POLITYKA BEZPIECZEŃSTWA INFORMACJI SERWISU RESERVADO

Administratorem Informacji oraz Podmiotem przetwarzającym Informacje przetwarzane w ramach Serwisu jest:

CIS Software Spółka z ograniczoną odpowiedzialnością Spółka komandytowa

ul. Balladyny 3, 81-859 Gdynia, KRS 0000660730

Adres e-mail: biuro@reservado.pl

DEFINICJE:

Administrator Informacji – CIS Software Spółka z ograniczoną odpowiedzialnością Spółka komandytowa (zwana dalej w skrócie „CIS"), będąca producentem i dostawcą aplikacji internetowej o nazwie *Reservado* dostępnej pod adresem internetowym reservado.pl, w zakresie danych osobowych przetwarzanych na podstawie i w zakresie zgody udzielonej przez Klienta serwisu.

Podmiot przetwarzający - CIS Software Spółka z ograniczoną odpowiedzialnością Spółka komandytowa (zwana dalej w skrócie „CIS"), będąca producentem i dostawcą aplikacji internetowej o nazwie *Reservado* dostępnej pod adresem internetowym reservado.pl, w zakresie danych osobowych przetwarzanych na podstawie i w zakresie umowy o powierzenie przetwarzania danych osobowych zawartej z Klientem serwisu.

Serwis – Aplikacja internetowa *Reservado* oraz usługi jej towarzyszące, świadczone przez CIS.

Serwer – Serwer, za pomocą którego działa Serwis i świadczone są usługi z nim związane, a także serwer CDN – *Content Delivery Network* oferujące poszczególne zasoby Serwisu w celu przyspieszenia jego działania i rozłożenia załadunku Serwisu na kilka serwerów, w tym skrypty, frameworki oraz inne elementy Serwisu, aby zapewnić prawidłowe działanie Serwisu możliwie największej liczbie Użytkowników w danej jednostce czasu,

Użytkownik – osoba korzystająca z Serwisu, która przeszła proces rejestracji, a także każda inna osoba, bez względu na jej charakter i formę prawną, której Użytkownik umożliwił korzystanie z Serwisu.

Klient Użytkownika Serwisu – osoba korzystająca z Serwisu poprzez funkcjonalność „Umów na wizytę" udostępnioną przez Użytkownika Serwisu na stronie internetowej Użytkownika, bądź osoba, której dane wprowadził Użytkownik Serwisu do systemu.

Identyfikator Użytkownika (Login / ID) – w znaczeniu nadanym w § 2 Rozporządzenia

Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004 r., tj. ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (tj. Użytkownika Serwisu).

Hasło Użytkownika - w znaczeniu nadanym w § 2 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004 r., tj. ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (tj. Użytkownikowi Serwisu).

Poufność – środki techniczne uniemożliwiające osobom trzecim oraz osobom do tego nieupoważnionym, korzystanie z chronionego zbioru danych osobowych, przetwarzanych w ramach Serwisu.

Integralność – kompletność danych wprowadzonych do Serwisu przez Użytkownika i uniemożliwienie ich nieautoryzowanej zmiany, sporządzania kopii, ich skasowania, bądź zniszczenia, przejęcia bądź przechwycenia.

Informacje – zbiór danych, w tym w szczególności danych osobowych oraz innych danych podlegających szczególnej ochronie, których dotyczy niniejsza Polityka Bezpieczeństwa Informacji.

Rejestr Zgód – rejestr prowadzony przez CIS rejestrujący zgody na przetwarzanie Informacji, w tym danych osobowych.

Rejestr Czynności Przetwarzania - rejestr prowadzony przez CIS rejestrujący czynności przetwarzania Informacji, w tym danych osobowych, w tym przetwarzania Informacji powierzonych stosowną umową.

Dysponent Danych Osobowych – „dysponent danych" bądź „dysponent danych osobowych" oznacza osobę, której dotyczą Informacje – w szczególności dane osobowe, bądź osobę, podmiot, tudzież inny twór, mogący zarządzać Informacjami bądź danymi osobowymi, legitymujący się ważną podstawą prawną do takich czynności.

§ 1. POSTANOWIENIA OGÓLNE.

1. CIS oświadcza, iż Serwis przechowuje minimum niezbędnych Informacji, w tym danych osobowych, z całkowitym wyłączeniem „danych wrażliwych", wskazanych pkt 2, służących celom:
   a. założenia konta (procesu rejestracji) w Serwisie oraz celem wystawiania faktur na Użytkowników tytułem korzystania z Serwisu – co obejmuje takie dane, jak:
      - Imię i nazwisko Użytkownika,
      - Firma przedsiębiorstwa oraz jego forma prawna,
      - Adres przedsiębiorstwa,
      - Numer NIP w celach wystawiania faktury oraz rozliczenia należności za

świadczone usługi przez Administratora Informacji Użytkownikowi oraz zapewnienia bezpieczeństwa transakcji oraz w celu podpisania z Użytkownikiem umowy powierzenia przetwarzania danych osobowych (tylko jeżeli te dane okażą się niezbędne do prawidłowego świadczenia usługi),
    - Imiona i nazwiska pracowników bądź osób wykonujących obowiązki na podstawie umów cywilnoprawnych,
    - Numer telefonu komórkowego,
    - Adres e-mail,
    - Login oraz Hasło przypisany Użytkownikowi Serwisu.

b. rejestracji wizyt, tj.
    - Imię i nazwisko Klienta Użytkownika Serwisu,
    - Numer telefonu komórkowego – w celu umożliwienia udzielenia informacji Klientowi Użytkownika Serwisu o przesunięcia terminu wizyty, jej odwołaniu lub wyznaczeniu innego terminu jej odbycia,
    - Rodzaj wizyty,
    - Cennik świadczonych przez Użytkownika usług.

2. CIS oświadcza, iż Serwis nie przechowuje oraz nie wymaga podawania przez Użytkowników, a także nie przetwarza w żaden sposób danych uznawanych jako „dane wrażliwe", objętych zakazem przetwarzania wskazanych w art. 27 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922). Oraz w innych przepisach dotyczących ochrony danych osobowych. Gromadzenie takich danych nie jest zgodne z Polityką Serwisu, a takie dane nie są wymagane w żadnym zakresie do jego działania.
3. CIS oświadcza, iż informacje, w tym dane osobowe wskazane w pkt 1, podawane przez Użytkowników Serwisu i Kontrahentów Użytkowników Serwisu służą jedynie funkcjonowaniu Serwisu, w szczególności rejestracji wizyt w siedzibach Użytkowników. Informacje te obejmują jedynie wąski zakres danych, które umożliwiają rejestrację. Nie obejmują w żaden sposób szczegółowych informacji dotyczących spraw zlecanych Użytkownikom – profesjonalnym pełnomocnikom, takim jak adwokatom czy radcom prawnym. Serwis nie przechowuje tego typu dokumentów, a także nie posiada funkcjonalności pozwalającej na wymianę skanów dokumentów w jakimkolwiek formacie, czy też treści takich dokumentów. Funkcjonalność Serwisu opiera się jedynie na pośredniczeniu w dokonywaniu rejestracji oraz planowania grafiku rejestracji, czy też wizyt, tudzież spotkań pomiędzy Kontrahentami, a Użytkownikami Serwisu. Administrator Informacji zobowiązuje się jednak rozszerzyć postanowienia niniejszej Polityki w razie wprowadzenia takich dodatkowych funkcjonalności o nowe postanowienia i zwiększony zakres ochrony.
4. CIS oświadcza, iż w zakresie Informacji, na których przetwarzanie wyraził zgodę Użytkownik, pełni wobec Użytkownika funkcję Administratora Informacji. Natomiast w zakresie Informacji, co do których Użytkownik powierzył CIS ich przetwarzanie, pełni wobec Użytkownika funkcję podmiotu przetwarzającego dane osobowe.

§ 2. MECHANIZMY OCHRONY INFORMACJI.

1. CIS oświadcza, iż Serwis posiada szereg mechanizmów zabezpieczających dane przed nieautoryzowanym dostępem tzw. **mechanizmy ochrony prewencyjnej informacji**, przede wszystkim:

a. Serwis posiada wbudowany mechanizm z ochrony przede wszystkim przed atakami DDoS (*Denial of Service*) polegającym na zautomatyzowanym uruchomieniu złośliwego kodu, zwykle za pomocą przejętych przez przestępców komputerów z zainstalowanym złośliwym oprogramowaniem, w celu wygenerowania sztucznego ruchu na serwerze Serwisu w celu jego przeciążenia, odmowy współpracy (*crash, Denial of Service)* i następnie przechwycenia danych znajdujących się na serwerze/serwerach Serwisu.
b. Serwis posiada wbudowany mechanizm ochrony przed działaniem *botów* (zautomatyzowanych skryptów umożliwiających na wielokrotne automatyczne próby logowania, w celu odgadnięcia hasła danego Użytkownika metodą ataku *brute-force* – tzn. poprzez generowanie możliwych haseł przy użyciu wszystkich znaków dostępnych na klawiaturze w różnych kombinacjach, a także metodą ataku *dictionary* – tzw. metody słownikowej, która wykorzystuje predefiniowane listy możliwych haseł, takich jak popularne imiona, nazwiska) oraz innych złośliwych skryptów w postaci mechanizmu **captcha** dostarczanego przez **Google Inc**.
c. Serwis przechowuje hasła jedynie w postaci zakodowanej (w postaci *hash code* z odpowiednim szyfrowaniem), a Administrator Informacji nie posiada możliwości ich odkodowania i przekazania ich Użytkownikowi. W przypadku utraty hasła, jego odzyskanie jest możliwe jedynie po skorzystaniu z procedury Odzyskiwania hasła Serwisu, które polega na wpisaniu adresu e-mail używanego przy Rejestracji oraz / i numeru telefonu komórkowego, bądź innych danych użytych przy Rejestracji albo tzw. pytania pomocniczego (np. Nazwisko panieńskie matki). Nie jest możliwe za pomocą tej procedury odzyskanie dotychczasowego hasła, lecz jedynie utworzenie nowego hasła dostępu do Serwisu.
d. Serwis posiada prawidłową konstrukcję bazy danych, tj. dane dotyczące danego Użytkownika nie są dostępne do podglądu innym Użytkownikom, a wszelkie dane wprowadzone do bazy danych, do których dostęp ma Użytkownik są odpowiednio oddzielone od innych Użytkowników. Użytkownicy mają jedynie dostęp do danych przez siebie wprowadzonych i dotyczących siebie.
e. Serwis posiada odpowiednie blokady, uniemożliwiające na *listing* plików znajdujących się na serwerze przez osoby trzecie bez autoryzowanego dostępu. Serwis posiada odpowiednio ustawione przekierowania na strony z błędem typu *404 (nie znaleziono strony)* – oraz inne *error pages.*
f. Serwis posiada odpowiednie blokady uniemożliwiające dostęp i modyfikację plików na podstawie których działa Serwis nieautoryzowanym osobom, poza Administratorem Informacji i bezpośrednimi współpracownikami poza serwerem FTP, na którym znajdują się pliki Serwisu. Pliki znajdujące się na serwerze FTP posiadają odpowiednio ustawione uprawnienia – atrybuty dla plików (tzw. *CHMODy – change mode* - atrybuty*)* uniemożliwiające ingerowanie w pliki na podstawie których działa Serwis. Taka zmiana jest możliwa jedynie przez Administratora Informacji, który posiada bezpośredni dostęp do konta FTP. Dostęp do trybu edycji, nadpisywania czy usuwania plików spoza bezpośredniego dostępu do konta FTP jest niemożliwy, a pliki na których opiera się Serwis są dostępne na zewnątrz tylko w zakresie odczytu (*read mode)* i tylko w zakresie plików, które dotyczą korzystania z Serwisu.
g. Serwer, z którego operuje Serwis, posiada zainstalowane najnowsze i

najbezpieczniejsze wersje oprogramowania, z których w obecnej chwili korzysta i z tych w których w przyszłości będzie korzystał Serwis. Administrator Informacji oświadcza, iż kod źródłowy Serwisu nie zawiera metod komunikacji z bazą danych jako *deprecated* – tj. uznawanych powszechnie, jako nieaktualnych, a w szczególności takich, z których korzystanie jest powszechnie uważane w branży IT jako niebezpieczne i wobec których wyizolowano, a następnie załatano luki w zabezpieczeniach, pozwalające na nieautoryzowany dostęp do Informacji, a fragmenty skryptów i kodu źródłowego, które odpowiadają za komunikację z serwerem są umieszczone w osobnych plikach z nazwami utrudniającym ich odgadnięcie, a także uniemożliwiające ich podgląd, modyfikację poza bezpośrednim dostępem do serwera FTP,

h. CIS oświadcza, iż Serwis został stworzony według powszechnie znanych, bezpiecznych zasad programowania, w szczególności fragmenty kodu źródłowego, które są możliwe do podejrzenia w oknie przeglądarki (za pomocą opcji „Pokaż źródło") uniemożliwiają podgląd i wyizolowanie danych umożliwiających połączenie z bazą danych w tym dane dotyczące nazwy hosta, portu, loginu, czy hasła i dostęp do bazy danych, tudzież serwera FTP przez osoby nieautoryzowane,
i. CIS oświadcza, iż Serwis posiada wbudowany mechanizm regularnego wykonywania kopii zapasowych zarówno plików umieszczonych na Serwerze / Serwerach, a także zawartości baz danych, aby w razie ewentualnego ataku zagrażającego bezpieczeństwu Serwisu możliwe było jak najszybsze przywrócenie jego działania.
j. CIS oświadcza, iż Serwis posiada **ważny certyfikat SSL.** Administrator Informacji dochowa należytej staranności, aby zachować ciągłość i aktualność ww. certyfikatu.

2. CIS oświadcza, iż Serwis posiada przygotowane mechanizmy i sposób postępowania, umożliwiające na podjęcie działań po ewentualnym dokonanym ataku cyberprzestępców (tj. hakerów) – **mechanizmy ochrony w razie przeprowadzonego ataku**, przede wszystkim:
   a. blokada dostępu do Serwisu na czas ustalenia danych identyfikacyjnych osoby, która dokonała ataku, bądź wyizolowania takich danych i przekazania ich odpowiednim organom ścigania, w szczególności Policji, Prokuraturze, ABW, SW i innym służbom bezpieczeństwa, jednocześnie mając na względzie dobro Użytkowników i umożliwienie jak najszybsze ponowne korzystanie z Serwisu przy użyciu jak najmniej odległej czasowo kopii zapasowej danych,
   b. tzw. automatyczne sporządzanie logów (dziennik zdarzeń) przez serwer Serwisu adresów IP, czasu spędzonego w Serwisie w ramach sesji przez adres IP, przybliżonego miejsca z którego pochodzi adres IP (w postaci kraju) oraz w miarę możliwości domeny, z którego pochodzi adres IP w danej jednostce czasu, aby możliwe było przekazanie tych danych organom wskazanym w pkt a, w celu ustalenia osoby odpowiadającej za naruszenie.
   c. możliwość przywrócenia kopii zapasowej danych na serwerze / serwerach FTP czy też kopii zapasowej bazy danych w razie utraty tych danych wskutek ewentualnego ataku na bezpieczeństwo danych Serwisu.

§ 3. UPRAWNIENIA DOSTĘPU DO INFORMACJI.

1. CIS oświadcza, iż wszystkie osoby biorące udział w tworzeniu Serwisu, w tym pracownicy, osoby wykonujące czynności na podstawie umów cywilnoprawnych, a także podmioty zewnętrzne (jeżeli takie są) uczestniczące w tworzeniu Serwisu, wykonują czynności za pomocą stanowisk komputerowych – urządzeń za pomocą których jest tworzony i rozwijany Serwis, posiadających aktualne wersje systemów operacyjnych, programy antywirusowe wyposażone w aktualne bazy danych wirusów – bądź inne pokrewne programy zapewniające wysoki stopień bezpieczeństwa – np. programy typu anti-malware, odpowiednio skonfigurowany Firewall uniemożliwiający przejęcie nieautoryzowanej kontroli nad komputerem, a także stanowiska używające nadal wspieranych systemów operacyjnych i nie wykorzystujących systemów operacyjnych, w których zakończono ich wspieranie.
2. CIS oświadcza, iż Serwis tworzony jest na zasadzie „minimum uprawnień". Oznacza to, iż pracownicy, bądź inne osoby fizyczne albo podmioty, wskazane w ust. 1 posiadają tylko taką ilość uprawnień w celu modyfikacji plików Serwisu, jaka jest potrzebna do ich pracy na stanowisku.
3. CIS oświadcza, iż Serwis jest gotowy, w miarę rozwoju i zatrudniania nowych pracowników, czy innych osób fizycznych albo podmiotów wskazanych w pkt. 1, do wprowadzenia szeregu typów kont pracowniczych ze zmienną liczbą uprawnień, poczynając od Użytkownika, którego uprawnienia ograniczają się do korzystania z Serwisu, do Pracownika, którego uprawnienia umożliwiają ograniczoną modyfikację plików źródłowych Serwisu, a także Administratora umożliwiającą pełną kontrolę nad danymi, z wyłączeniem danych, które w niniejszej Polityce zostały wskazane jako zakodowane, np. hasła użytkowników.
4. CIS oświadcza, iż kopie zapasowe, pliki źródłowe Serwisu są przechowywane w sposób uniemożliwiający ich kradzież bądź przypadkową utratę. Pliki nie są umieszczane za pomocą ogólnodostępnych wirtualnych dysków w chmurze, ani za pomocą *cloud backup*, ani w formie załącznika e-mail, za pomocą ogólnodostępnych serwisów do przesyłania plików, czy też serwisów społecznościowych, lecz są przesyłane wewnętrznymi kanałami komunikacyjnymi ze wzmożonymi zabezpieczeniami.
5. CIS oświadcza, iż Serwis posiada serwer zapasowy umożliwiający na wznowienie działania Serwisu mimo awarii, w jak najkrótszym możliwym czasie.
6. Po rozwiązaniu stosunku pracy, zakończeniu współpracy, bądź rozwiązaniu umowy cywilnoprawnej z osobą, która miała dostęp do danych Serwisu, jego bazy danych, Administrator Informacji zobowiązuje się podjąć natychmiastowe kroki w celu dezaktywacji i uniemożliwienia takiej osobie dostępu do danych – oznacza to, w zależności od potrzeb – usunięcie konta takiej osoby w Serwisie, bądź zmianę nazwy użytkownika i/lub hasła również innym osobom pracującym przy tworzeniu Serwisu, jeżeli istnieje prawdopodobieństwo, iż taka osoba mogła przypadkowo wejść w posiadanie takich danych należących do innej osoby.

§ 4. KOPIE ZAPASOWE. OCHRONA INFORMACJI W RAZIE AWARII.

1. CIS zobowiązuje się do wykonywania regularnych okresowych kopii zapasowych składających się na kopię bazy danych oraz plików źródłowych Serwisu, weryfikowalnych pod względem ich integralności i kompletności za pomocą sum kontrolnych (tzw. *checksum*) oraz przechowywania okresowych kopii zapasowych w odpowiednio zabezpieczony miejscu, do którego nie mają dostępu osoby

nieupoważnione, aby możliwe było natychmiastowe i pełne ich odtworzenie i wznowienie działania Serwisu po awarii.
2. CIS zobowiązuje się do okresowego sprawdzania kopii zapasowych pod kątem możliwości rzeczywistego odtworzenia danych się na nich znajdujących.

§ 5. NARUSZENIA OCHRONY INFORMACJI. PROCEDURA ZGŁASZANIA NARUSZEŃ.

1. CIS prowadzi Rejestr Naruszeń Ochrony Informacji.
2. CIS zobowiązuje się do zgłoszenia naruszenia Ochrony Informacji, w szczególności naruszenia ochrony danych osobowych właściwemu organowi niezwłocznie, lecz nie później niż w ciągu 72 godzin, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
3. Podmioty wskazane w § 3 ust. 1 niniejszej Polityki, jak również wszelkie inne osoby, które weszły w posiadanie danych Serwisu, bądź kopii zapasowych, świadomie, jak i wskutek niezachowania ostrożności, czy też przypadkowo, są zobowiązane natychmiastowo zgłosić naruszenie ochrony informacji – ustnie, na piśmie, drogą telefoniczną lub SMS, wiadomością e-mail, a także w każdy inny możliwy sposób – w pierwszej kolejności Administratorowi Informacji, a w razie niemożności kontaktu z Administratorem Informacji, dowolnej osobie współpracującej przy Serwisie, fakt takiego naruszenia, opisując w miarę możliwości dokładnie na czym polegało naruszenie.
4. Osoby wskazane w pkt 1, które otrzymały w pierwszej kolejności informację o naruszeniu, są zobowiązane sporządzić z takiego zgłoszenia niezwłocznie notatkę służbową i przesłać CIS treść tej notatki oraz dane kontaktowe do osoby, która zgłosiła naruszenie.
5. Osoba zgłaszająca naruszenie, która weszła w posiadanie nośników danych, bądź plików jest zobowiązana do niezwłocznego ich zwrotu CIS i zniszczenia wszelkich kopii danych, których dokonała.
6. CIS jest zobowiązany do niezwłocznej oceny zgłoszenia i zweryfikowania czy mogło dojść potencjalnie do naruszenia ochrony informacji, ocenić skalę zagrożenia i bezzwłocznie podjąć niezbędne środki zaradcze w celu wyeliminowania zagrożenia, bądź ograniczenia skali zagrożenia. Może w tym celu podjąć wszelkie niezbędne środki, z wyłączeniem Serwisu włącznie, informując jednak Użytkowników o ewentualnym ataku, bądź możliwości przedostania się wrażliwych danych na zewnątrz. W razie oceny, iż doszło do naruszenia, CIS niezwłocznie dokona rejestracji w Rejestrze Naruszeń Ochrony Informacji szczegółowych informacji o naruszeniu, wskazując datę, możliwie godzinę – a jeżeli nie jest to możliwe – przybliżoną godzinę, a także dokładny opis naruszenia, ze wskazaniem danych, które potencjalnie mogły zostać albo zostały naruszone, w szczególności liczby osób, których dane mogły zostać dotknięte naruszeniem.
7. CIS zobowiązuje się dokonywać również kopii zapasowych rejestru o którym mowa w ust. 1.

§ 6. REJESTRY ORAZ REALIZACJA PRAW JEDNOSTKI.

1. CIS prowadzi Rejestr Zgód oraz Rejestr Czynności Przetwarzania.
2. CIS oświadcza, iż posiada środki techniczne i możliwości realizacji żądań dysponentów Informacji, w szczególności danych osobowych, takich jak: prawo do

sprostowania danych osobowych, prawo do bycia zapomnianym, prawo do ograniczenia przetwarzania i prawo do dostępu do danych osobowych oraz innych przewidzianych powszechnie obowiązującymi przepisami dotyczących ochrony danych osobowych.

3. CIS zobowiązuje się do ścisłej współpracy z podmiotem, który powierzył CIS przetwarzanie danych osobowych w szczególności w zakresie realizacji żądań wskazanych w ust. 2.
4. CIS zobowiązuje się do bezzwłocznej realizacji żądań wskazanych w ust. 2. W razie opóźnienia, CIS zobowiązuje się do podania przyczyny takie opóźnienia.
5. CIS zobowiązuje się do realizacji żądań wskazanych w ust. 2 w formie wskazanej przez żądającego, w szczególności w formacie nadającym się do odczytu maszynowego.
6. CIS zastrzega sobie prawo do odmowy realizacji żądań wskazanych w ust. 2 w sytuacji, gdy:
   a. żądanie zostało zgłoszone przez osobę nieuprawnioną, dąży do ominięcia prawa bądź nie jest oparte na ważnej podstawie prawnej,
   b. żądanie dąży do pozyskania danych z naruszeniem przepisów dotyczących ochrony danych osobowych,
   c. żądanie wiąże się z nadmiernymi kosztami bądź wydatkami po stronie CIS, chyba że Żądający zobowiąże się do pokrycia tychże kosztów,
   d. żądanie może spowodować naruszenie ochrony danych osobowych.
8. CIS zobowiązuje się dokonywać również kopii zapasowych rejestrów o których mowa w ust. 1.

§ 7. POWIERZENIE PRZETWARZANIA DANYCH.

1. Powierzenie przetwarzania danych odbywa się na podstawie Umowy o powierzeniu przetwarzania danych osobowych (zwaną dalej „Umową") zawartą pomiędzy CIS a Użytkownikiem Serwisu. Przetwarzanie danych odbywa się w zakresie i na zasadach określonych w Umowie zawartej z Użytkownikiem.
2. Czynność Użytkownika polegająca na wprowadzeniu Informacji, w tym w szczególności danych osobowych do Serwisu, CIS poczytuje jako wydanie polecenia przetwarzania danych osobowych.
3. Przetwarzanie danych w ramach funkcjonowania Serwisu, tj. rejestrowanie wizyt, informowanie o nadchodzących wizytach za pomocą SMS / E-mail i inne odbywa się w sposób zautomatyzowany, w zakresie i na podstawie Umowy.
4. Użytkownik ma prawo żądania ograniczenia przetwarzania określonych danych, co do których jest administratorem w każdej chwili. CIS zobowiązuje się do bezzwłocznej realizacji żądania wskazanego w zd. 1 i poinformowania o realizacji żądania Użytkownika.
5. Użytkownik zobowiązuje się do wprowadzania do Serwisu jedynie tych Informacji, w tym w szczególności danych osobowych, co do których może dokonywać czynności przetwarzania zgodnie z ważną podstawą prawną. W razie wprowadzenia danych, których Użytkownik nie może zgodnie z prawem przetwarzać, bądź nie legitymuje się odpowiednim tytułem prawnym do takich celów, CIS nie ponosi odpowiedzialności za ewentualne szkody, bądź naruszenia spowodowane takim wprowadzeniem.
6. Za ważną podstawa prawną czynności przetwarzania uznaje się w szczególności:
   a. zgodę osoby uprawnionej, uzyskaną w sposób zgodny z prawem i spełniająca

wymogi określone w powszechnie obowiązujących przepisach dotyczących ochrony danych osobowych,

b. umowę o powierzenie przetwarzania danych osobowych lub umowę równoważną.

8. W razie powzięcia przez CIS należycie uzasadnionej wątpliwości co do podstawy prawnej czynności przetwarzania, Użytkownik jest zobowiązany do przedstawienia tytułu prawnego do czynności przetwarzania, bądź uprawdopodobnienia w stosownej formie, iż takim tytułem się legitymuje.
9. Za należycie uzasadnioną wątpliwość uznaje się w szczególności:
   a. powzięcie przez CIS wiarygodnych informacji, iż tytuł prawny do przetwarzania danych przez Użytkownika stracił ważność, został uznany za nieważny, bądź z innych względów Użytkownik utracił prawo do przetwarzania danych,
   b. powzięcie przez CIS wiarygodnych informacji, iż doszło u Użytkownika do wycieku danych osobowych, ataku hakerskiego, bądź innego naruszenia danych osobowych,
   c. powzięcie przez CIS wiarygodnych informacji, iż Użytkownik uczestniczył w procederze sprzedaży danych osobowych.
10. W razie odmowy przedstawienia tytułu prawnego upoważniającego Użytkownika do czynności przetwarzania, CIS zastrzega sobie prawo do odmowy przetwarzania powierzonych przez Użytkownika danych co do których powziął należycie uzasadnioną wątpliwość, aż do wyjaśnienia wątpliwości. W takim przypadku Użytkownikowi nie przysługuje rekompensata za odmowę przetwarzania powierzonych danych, chyba że odmowa ta nastąpiła z wyłącznej winy CIS i nie była należycie uzasadniona. Prawo do odmowy przetwarzania powierzonych danych obejmuje jedynie te dane, które są objęte wątpliwością.

§ 8. WDRAŻANIE POSTANOWIEŃ NINIEJSZEJ POLITYKI.

1. Za wdrożenie niniejszej Polityki odpowiada CIS.
2. CIS oświadcza, iż dokonał przeszkolenia personelu z zasad ochrony danych osobowych oraz wdrożył postanowienia niniejszej polityki.
3. CIS zastrzega sobie prawo do zmiany niniejszej Polityki Bezpieczeństwa w każdej chwili, za uprzednim poinformowaniem Użytkowników czytelnym komunikatem widocznym w Serwisie. Zobowiązuje się jednak zachować poziom bezpieczeństwa informacji wskazany w jej pierwotnym kształcie, a wprowadzane zmiany mogą polegać jedynie na rozszerzeniu zakresu ochrony.