POLITYKA PRYWATNOŚCI

Grupa PZU przywiązuje szczególną wagę do poszanowania prywatności użytkowników odwiedzających naszą stronę internetową. Dane gromadzone w dziennikach logów są wykorzystywane tylko i wyłącznie do celów administrowania serwisem. Nie zabiegamy o identyfikację Użytkowników strony.

Dane identyfikacyjne nie są kojarzone z konkretnymi osobami przeglądającymi stronę Grupy PZU, z wyjątkiem danych zamieszczonych przez Użytkowników w formularzu Generowania Deklaracji Przystąpienia Do Grupowego Ubezpieczenia Zdrowotnego TUW PZUW Opieka Medyczna Dla Pekao S.A.

Dla zapewnienia jak najwyższej jakości serwisu, okazjonalnie analizujemy pliki z logami w celu określenia, jakie przeglądarki stron WWW są stosowane, czy struktura strony nie zawiera błędów, itp.

Odnośniki do innych stron internetowych

Polityka prywatności dotyczy tylko wskazanej strony internetowej.
W przypadku umieszczenia na stronie internetowej odnośników do innych stron WWW, spółki Grupy PZU nie ponoszą odpowiedzialności za zasady zachowania prywatności obowiązujące na tych stronach. Po wejściu na strony internetowe innych podmiotów rekomendujemy zapoznanie się z polityką prywatności tam ustaloną.

Prawa autorskie

Zawartość stron internetowych Serwisu jest własnością Podmiotów Grupy PZU. Wszelkie prawa autorskie osobiste i majątkowe do jakichkolwiek elementów Serwisu (tekstowych, graficznych, układu strony, itp.) są zastrzeżone.
Serwis oraz wszystkie jego elementy są chronione przepisami prawa, w szczególności ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych oraz ustawy z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji.

Informacja o zagrożeniach wynikających ze świadczenia usług drogą elektroniczną/ elektronicznych kanałów dostępu

Podstawowe zagrożenia związane z korzystaniem z usług w Internecie – w tym usług oferowanych przez Grupę PZU w ramach elektronicznych kanałów dostępu – to:

- działanie oprogramowania szpiegującego,
- podszywanie się w celu wyłudzenia informacji,
- wirusy komputerowe,
- spam.

Zagrożenia dotyczą nie tylko komputerów, ale też innego sprzętu przenośnego, np. smartfonów, tabletów.

Oprogramowanie szpiegujące to takie, które w sposób ukryty może zostać zainstalowane na urządzeniu użytkownika np. przez wejście na spreparowaną stronę lub uruchomienie pliku przesłanego w poczcie. Może monitorować/przesyłać do atakującego zarówno dane umieszczone na urządzeniu, jak i nasze działania: ruchy myszką, tekst wpisywany z klawiatury, uruchamiać podgląd/podsłuch z kamery i mikrofonu.

Podszywanie się (ang. phishing) to umieszczenie w Internecie fałszywych stron naśladujących

oryginalne i nakłanianiu użytkowników do zalogowania się na nie np. przez wysłanie spreparowanej wiadomości pocztowej, która udaje komunikat od autentycznej instytucji lub osoby. Celem jest przechwycenie danych dostępowych do usługi (loginu, hasła).

Wirus komputerowy to oprogramowanie złośliwe, które przenosi się poprzez zapis zainfekowanego pliku na nośniku danych np. dysku twardym, pendrive. Celem wirusa jest kradzież lub usunięcie danych, zakłócenie pracy urządzenia lub przejęcie kontroli nad komputerem. Najczęściej do zarażenia wirusem elektronicznym dochodzi przy pobieraniu plików z niezaufanego źródła internetowego lub otwarciu załącznika w poczcie elektronicznej.

Spam to niezamawiane lub niepotrzebne wiadomości elektroniczne rozsyłane jednocześnie do wielu odbiorców. Często przenoszą wirusy komputerowe, oprogramowanie szpiegujące, odnośniki do złośliwych stron.

Podstawowe zasady bezpieczeństwa

1. Każdy użytkownik Internetu powinien dbać o bezpieczeństwo swojego urządzenia. Komputer powinien posiadać program antywirusowy z aktualną bazą definicji wirusów, aktualną i bezpieczną wersję przeglądarki internetowej oraz włączoną zaporę sieciową (ang. firewall). Użytkownik powinien ponadto cyklicznie sprawdzać, czy system operacyjny i programy zainstalowane na nim posiadają najnowsze aktualizacje, ponieważ w atakach wykorzystywane są błędy wykryte w zainstalowanym oprogramowaniu. Producenci programów starają się eliminować takie podatności za pomocą aktualizacji.
2. Dane dostępowe do usług oferowanych w Internecie – np. loginy, hasła, PIN, certyfikaty elektroniczne itp. powinny być zabezpieczone. Nie należy ich ujawniać lub przechowywać na urządzeniu w formie, która umożliwia łatwy dostęp lub odczyt.
3. Zaleca się ostrożność podczas otwierania załączników lub klikania odnośników w wiadomościach, których się nie spodziewaliśmy np. od nieznanych nadawców. W przypadku jakichkolwiek wątpliwości warto się skontaktować z nadawcą.
4. Zaleca się uruchomienie w przeglądarce internetowej narzędzi, które sprawdzają, czy wyświetlona strona internetowa nie wyłudza informacji, np. poprzez podszywanie się pod osobę lub instytucję. Zastosowanie filtrów antyphishingowych znacznie zmniejsza ryzyko kradzieży danych.
5. Ważne jest korzystanie z programów antywirusowych, które zabezpieczają komputery przed szkodliwym oprogramowaniem oraz z zapory sieciowej (tzw. firewall), która kontroluje przesyłanie informacji do i z Internetu, dzięki czemu zapobiega przekazywaniu poufnych danych.
6. Pliki powinny być pobierane tylko z zaufanych miejsc. Wysoce ryzykowne jest instalowanie oprogramowania z niezweryfikowanych źródeł. Dotyczy to również urządzeń przenośnych, np. smartfonów, tabletów.
7. Podczas używania domowej sieci bezprzewodowej (Wi-Fi) należy ustalić bezpieczne i trudne do złamania hasło dostępu do sieci. Rekomenduje się także korzystanie z zaufanych standardów szyfrowania sieci bezprzewodowych Wi-Fi np. WPA2.
8. Istotne jest też utrzymanie w miarę możliwości fizycznej kontroli dostępu nad sprzętem. Jeśli osoba niepowołana dołącza do niego jakieś dodatkowe urządzenia, manipuluje nim, może dojść do zainfekowania złośliwym programem lub podłączenia urządzeń szpiegujących np. keyloggerów, które służą do przechwytywania tekstu wpisywanego na klawiaturze.

Ochrona danych osobowych

Użytkownicy podają w portalu swoje dane osobowe dobrowolnie.
Dane osobowe to wszystkie informacje o osobie fizycznej zidentyfikowanej lub możliwej do zidentyfikowania poprzez jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość, w tym

wizerunek, nagranie głosu, dane kontaktowe, dane o lokalizacji, informacje zawarte w korespondencji, informacje gromadzone za pośrednictwem sprzętu rejestrującego lub innej podobnej technologii.

Administrator Danych Osobowych

Administratorem danych osobowych jest Towarzystwo Ubezpieczeń Wzajemnych Polski Zakład Ubezpieczeń Wzajemnych z siedzibą przy ul. Ogrodowej 58, 00-876 Warszawa.

Przetwarzanie danych przez administratora

Administrator może przetwarzać Pani/Pana dane w celu:

- wykonania umowy ubezpieczenia na podstawie art. 6 ust. 1 lit. b ogólnego rozporządzenia o ochronie danych osobowych nr 2016/679 („Rozporządzenie 2016/679"), a w zakresie danych o stanie zdrowia (informacji o rodzaju zrealizowanych usług medycznych), które przekazane zostaną administratorowi przez PZU Zdrowie SA z siedzibą w Warszawie, na podstawie wyrażonej przez Panią/Pana zgody, zgodnie z art. 6 ust. 1 lit. a Rozporządzenia 2016/679;
- marketingu bezpośredniego produktów i usług własnych administratora, obejmującego również profilowanie w celu dostosowania przesyłanych treści marketingowych – podstawą prawną przetwarzania jest niezbędność przetwarzania do realizacji prawnie uzasadnionego interesu administratora (art. 6 ust. 1 lit. f Rozporządzenia 2016/679); uzasadnionym interesem administratora jest dostarczanie klientom informacji o produktach ubezpieczeniowych i innych produktach finansowych oferowanych przez Towarzystwo Ubezpieczeń Wzajemnych Polski Zakład Ubezpieczeń Wzajemnych; w przypadku wyrażenia zgody na przetwarzanie danych osobowych w celach marketingowych, gdy nie posiada Pani/Pan ubezpieczenia w Towarzystwie Ubezpieczeń Wzajemnych Polskim Zakładzie Ubezpieczeń Wzajemnych, tj. po rozwiązaniu umowy ubezpieczenia na podstawie wyrażonej przez Panią/Pana zgody, zgodnie z art. 6 ust. 1 lit. a Rozporządzenia 2016/679; do celów marketingu wykorzystywane będą podane dane kontaktowe oraz dane kontaktowe pozyskane w przyszłości;
- dochodzenia ewentualnych roszczeń lub obrony przed roszczeniami związanymi z umową ubezpieczenia – podstawą prawną przetwarzania jest niezbędność przetwarzania do realizacji prawnie uzasadnionego interesu administratora (art. 6 ust. 1 lit. f Rozporządzenia 2016/679); uzasadnionym interesem administratora jest możliwość dochodzenia przez niego roszczeń oraz obrony przed roszczeniami wynikającymi z zawartej umowy ubezpieczenia;
- podejmowania ewentualnych czynności w związku z przeciwdziałaniem wypłacaniu nienależnych świadczeń lub odszkodowań oraz przeciwdziałaniem przestępstwom – podstawą prawną przetwarzania jest niezbędność przetwarzania do realizacji prawnie uzasadnionego interesu administratora (art. 6 ust. 1 lit. f Rozporządzenia 2016/679); uzasadnionym interesem administratora jest możliwość przeciwdziałania wypłacaniu nienależnych świadczeń lub odszkodowań oraz przeciwdziałania przestępstwom, w tym w szczególności oszustwom ubezpieczeniowym poprzez monitorowanie, identyfikowanie, zgłaszanie i rejestrowanie zdarzeń mogących stanowić czyn zabroniony;
- wypełnienia przez administratora obowiązków związanych z przeciwdziałaniem praniu pieniędzy oraz finansowaniu terroryzmu – podstawą prawną przetwarzania danych jest niezbędność do wypełnienia obowiązku prawnego ciążącego na administratorze wynikającego z przepisów o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (art. 6 ust. 1 lit. c Rozporządzenia 2016/679);
- wypełniania przez administratora obowiązków dotyczących przechowywania dowodów księgowych dotyczących umów ubezpieczenia oraz obowiązku przechowywania dokumentacji z postępowania obsługowego dla celów dowodowych – podstawą prawną przetwarzania jest niezbędność do wypełnienia obowiązku prawnego ciążącego na administratorze wynikającego

z przepisów prawa, w szczególności z przepisów ustawy o rachunkowości (art. 6 ust. 1 lit. c Rozporządzenia 2016/679).

Podanie danych osobowych w związku z zawieraną umową jest dobrowolne, jednak konieczne do wykonywania umowy ubezpieczenia – bez podania danych osobowych nie jest możliwe objęcie ubezpieczeniem.

Podanie danych osobowych w celach marketingowych jest dobrowolne.

Kontakt z administratorem

We wszystkich sprawach z zakresu ochrony danych osobowych może Pani/Pan kontaktować się z wyznaczonym przez administratora Inspektorem Ochrony Danych. Taki kontakt może się odbyć drogą elektroniczną na adres e-mail IOD@tuwpzuw.pl lub pisemnie na adres siedziby administratora, z dopiskiem „Inspektor Ochrony Danych".

Odbiorcy danych

Pani/Pana dane osobowe mogą być udostępnione ubezpieczającemu, podmiotom i organom upoważnionym do przetwarzania tych danych na podstawie przepisów prawa.
Pani/Pana dane osobowe mogą być przekazywane innym podmiotom z Grupy PZU, jeśli wyrażona została zgoda na takie przekazanie.
Pani/Pana dane osobowe mogą być przekazywane podmiotom przetwarzającym dane osobowe na zlecenie administratora, w szczególności: osobom zajmującym się windykacją należności, agencjom marketingowym, przy czym takie podmioty i osoby przetwarzają dane na podstawie pisemnej umowy z administratorem lub podmiotem przetwarzającym dane osobowe w imieniu administratora i wyłącznie zgodnie z ich poleceniami. Pani/Pana dane osobowe mogą być udostępnione podmiotom w państwach poza Europejskim Obszarem Gospodarczym w związku z realizacją umowy ubezpieczenia.

Prawa osób, których dane dotyczą

Przysługuje Pani/Panu prawo dostępu do swoich danych osobowych oraz prawo żądania ich sprostowania, usunięcia lub ograniczenia ich przetwarzania.
W zakresie, w jakim przetwarzanie odbywa się w sposób zautomatyzowany na podstawie zgody lub na podstawie umowy przysługuje Pani/Panu prawo do przenoszenia danych osobowych, tj. prawo do otrzymania od administratora Pani/Pana danych osobowych w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, celem przesłania tych danych innemu administratorowi.
W zakresie, w jakim podstawą przetwarzania Pani/Pana danych osobowych jest przesłanka prawnie uzasadnionego interesu administratora, przysługuje Pani/Panu prawo do wniesienia w dowolnym momencie sprzeciwu wobec przetwarzania Pani/Pana danych osobowych, z przyczyn związanych z Pani/Pana szczególną sytuacją. W szczególności przysługuje Pani/Panu prawo do sprzeciwu wobec przetwarzania danych na potrzeby marketingu bezpośredniego, w tym profilowania. Po przyjęciu wniosku w tej sprawie administrator jest zobowiązany do zaprzestania przetwarzania danych w tym celu, chyba że administrator wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą lub praw do ustalenia, dochodzenia lub obrony przed roszczeniami.
W zakresie, w jakim podstawą przetwarzania Pani/Pana danych osobowych jest zgoda, ma Pani/Pan prawo jej wycofania. Zgodę można odwołać w dowolnym momencie. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania dokonanego na podstawie zgody wyrażonej przed jej wycofaniem.

W celu skorzystania z przysługujących Pani/Panu praw należy skontaktować się z administratorem lub z wyznaczonym przez niego Inspektorem Ochrony Danych, korzystając ze wskazanych powyżej danych kontaktowych.
W przypadku uznania, że administrator przetwarza Pani/Pana dane osobowe z naruszeniem przepisów prawa, przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych - w szczególności w państwie członkowskim UE Pani/Pana zwykłego pobytu, miejsca pracy lub miejsca popełnienia domniemanego naruszenia. W Polsce takim organem nadzorczym jest Prezes Urzędu Ochrony Danych Osobowych.

Zasady pobierania opłat
Postępowanie w sprawie składanych wniosków jest nieodpłatne.

Bezpieczeństwo danych

W celu zapewnienia integralności i poufności danych wdrożono procedury umożliwiające dostęp do danych osobowych jedynie osobom upoważnionym i wyłącznie w zakresie, w jakim jest to niezbędne ze względu na wykonywane przez nie zadania. Zastosowano rozwiązania organizacyjne i techniczne w celu zapewnienia, że wszystkie operacje na danych osobowych są rejestrowane i dokonywane tylko przez osoby uprawnione.
Podjęto ponadto wszelkie niezbędne działania, by także podwykonawcy i inne podmioty współpracujące dawały gwarancję stosowania odpowiednich środków bezpieczeństwa w każdym przypadku, gdy przetwarzają dane osobowe na zlecenie Administratora.
Na bieżąco prowadzi się analizę ryzyka i monitoruje adekwatność stosowanych zabezpieczeń danych do identyfikowanych zagrożeń. W razie konieczności wdrażane są dodatkowe środki służące zwiększeniu bezpieczeństwa danych.

Inne ujawniane informacje (pliki Cookies)

Strona internetowa wykorzystuje technologię plików cookie (ciasteczka), czyli niewielkie informacje tekstowe, przechowywane na urządzeniu końcowym Użytkownika (np. komputerze, tablecie, smartfonie). Cookies mogą być odczytywane przez system teleinformatyczny Administratora strony.

Służą one do zapewnienia optymalnej obsługi podczas wizyty na naszej stronie oraz umożliwiają szybszy i łatwiejszy dostęp do informacji. Pliki Cookies nie służą do przetwarzania danych osobowych a ich zawartość nie pozwala na identyfikacje Użytkownika. Przy następnej wizycie z tego samego urządzenia przeglądarka może sprawdzić, czy na urządzeniu zapisany jest odpowiedni plik cookie (tzn. plik zawierający nazwę strony) i przesłać zawarte w nim dane ponownie do strony, która zapisała ciasteczko. Dzięki temu można rozpoznać, że dany Użytkownik odwiedził ją w przeszłości, i w niektórych przypadkach dopasować prezentowaną treść do odbiorcy.
Z uwagi na czas życia cookies i innych podobnych technologii, stosujemy dwa zasadnicze rodzaje tych plików:

- **sesyjne** - pliki tymczasowe przechowywane w urządzeniu końcowym Użytkownika do czasu wylogowania, opuszczenia strony internetowej i aplikacji lub wyłączenia oprogramowania (przeglądarki internetowej);
- **stałe** - przechowywane w urządzeniu końcowym Użytkownika przez czas określony w parametrach plików cookies lub do czasu ich usunięcia przez Użytkownika.

  Ze względu na cel, jakiemu służą pliki cookies i inne podobne technologie, stosujemy ich następujące rodzaje:

- **niezbędne do działania usługi i aplikacji** - umożliwiające korzystanie z naszych usług, np. uwierzytelniające pliki cookies wykorzystywane do usług wymagających uwierzytelniania;
- **pliki służące do zapewnienia bezpieczeństwa**, np. wykorzystywane do wykrywania nadużyć w zakresie uwierzytelniania;
- **wydajnościowe** - umożliwiające zbieranie informacji o sposobie korzystania ze stron internetowych i aplikacji;
- **funkcjonalne** - umożliwiające "zapamiętanie" wybranych przez Użytkownika ustawień i personalizację interfejsu Użytkownika, np. w zakresie wybranego języka lub regionu, z którego pochodzi Użytkownik, rozmiaru czcionki, wyglądu strony internetowej i aplikacji itp.;
- **reklamowe** - umożliwiające dostarczanie Użytkownikom treści reklamowych bardziej dostosowanych do ich zainteresowań;
- **statystyczne** - służące do zliczana statystyk dotyczących stron internetowych i aplikacji.

  Użytkownik może w każdej chwili usunąć umieszczone pliki cookie lub zablokować umieszczanie plików cookie za pomocą opcji dostępnych w jego przeglądarce internetowej. Usunięcie lub zablokowanie umieszczania plików cookie może spowodować utrudnienia korzystania z serwisu, a nawet uniemożliwić korzystanie z niektórych jego opcji. Zarządzanie i usuwanie plików cookie różni się w zależności od używanej przeglądarki. Dokładne informacje na ten temat można uzyskać, korzystając z funkcji Pomoc w przeglądarce. Większość przeglądarek oferuje możliwość akceptowania lub odrzucania wszystkich plików cookie, akceptowania tylko niektórych rodzajów albo informowania użytkownika za każdym razem, gdy strona internetowa próbuje je zapisać. Użytkownik może również z łatwością usuwać pliki cookie, które zostały już zapisane na urządzeniu przez przeglądarkę.

  Zmiana warunków przechowywania lub otrzymywania plików cookies jest możliwa poprzez konfigurację ustawień w przeglądarkach internetowych m.in.:
  - w przeglądarce Internet Explorer
  - w przeglądarce Mozilla Firefox
  - w przeglądarce Chrome
  - w przeglądarce Opera

Dowiedz się jak wyłączyć pliki Cookies w różnych przeglądarkach

Internet Explorer: Blokowanie lub dopuszczanie wszystkich plików Cookies:
1. Kliknij przycisk **Narzędzia**, a następnie kliknij polecenie **Opcje internetowe,**
2. Kliknij kartę **Prywatność**, a następnie w obszarze **Ustawienia** przesuń suwak do najwyższego położenia, aby zablokować wszystkie pliki Cookies, lub do najniższego położenia, aby zezwolić na wszystkie pliki Cookies, a następnie kliknij przycisk **OK,**
3. Zablokowanie plików Cookies może uniemożliwić poprawne wyświetlanie niektórych stron sieci Web.

Firefox: Aby sprawdzić lub zmienić ustawienia:
1. Na górze okna Firefoksa naciśnij przycisk **Firefox** (w systemie Windows XP kliknij menu **Narzędzia**) i wybierz **Opcje,**
2. Wybierz panel **Prywatność,**
3. Z menu rozwijanego elementu **Program Firefox**: wybierz opcję **będzie używał ustawień historii użytkownika,**
4. Odznacz opcję **Akceptuj ciasteczka,** aby wyłączyć obsługę ciasteczek, lub zaznacz, aby ponownie ją włączyć.

Chrome: Dostosowywanie uprawnień plików Cookies i danych stron:
1. Kliknij menu Chrome na pasku narzędzi przeglądarki.

2. Wybierz **Ustawienia,**
3. W sekcji „Prywatność” kliknij przycisk **Ustawienia treści,**
4. W sekcji „Pliki Cookies” możesz zmienić następujące ustawienia plików:
    1. Usuwanie plików Cookies
    2. Domyślne blokowanie plików Cookies
        - Blokowanie wszystkich plików Cookies
        - Blokowanie tylko plików Cookies innych firm
    3. Domyśle zezwalanie na pliki Cookies

Opera: Wyłączanie i włączania ciasteczek:

1. Na górze okna przeglądarki Opera naciśnij przycisk **Opera** i wybierz **Ustawienia**, a następnie **Preferencje**. Ten sam efekt możesz uzyskać naciskając kombinację klawiszy CTRL+F12,
2. Wybierz zakładkę **Zaawansowane,**
3. Wybierz z lewej strony pozycję **Ciasteczka,**
4. Zaznacz odpowiednią opcję, w zależności of preferencji:
    - Akceptuj ciasteczka
    - Akceptuj ciasteczka tylko dla witryny, którą odwiedzam
    - **Nigdy nie akceptuj ciasteczek**

Lista plików Cookie

Przekazywanie danych poza EOG

Poziom ochrony danych osobowych poza Europejskim Obszarem Gospodarczym (EOG) różni się od tego zapewnianego przez prawo europejskie. Z tego powodu dane osobowe są przekazywane poza EOG tylko wtedy, gdy jest to konieczne, i z zapewnieniem odpowiedniego stopnia ochrony, przede wszystkim poprzez:

- współpracę z podmiotami przetwarzającymi dane osobowe w państwach, w odniesieniu do których została wydana stosowna decyzja Komisji Europejskiej;
- stosowanie standardowych klauzul umownych wydanych przez Komisję Europejską;
- stosowanie wiążących reguł korporacyjnych zatwierdzonych przez właściwy organ nadzorczy;
- w razie przekazywania danych do USA – współpracę z podmiotami uczestniczącymi w programie Tarcza Prywatności (Privacy Shield) zatwierdzonym decyzją Komisji Europejskiej.
  Administrator zawsze informuje o zamiarze przekazania danych osobowych poza EOG na etapie ich zbierania.