POLITYKA BEZPIECZEŃSTWA INFORMACJI SERWISU RESERVADO

Administratorem Informacji przetwarzanych 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 – Serwis prowadzony przez CIS Software Spółka z ograniczoną odpowiedzialnością Spółka komandytowa, będąca producentem aplikacji internetowej o nazwie *Reservado* dostępnej pod adresem internetowym http://reservado.pl.

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

Serwer – Serwer, bądź Serwery, będące Serwerami za pomocą których działa Serwis i świadczone są usługi z nim związane, a także serwery 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 rejestrację na wizytę, związaną z działalnością Użytkownika.

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 – zapewnienie poufności uniemożliwia osobom trzecim oraz osobom do tego nieupoważnionym, korzystanie z chronionego zbioru danych osobowych, przetwarzanych w ramach Serwisu.

Integralność – zapewnienie kompletności 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 danych osobowych oraz innych danych podlegających szczególnej ochronie, których dotyczy niniejsza Polityka Bezpieczeństwa Informacji.

§ 1. POSTANOWIENIA OGÓLNE.

1. Administrator Informacji oświadcza, iż Serwis przechowuje minimum niezbędnych Informacji, w tym danych osobowych, lecz z 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 prowadzonego w danej formie prawnej,
      - Imiona i nazwiska pracowników bądź osób wykonujących obowiązki na podstawie umów cywilnoprawnych,
      - Numer telefonu komórkowego,
      - Adres E-mail,
      - Numer rachunku bankowego, z którego Użytkownik pragnie dokonać zapłaty za świadczone usługi,
      - Numer NIP / PESEL w celach wystawiania faktury za świadczone usługi przez Administratora Informacji Użytkownikowi oraz zapewnienia bezpieczeństwa transakcji,
      - 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 na wypadek przesunięcia terminu wizyty, tudzież w innych przypadkach,
      - Rodzaj wybranej gałęzi prawnej, której dotyczy wizyta,
      - Krótki opis problemu prawnego, którego będzie dotyczyć wizyta,
      - Cennik świadczonych usług.
2. Administrator Serwisu 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).** Gromadzenie takich danych nie jest zgodne z Polityką Serwisu, a takie dane nie są wymagane w żadnym zakresie do jego działania.

3. Administrator Serwisu oświadcza, iż informacje, w tym dane osobowe wskazane w pkt 1, podawane przez Użytkowników Serwisu i Kontrahentów Serwisu służą jedynie funkcjonowaniu Serwisu, a przede wszystkim rejestracji wizyt w siedzibach Użytkowników. Informacje te obejmują jedynie wąski zakres danych, które umożliwiają rejestrację wizyty i jej odbycie. 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 umawianiu wizyt oraz planowania grafiku 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.

§ 2. MECHANIZMY OCHRONY INFORMACJI.

1. Administrator Informacji oświadcza, iż Serwis posiada szereg mechanizmów zabezpieczających dane przed nieautoryzowanym dostępem – **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.**, a także blokadę dostępu przy określonej liczbie prób wpisania hasła.
   c. Serwis przechowuje hasła jedynie w postaci zakodowanej (w postaci *hash code* z odpowiednim szyfrowaniem), a Administrator Informacji nie posiada możliwości ich zdekodowania 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. Nie jest możliwe za pomocą tej procedury odzyskanie dotychczasowego hasła, lecz jedynie utworzenie nowego hasła dostępu do Serwisu. Jednocześnie Administrator Informacji nie odpowiada za długość, ani stopień skomplikowania haseł wprowadzanych przez Użytkowników w procesie rejestracji, jednocześnie jednak wprowadza mechanizmy nakazujące Użytkownikom wprowadzanie haseł o skomplikowanych parametrach. Administrator Informacji zaleca jednak, aby hasła

miały długość przynajmniej 6 znaków i posiadały przynajmniej jedną literę dużą, jedną małą, cyfrę oraz symbol, aby zabezpieczyć hasło przed przypadkowym odgadnięciem, a także nie używanie prostych kombinacji, łatwych do odszyfrowania.

d. Serwis posiada prawidłową konstrukcję bazy danych, zapewniającą, iż 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 / 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 oraz wykonywania (*execute*) skryptu określanych jako *deprecated* – tj. przestarzałych, 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. Administrator Informacji 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 (np. MySQL / MongoDB), w tym dane dotyczące nazwy hosta, portu, loginu, czy hasła i dostęp do bazy danych, tudzież serwera FTP przez osoby nieautoryzowane,
i. Administrator Informacji 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. Administrator Informacji oświadcza, iż Serwis posiada **ważny certyfikat SSL.** Administrator Informacji dochowa należytej staranności, aby zachować ciągłość i aktualność ww. certyfikatu.

2. Administrator Informacji 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. natychmiastowa reakcja na podejrzany ruch w postaci blokady dostępu do Serwisu, w celu zapobieżenia kolejnym atakom,
   d. 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. Administrator Informacji 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 antimalware, 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 – dla przykładu system Windows XP, dla którego producent całkowicie zaprzestał wsparcia technicznego.
2. Administrator Informacji oświadcza, iż Serwis tworzony jest na zasadzie „minimum uprawnień". Oznacza to, iż pracownicy, bądź inne osoby fizyczne albo podmioty, wskazane w pkt 1 posiadają tylko taką ilość uprawnień w celu modyfikacji plików Serwisu, jaka jest potrzebna do ich pracy na stanowisku. Osoba odpowiedzialna jedynie za szatę graficzną, czy też wizualną Serwisu nie posiada dostępu do bazy danych, lecz jedynie taką ilość uprawnień, która jest niezbędna do prawidłowego wykonywania swojej pracy w

tworzeniu Serwisu.

3. Administrator Informacji 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. Administrator Informacji 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 typu Sendspace, WeTransfer i tym podobne, czy też serwisów społecznościowych typu Facebook, Twitter i tym podobne, lecz są przesyłane wewnętrznymi kanałami komunikacyjnymi ze wzmożonymi zabezpieczeniami, takimi jak serwer FTP, do którego dostęp ma Serwis.
5. Administrator Informacji oświadcza, iż praca nad rozwojem Serwisu odbywa się zarówno w siedzibie głównej Serwisu, jak i na odległość, za pomocą pracy zdalnej. Przy pracy zdalnej również obowiązują zasady bezpieczeństwa przesyłanych informacji, zgodnie z zasadami wskazanymi w niniejszej Polityce.
6. Administrator Informacji oświadcza, iż Serwis posiada serwer zapasowy umożliwiający na wznowienie działania Serwisu mimo awarii, w jak najkrótszym możliwym czasie.
7. Po rozwiązaniu stosunku pracy, zakończeniu współpracy, bądź rozwiązaniu umowy cywilnoprawnej z osobą bądź podmiotem, która miała, bądź które miały 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 / 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. Administrator Informacji 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*) w różnych formatach np. MD5 oraz przechowywania okresowych kopii zapasowych w kilku różnych miejscach, do których nie mają dostępu osoby nieupoważnione, aby możliwe było natychmiastowe i pełne ich odtworzenie i wznowienie działania Serwisu po awarii.
2. Administrator Informacji zobowiązuje się do okresowego sprawdzania kopii zapasowych pod kątem możliwości rzeczywistego odtworzenia danych się na nich znajdujących – w razie przechowywania kopii zapasowych na nośnikach danych typu: nośniki optyczne, nośniki mechaniczne, pamięci *flash* oznacza to konieczność sprawdzenia, czy ww. nośniki nie uległy uszkodzeniu, czy też zużyciu, poprzez weryfikację kopii z sumą kontrolną,

wskazaną w pkt 1.

§ 5. NARUSZENIA OCHRONY INFORMACJI. PROCEDURA ZGŁASZANIA NARUSZEŃ.

1. 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.
2. Osoby wskazane w pkt 1, które otrzymały w pierwszej kolejności informację o naruszeniu, są zobowiązane sporządzić z takiego zgłoszenia niezwłocznie notatkę służbową i przesłać Administratorowi Informacji treść tej notatki oraz dane kontaktowe do osoby, która zgłosiła naruszenie.
3. Osoba zgłaszająca naruszenie, która weszła w posiadanie nośników danych, bądź plików jest zobowiązana do niezwłocznego ich zwrotu Administratorowi Informacji i zniszczenia wszelkich kopii danych, których dokonała.
4. Administrator Informacji jest zobowiązany do prowadzenia odpowiedniego Rejestru Naruszeń Ochrony Informacji w dowolnej formie – papierowej, bądź elektronicznej, tak aby zapewnić należytą ochronę tego Rejestru.
5. Administrator Informacji 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, Administrator Informacji 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.
6. Administrator Informacji zobowiązuje się dokonywać również kopii zapasowych rejestru o którym mowa w pkt 4.

§ 6. WDRAŻANIE POSTANOWIEŃ NINIEJSZEJ POLITYKI.

1. Za wdrożenie niniejszej Polityki odpowiada Administrator Informacji.
2. W przypadku rozwoju Serwisu, jak i personelu nad niego pracującym, Administrator Informacji zastrzega sobie prawo do powołania osoby odpowiedzialnej za sprawy bezpieczeństwa Informacji, na stanowisko Administratora Bezpieczeństwa Informacji w rozumieniu Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922). Administrator Informacji zastrzega sobie prawo do powierzenia jej kwestii ochrony informacji.
3. Administrator Informacji 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.