12. Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, ADO podaje osobie, której dane dotyczą, informacje, o których mowa w Rozdziale III ust. 8 niniejszej Polityki Bezpieczeństwa oraz informacje o:
   a) kategoriach odnośnych danych osobowych;
   b) źródle pochodzenia danych osobowych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych.

13. Celem przetwarzania danych osobowych przez Przedsiębiorcę jest:
   a) świadczenie usług na podstawie umów zawieranych z podmiotami, które są Administratorami Danych Osobowych zgodnie z obowiązującymi przepisami;
   b) wykonywanie praw i obowiązków Przedsiębiorcy jako pracodawcy.

14. Przetwarzane dane osobowe muszą odzwierciedlać stan faktyczny.

15. Wymagana jest ponowna zgoda osoby, której dane dotyczą, jeżeli cel przetwarzania uległ zmianie.

16. Przetwarzanie danych dla innych celów niż te, dla których zostały zebrane, jest dopuszczalne jeśli:
    a) cele te są zgodne;
    b) nie narusza praw i wolności osoby, której dane dotyczą;
    c) następuje w celach statystycznych z poszanowaniem stosownych przepisów.

17. Aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane - ADO bierze pod uwagę przede wszystkim:
    a) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania;
    b) kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a ADO;
    c) charakter danych osobowych, w szczególności czy przetwarzane są dane sensytywne;
    d) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą;
    e) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji.

18. Jeżeli ADO planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w Rozdziale III ust. 8 niniejszej Polityki Bezpieczeństwa.

19. Dane osobowe są przetwarzane przez Przedsiębiorcę:
    a) zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
    b) w zakresie niezbędnym do celów, w których są przetwarzane, i tylko w takim zakresie;
    c) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
    d) w sposób zapewniający ich bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.

20. Przetwarzanie danych sensytywnych jest możliwe jedynie w przypadku spełnienia jednej z poniższych przesłanek:
    a) osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych;
    b) przepis szczególny zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony;
    c) przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora;

d) jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych;
e) przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem;
f) przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w stosownych przepisach;
g) przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych;
h) przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą; jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego;
i) publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone;
j) przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

21. ADO dba o prawidłowość przetwarzanych danych, a w razie potrzeby dokonuje ich uaktualnienia. Przedsiębiorca podejmie wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

22. Udostępnianie danych osobowych może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien mieć formę pisemną i zawierać następujące informacje:
    a) oznaczenie wnioskodawcy;
    b) wskazanie podstawy prawnej;
    c) określenie rodzaju i zakresu potrzebnych informacji oraz formy ich przekazania lub udostępnienia;
    d) wskazanie imienia, nazwiska osoby upoważnionej do pobrania informacji lub zapoznania się z ich treścią.

23. Udostępnianie danych osobowych na podstawie ustnego wniosku jest dopuszczalne tylko w przypadku, gdy zachodzi konieczność niezwłocznego działania.

24. Przedsiębiorca informuje każdego odbiorcę, któremu ujawniono dane osobowe, o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Przedsiębiorca informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

25. Przedsiębiorca prowadzi rejestr udostępnień danych osobowych, który stanowi Załącznik nr 1 do niniejszej Polityki Bezpieczeństwa.

26. Wszelkie czynności przetwarzania danych osobowych odnotowuje się w Rejestrze czynności przetwarzania, który stanowi Załącznik nr 10 do niniejszej Polityki Bezpieczeństwa. Rejestr czynności przetwarzania prowadzony jest w wersji elektronicznej.

IV. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Przetwarzać dane osobowe może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych wydane przez Przedsiębiorcę i wpisane do Ewidencji Upoważnień, oraz która złożyła pisemne oświadczenie o zachowaniu danych osobowych w poufności.

2. Wzór upoważnienia stanowi Załącznik nr 2 do niniejszej Polityki Bezpieczeństwa, wzór oświadczenia o zachowaniu danych w poufności – Załącznik nr 3, a Ewidencja Upoważnień – Załącznik nr 4.

3. Osoba posiadająca upoważnienie do przetwarzania danych osobowych jest uprawniona do ich przetwarzania wyłącznie w zakresie i czasie wskazanym w upoważnieniu.

4. Osoba upoważniona do przetwarzania danych osobowych musi zostać uprzednio odpowiednio przeszkolona, zapoznana z Polityką Bezpieczeństwa, Instrukcją oraz obowiązującymi przepisami.

5. Osoba upoważniona do przetwarzania danych osobowych ma obowiązek:
   a) zachować tajemnicę danych osobowych;
   b) przestrzegać procedur bezpiecznego przetwarzania danych osobowych zawartych w szczególności w Polityce Bezpieczeństwa oraz Instrukcji;
   c) zabezpieczać dane osobowe przed ich udostępnianiem osobom nieupoważnionym, utratą oraz niepożądaną zmianą;
   d) nieprzenosić danych osobowych poza zbiór danych, w szczególności nie wykonywać wydruków ani nieautoryzowanych kopii zapasowych;
   e) wylogowywać się w trakcie przerwy a także po zakończeniu pracy na komputerze posiadającym dostęp do zbioru danych;
   f) udostępniać dane osobowe drogą elektroniczną tylko w postaci zaszyfrowanej;
   g) niepozostawiać osób trzecich w pomieszczeniach, w których przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;
   h) zamykać okna w razie opuszczania pomieszczeń, w których przetwarzane są dane osobowe;
   i) zamykania drzwi na klucz w razie opuszczania pomieszczeń, w których przetwarzane są dane osobowe.

6. Przedsiębiorca może powierzyć przetwarzanie danych osobowych podmiotowi trzeciemu. Dotyczy to w szczególności przedsiębiorstw hostingowych.

Powierzenie następuje na podstawie umowy i pod warunkiem wyrażenia na jej zawarcie zgody przez ADO, wobec którego Przedsiębiorca działa jako Procesor.

V. WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

1. Przetwarzanie danych osobowych dopuszczalne jest wyłącznie na wyznaczonym do tego obszarze.

2. Szczegółowy wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe, znajduje się w Załączniku nr 5 do niniejszej Polityki Bezpieczeństwa.

VI. WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH WRAZ Z OPISEM STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY NIMI

1. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzana tych danych wraz z opisem struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi znajduje się w Załączniku nr 6 do niniejszej Polityki Bezpieczeństwa.

VII. SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

1. U Przedsiębiorcy poszczególne systemy nie są ze sobą powiązane, ponieważ każdy (oprócz zbioru danych osobowych pracowników) jest przeznaczony dla innego Administratora Danych Osobowych – klienta Przedsiębiorcy. Przedsiębiorca przetwarza dane osobowe przede wszystkim jako Procesor.

2. Dane ze zbioru danych osobowych pracowników również nie podlegają przepływowi pomiędzy systemami.

VIII. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANIA DANYCH

1. Ochrona danych osobowych jest realizowana poprzez zabezpieczenia fizyczne, zabezpieczenia organizacyjne, zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej, zabezpieczenia narzędzi programowych i baz danych oraz przez osoby upoważnione.

2. Zabezpieczenia organizacyjne:
   a) Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych;
   b) Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego;
   c) Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
   d) Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane – nie są skierowane w stronę okien ani drzwi;
   e) Kopie zapasowe są przechowywane na innym serwerze, niż serwery, na których przetwarzane są dane osobowe.

3. Zabezpieczenia ochrony fizycznej danych osobowych:
   a) Zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonych drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi);
   b) Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest nadzorowany przez służbę ochrony;
   c) Pomieszczenia, w których przetwarzane są dane osobowych, posiadają zabezpieczenia przeciwpożarowe – czujnik dymu oraz gaśnicę.

4. Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej:
   a) Zbiór danych osobowych przetwarzany jest przy użyciu komputerów przenośnych;
   b) Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej lub komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS;
   c) Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
   d) Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł;
   e) Zastosowano system rejestracji dostępu do systemu;
   f) Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji;
   g) Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnieni;
   h) Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity;
   i) Użyto system Firewall do ochrony dostępu do sieci komputerowej.

5. Zabezpieczenia narzędzi programowych i baz danych:
    a) Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych;
    b) Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
    c) Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
    d) Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

6. Zastosowane zabezpieczenia mają służyć osiągnięciu celów przetwarzania danych oraz zapewnić poufność, integralność i rozliczalność danych osobowych oraz integralność systemu.

IX. PROCEDURA POSTĘPOWANIA W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest poinformować Przedsiębiorcę o każdym przypadku stwierdzenia zagrożenia bezpieczeństwa danych osobowych lub zaistnienia incydentu.

2. Przez zagrożenie bezpieczeństwa danych osobowych rozumie się każde zdarzenie, zależne jak i niezależne od woli ludzkiej, które może powodować utratę integralności, poufności lub rozliczalności danych osobowych. W razie wątpliwości za zagrożenie bezpieczeństwa danych osobowych uważa się w szczególności:
    a) niewłaściwe zabezpieczenie pomieszczeń i urządzeń;
    b) niewłaściwe zabezpieczenie sprzętu informatycznego lub oprogramowania przed nieupoważnionym dostępem podmiotów trzecich, kradzieżą i utratą danych osobowych;
    c) nieprzestrzeganie zasad Polityki Bezpieczeństwa, Instrukcji, lub stosownych przepisów prawa;
    d) naruszenie zabezpieczeń fizycznych przez podmiot trzeci.

3. Przez incydent uważa się naruszenie bezpieczeństwa danych osobowych, które spowodowało ich nieuprawnione udostępnienie, zniszczenie lub uszkodzenie. W razie wątpliwości za incydent uważa się w szczególności:
    a) zdarzenia losowe zewnętrzne, takie jak pożar czy zalanie, skutkujące zniszczeniem urządzeń służących do przetwarzania danych;
    b) zdarzenia losowe wewnętrzne, takie jak awaria systemu, urządzeń, oprogramowania;
    c) zachowania nieumyślne, takie jak utrata danych osobowych, pomyłka użytkownika systemu;
    d) zachowania umyślne, takie jak włamanie do systemu informatycznego lub pomieszczeń, kradzież danych lub sprzętu, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie danych lub sprzętu, działanie szkodliwego oprogramowania.

4. W przypadku stwierdzenia zaistnienia zagrożenia lub incydentu Przedsiębiorca prowadzi postępowanie wyjaśniające, w toku którego ustala:

a) przyczynę sytuacji;
b) jakie mogą być jej skutki;
c) jakie działania należy podjąć w celu zapobieżenia skutkom;
d) osoby odpowiedzialne za sytuację.

5. W toku postępowania wyjaśniającego Przedsiębiorca zabezpiecza dowody i dokumentuje poczynione ustalenia, o których mowa w Rozdziale IX ust. 4 niniejszej Polityki Bezpieczeństwa.

6. Po przeprowadzeniu postępowania wyjaśniającego Przedsiębiorca w ciągu 21 dni sporządza raport. Wzór raportu stanowi Załącznik nr 7 do niniejszej Polityki Bezpieczeństwa .

7. Przedsiębiorca po każdym zagrożeniu bezpieczeństwa danych osobowych lub incydencie analizuje możliwość i zasadność podjęcia działań, które zminimalizują ryzyko zaistnienia podobnej sytuacji w przyszłości.

8. Nie później niż w terminie 72 godzin po stwierdzeniu naruszenia Przedsiębiorca zgłasza incydent właściwemu ADO oraz organowi nadzorczemu właściwemu zgodnie z art. 55 RODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Wzór zgłoszenia stanowi Załącznik nr 8 do niniejszej Polityki Bezpieczeństwa.

9. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie formułowane jest prostym i jasnym językiem i zawiera takie informacje, jakichkolwiek oznaczenie osoby, od której można uzyskać więcej informacji, opis możliwych konsekwencje naruszenia ochrony danych osobowych oraz opis zastosowanych lub proponowanych środków zmierzających do zaradzenia naruszeniu ochrony danych osobowych i jego ewentualnym skutkom. Wzór zgłoszenia stanowi Załącznik nr 9 do niniejszej Polityki Bezpieczeństwa.

10. Zawiadomienie, o którym mowa w Rozdziale IX ust. 9 niniejszej Polityki Bezpieczeństwa nie jest konieczne, jeśli
    a) zostały wdrożone odpowiednie techniczne i organizacyjne środki ochrony uniemożliwiające odczyt danych osobowych, których bezpieczeństwo zostało naruszone – np. zostały one zaszyfrowane;
    b) wymagałoby ono niewspółmiernie dużego wysiłku.

11. W sytuacji, o której mowa w Rozdziale IX ust. 10 lit. b niniejszej Polityki Bezpieczeństwa, Przedsiębiorca zamieści publiczny komunikat zawierający odnośnie informacje, lub zobowiąże do tego właściwego ADO.

X. PRZEGLĄDY POLITYKI BEZPIECZEŃSTWA

1. Co najmniej raz w każdym roku kalendarzowym dokonuje się przeglądu niniejszej Polityki Bezpieczeństwa pod kątem aktualności oraz zgodności deklarowanego w niej stanu z prawem.

2. Polityka podlega aktualizacji w każdym przypadku, gdy zaistnieje taka potrzeba.

XI. POSTANOWIENIA KOŃCOWE

1. Przypadki nieuzasadnionego zaniechania obowiązków lub naruszenia innych zasad wynikających z niniejszej Polityki Bezpieczeństwa mogą stanowić podstawę do pociągnięcia danej osoby do odpowiedzialności, adekwatnie do łączącego ją z Przedsiębiorcą stosunku prawnego.

2. W sprawach nieuregulowanych niniejszą Polityką Bezpieczeństwa mają zastosowanie przepisy adekwatnych aktów prawnych.

XII. WYKAZ ZAŁĄCZNIKÓW

Załącznik nr 1	Rejestr udostępnień danych osobowych
Załącznik nr 2	Wzór upoważnienia do przetwarzania danych osobowych
Załącznik nr 3	Wzór oświadczenia o zachowaniu danych w poufności
Załącznik nr 4	Ewidencja Upoważnień
Załącznik nr 5	Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe
Załącznik nr 6	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzana tych danych wraz z opisem struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi
Załącznik nr 7	Wzór raportu stwierdzenia zagrożenia bezpieczeństwa danych osobowych lub incydentu (naruszenia bezpieczeństwa danych osobowych)
Załącznik nr 8	Wzór zgłoszenia naruszenia bezpieczeństwa danych osobowych
Załącznik nr 9	Wzór informacji o naruszeniu bezpieczeństwa danych osobowych
Załącznik nr 10	Rejestr czynności przetwarzania (wersja elektroniczna)