

POLITYKA PRYWATNOŚCI OŚRODKA WZASOWEGO POSEJNELE

1. Ochrona danych osobowych

Jednym z nadrzędnych celów w działalności Ośrodka Wczasowego Posejnele jest ochrona danych osobowych naszych Klientów, Pracowników i Współpracowników. W celu zebrania wszystkich zasad, którymi kierujemy się przy realizacji tego celu, powstała niniejsza Polityka.

2. Kto jest administratorem moich danych osobowych i z kim mogę się kontaktować?

Administratorem Państwa danych osobowych jest FZZPPR iTV w Polsce, OW Posejnele 16-506, Giby, Posejnele 26A, , tel. 87 516 50 16 (dalej "Ośrodek").

Z administratorem danych można kontaktować się poprzez adres email: info@posejnele.com.pl, telefonicznie pod numerem: 87 516 50 16 lub pisemnie na adres siedziby Ośrodka.

3. Jakie dane przetwarzamy, na jakiej podstawie i w jakim celu?

Ośrodek przetwarza przede wszystkim dane zawarte w rezerwacjach pobyków i i innych dokumentach związanych z pobytem i jego rezerwacją. Są to zatem podstawowe dane, takie jak imię i nazwisko lub adresy korespondencyjne. Podczas korzystania przez Państwa z naszej strony internetowej zbieramy też pliki cookies, szczegółowo opisane w dalszej części Polityki.

Podstawą przetwarzania danych osobowych w Ośrodku jest przede wszystkim Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) w skrócie: RODO oraz Ustawa o działalności ubezpieczeniowej i reasekuracyjnej. Znaczna część Państwa danych przetwarzana jest tylko wtedy, gdy wyrażą na to Państwo swoją zgodę.

4. W jaki sposób przechowujemy Państwa dane?

Państwa dane zawsze przechowywane są w sposób bezpieczny, tj. uniemożliwiający dostęp do nich osobom niepowołanym. Każdy pracownik lub współpracownik Ośrodka, który przetwarza dane osobowe jest odpowiednio przeszkolony i posiada stosowne upoważnienie.

Dane osobowe w Ośrodku nigdy nie są przechowywane w większej liczbie miejsc niż to konieczne i dłużej niż istnienie powodów dla ich przechowywania, a które zawsze wynikają z Państwa zgody lub bezpośrednio z przepisów prawa.

5. Kto może otrzymywać państwa dane?

Państwa dane przekazywane są tylko wtedy, gdy jest to konieczne i gdy dany podmiot jest upoważniony do ich otrzymywania. Takimi podmiotami są przede wszystkim organy administracji publicznej i inne organy państwowe, w tym organy ścigania oraz inne podmioty, które wykonują usługi na rzecz Ośrodka, przede wszystkim dostawcy usług informatycznych, prawnych i doradczych.

6. Jakie uprawnienia przysługują Państwu w związku z Państwa danymi osobowymi?

W stosunku do swoich danych mają Państwo szereg uprawnień, które mogą Państwo wykonywać w każdym czasie, o ile na przeszkodzie nie stoi powszechnie obowiązujący przepis prawa. Pośród nich jest przede wszystkim prawo dostępu i wglądu do swoich danych osobowych, prawo do ich przenoszenia, usunięcia, sprostowania oraz ograniczenia ich przetwarzania.

7. Jak chronimy transmisję przez Internet?

Ośrodek stosuje szereg nowoczesnych zabezpieczeń, które gwarantują bezpieczeństwo przy korzystaniu z jego usług i systemów. Zagadnienia bezpieczeństwa obejmują wiele obszarów, ale szczególnie istotna jest dla nas ochrona danych osobowych przekazywanych do Ośrodka i gromadzonych w trakcie korzystania z Serwisów Internetowych. Dzięki zastosowaniu najnowocześniejszych technologii Ośrodek gwarantuje wysoki standard bezpieczeństwa Użytkowników we wszystkich obszarach objętych działaniem Serwisów Internetowych.

8. Jakiego oprogramowania używamy w Serwisach Internetowych?

W Serwisach Internetowych mogą być wykorzystywane następujące technologie: Java, Javascript, XML, DHTML, cookies. Wybrane podstrony Serwisów Internetowych mogą wymagać logowania lub korzystania z szyfrowanego protokołu transmisji SSL.

9. Czym są Pliki Cookies i w jakim celu je zbieramy i przechowujemy?

Pliki cookies to niewielkie pliki tekstowe wysyłane przez odwiedzane strony internetowe i zapisywane w wybranym folderze przeglądarki internetowej na komputerze Użytkownika. Informacje w nich zawarte mogą być odczytane jedynie przez stronę, która je utworzyła i umieściła w folderze przeglądarki. Strona internetowa nie ma dostępu do innych plików, lub danych znajdujących się w Państwa komputerze. Pliki cookies dostarczają danych statystycznych o ruchu Użytkowników i korzystaniu przez nich z poszczególnych stron Serwisów Internetowych. Takie wykorzystanie plików cookies jest bardzo rozpowszechnione i stosowane w większości witryn internetowych. Dzięki niemu Ośrodek może np. określić, czy dany Użytkownik odwiedza stronę po raz pierwszy, a także które elementy Serwisów Internetowych są dla Państwa najbardziej atrakcyjne.

Pliki cookies stosowane w Serwisach Internetowych wykorzystywane są także w celu ułatwienia procesu rejestracji. Ośrodek nie stosuje plików cookies do przetwarzania danych osobowych Użytkowników, lub personalizowania ofert handlowych pod kątem preferencji Użytkownika.

W Serwisach Internetowych używane są dwa rodzaje plików cookies: sesyjne – pozostają w urządzeniu Użytkownika aż do opuszczenia strony internetowej lub wyłączenia oprogramowania (przeglądarki internetowej) oraz stałe – pozostają w urządzeniu Użytkownika przez określony czas albo do momentu ich ręcznego usunięcia z przeglądarki.

Użytkownik Serwisów Internetowych może w każdym czasie wybrać sposób obsługi plików cookies w strefie internetowej poprzez zastąpienie automatycznej obsługi plików cookies obsługą indywidualną, a także usunąć pliki cookies umieszczone w przeglądarce internetowej.

10. Jakie są najważniejsze zasady bezpiecznego korzystania z Internetu?

Korzystanie z Internetu może być związane z ryzykiem wywołanym przez zagrożenia ze strony oprogramowania szpiegującego, spamu, czy wirusów komputerowych.

Komputer każdego Użytkownika korzystającego z Internetu powinien być należycie chroniony. Podstawą zabezpieczenia jest zainstalowany program antywirusowy z aktualną bazą definicji wirusów, aktywną zaporą internetową (firewall) oraz korzystanie z bezpiecznej (aktualnej) wersji przeglądarki internetowej.

Dodatkowo należy zwrócić szczególną uwagę na regularne instalowanie najnowszych aktualizacji systemu operacyjnego w celu stabilizacji i optymalizacji poziomu ochrony komputera.

Programy antywirusowe chroniące komputer przed groźnym oprogramowaniem, w tym oprogramowaniem szpiegującym oraz wirusami komputerowymi, a także firewall, czyli zaporę internetową kontrolującą przepływ informacji pomiędzy komputerem Użytkownika a Internetem są kluczowymi środkami bezpieczeństwa, które uniemożliwiają przekazywanie poufnych danych nieznanym/ niepożądanym odbiorcom.

Należy wystrzegać się otwierania programów przesyłanych pocztą elektroniczną od nieznanych/ niezauważanych nadawców.

Pobierane pliki powinny pochodzić jedynie z zaufanych źródeł.

Instalowanie oprogramowania pochodzącego z nieznanego i niezweryfikowanego źródła stanowi podwyższone ryzyko dostępu nieuprawnionych osób do poufnych danych.

Przy korzystaniu z przeglądarki internetowej zaleca się uruchomienie narzędzi weryfikujących, czy wyświetlana witryna nie stanowi niebezpieczeństwa wyludzenia informacji przez osoby podszywające się pod godne zaufania osoby bądź instytucje.

Instalowanie filtrów antyphishingowych minimalizuje ryzyko bezprawnego dostępu do danych oraz ich kradzieży.

Rekomendowane jest ustalenie złożonego z różnych znaków, bezpiecznego i trudnego do złamania hasła dostępu do sieci. w przypadku korzystania z domowej, bezprzewodowej sieci Wi-Fi. Zaleca się również stosowanie szyfrowania sieci bezprzewodowych Wi-Fi metodą WPA, czy WPA2.