Polityka prywatności

Grupa PZU przywiązuje szczególną wagę do poszanowania prywatności użytkowników odwiedzających naszą stronę internetową. Gromadzone, w dziennikach logów, dane 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 formularzach kontaktowych. Dla zapewnienia jak najwyższej jakości serwisu, okazjonalnie analizujemy pliki z logami w celu określenia, które strony odwiedzane są najczęściej, jakie przeglądarki stron WWW są stosowane, czy struktura strony nie zawiera błędów, itp.

Odnośniki do innych stron internetowych

Polityka prywatności dotyczy tylko stron internetowych spółek Grupy PZU. W przypadku umieszczenia na stronie internetowej spółki Grupy PZU 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

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 PZU Cash SA 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 po 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.

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 ponad to 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 i 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 szyfro- wania 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 (ADO) jest PZU Cash SA, Rondo Ignacego Daszyńskiego 4, 00-843 Warszawa. Kontakt z administratorem jest możliwy za pośrednictwem adresu e-mail: spolka_cash@pzu.pl lub pisemnie na wyżej wskazany adres siedziby Administratora.

Przetwarzanie danych przez Administratora
W związku z prowadzoną działalnością gospodarczą administrator zbiera i przetwarza dane osobowe zgodnie z właściwymi przepisami, w tym w szczególności z RODO (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), i przewidzianymi w nich zasadami przetwarzania danych.

Administrator zapewnia przejrzystość przetwarzania danych, w szczególności zawsze informuje o przetwarzaniu danych w momencie ich zbierania, w tym o celu i podstawie prawnej przetwarzania – np. przy zawieraniu umowy sprzedaży towarów lub usług. Administrator dba o to, by dane były zbierane tylko w zakresie niezbędnym do wskazanego celu i przetwarzane tylko przez okres, w jakim jest to niezbędne. Przetwarzając dane, Administrator zapewnia ich bezpieczeństwo i poufność oraz dostęp do informacji o przetwarzaniu osobom, których dane dotyczą. Gdyby pomimo stosowanych środków bezpieczeństwa doszło do naruszenia ochrony danych osobowych (np. „wycieku" danych lub ich utraty), Administrator poinformuje o takim zdarzeniu osoby, których dane dotyczą, w sposób zgodny z przepisami.

Odbiorcy danych
W związku z prowadzeniem działalności wymagającej przetwarzania dane osobowe są ujawniane zewnętrznym podmiotom, w tym w szczególności dostawcom odpowiedzialnym za obsługę systemów informatycznych i sprzętu, podmiotom świadczącym usługi prawne lub księgowe, kurierom, agencjom marketingowym czy rekrutacyjnym. Dane są też ujawniane podmiotom powiązanym z Administratorem, w tym spółkom z jego grupy kapitałowej. Więcej informacji nt. grupy kapitałowej Administratora można znaleźć . Administrator zastrzega sobie prawo ujawnienia wybranych informacji dotyczących osoby, której dane dotyczą, właściwym organom bądź osobom trzecim, które zgłoszą żądanie udzielenia takich informacji, opierając się na odpowiedniej podstawie prawnej oraz zgodnie z przepisami obowiązującego prawa.

Okres przetwarzania danych osobowych
Okres przetwarzania danych przez Administratora zależy od rodzaju świadczonej usługi i celu przetwarzania. Okres przetwarzania danych może także wynikać z przepisów, gdy stanowią one podstawę przetwarzania. W przypadku przetwarzania danych na podstawie uzasadnionego interesu Administratora – np. ze względów bezpieczeństwa – dane przetwarzane są przez okres umożliwiający realizację tego interesu lub do zgłoszenia skutecznego sprzeciwu względem przetwarzania danych. Jeśli przetwarzanie odbywa się na podstawie zgody, dane przetwarzane są do jej wycofania. Gdy podstawę przetwarzania stanowi niezbędność do zawarcia i wykonania umowy, dane są przetwarzane do momentu jej rozwiązania.

Okres przetwarzania danych może być przedłużony w przypadku, gdy przetwarzanie jest niezbędne do ustalenia lub dochodzenia roszczeń lub obrony przed roszczeniami, a po tym

okresie – jedynie w przypadku i w zakresie, w jakim będą wymagać tego przepisy prawa. Po upływie okresu przetwarzania dane są nieodwracalnie usuwane lub anonimizowane.

Prawa osób, których dane dotyczą

Osoba, której dane dotyczą to każda osoba fizyczna, której dane osobowe przetwarzane są przez Administratora, np. osoba odwiedzająca lokal Administratora lub kierująca do niego zapytanie w formie e-maila.

PZU Cash SA zapewnia podmiotom danych realizację uprawnień wynikających z RODO. Osobom, których dane dotyczą, przysługują następujące prawa:

- **prawo do informacji o przetwarzaniu danych osobowych** – na tej podstawie osobie zgłaszającej żądanie Administrator przekazuje informację o przetwarzaniu danych, w tym przede wszystkim o celach i podstawach prawnych przetwarzania, zakresie posiadanych danych, podmiotach, którym są ujawniane, i planowanym terminie usunięcia danych;

- **prawo uzyskania kopii danych** – na tej podstawie Administrator przekazuje kopię przetwarzanych danych dotyczących osoby zgłaszającej żądanie;

- **prawo do sprostowania** – Administrator zobowiązany jest usuwać ewentualne niezgodności lub błędy przetwarzanych danych osobowych oraz uzupełniać je, jeśli są niekompletne;

- **prawo do usunięcia danych** – na tej podstawie można żądać usunięcia danych, których przetwarza- nie nie jest już niezbędne do realizowania żadnego z celów, dla których zostały zebrane;

- **prawo do ograniczenia przetwarzania** – w razie zgłoszenia takiego żądania Administrator zaprzestaje wykonywania operacji na danych osobowych – z wyjątkiem operacji, na które wyraziła zgodę osoba, której dane dotyczą – oraz ich przechowywania, zgodnie z przyjętymi zasadami retencji lub dopóki nie ustaną przyczyny ograniczenia przetwarzania danych (np. zostanie wydana decyzja organu nadzorcze- go zezwalająca na dalsze przetwarzanie danych);

- **prawo do przenoszenia danych** – na tej podstawie – w zakresie, w jakim dane są przetwarzane w związku z zawartą umową lub wyrażoną zgodą – Administrator wydaje dane dostarczone przez osobę, której one dotyczą, w formacie pozwalającym na ich odczyt przez komputer. Możliwe jest także zażą- danie przesłania tych danych innemu podmiotowi – jednak pod warunkiem, że istnieją w tym zakresie techniczne możliwości zarówno po stronie Administratora, jak również tego innego podmiotu;

- **prawo sprzeciwu wobec przetwarzania danych w celach marketingowych** – osoba, której dane dotyczą, może w każdym momencie sprzeciwić się przetwarzaniu danych osobowych w celach marketingowych, bez konieczności uzasadnienia takiego sprzeciwu;

- **prawo sprzeciwu wobec innych celów przetwarzania danych** – osoba, której dane dotyczą, może w każdym momencie sprzeciwić się przetwarzaniu danych osobowych, które odbywa się na podstawie uzasadnionego interesu Administratora (np. dla celów analitycznych lub statystycznych albo ze wzglę- dów związanych z ochroną mienia);

sprzeciw w tym zakresie powinien zawierać uzasadnienie;

- **prawo wycofania zgody** – jeśli dane przetwarzane są na podstawie wyrażonej zgody, osoba, której dane dotyczą, ma prawo ją wycofać w dowolnym momencie, co jednak nie wpływa na zgodność z prawem przetwarzania dokonanego przed wycofaniem zgody;

- **prawo do skargi** – w przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO lub inne przepisy dotyczące ochrony danych osobowych, osoba, której dane dotyczą, może złożyć skargę do Prezesa Urzędu Ochrony Danych Osobowych. W celu skorzystania z powyższych praw należy skontaktować się z Administratorem danych lub z Inspektorem Ochrony Danych, korzystając ze wskazanych wyżej danych kontaktowych.

Zgłaszanie żądań związanych z realizacją praw
Wniosek dotyczący realizacji praw podmiotów danych można złożyć:
- w formie pisemnej na adres: Rondo Ignacego Daszyńskiego 4, 00-843 Warszawa;
- drogą e-mailową na adres: kontakt@portalcash.pl.

Jeżeli Administrator nie będzie w stanie zidentyfikować osoby składającej wniosek na podstawie dokonanego zgłoszenia, zwróci się do wnioskodawcy o dodatkowe informacje. Wniosek może być złożony osobiście lub za pośrednictwem pełnomocnika (np. członka rodziny). Ze względu na bezpieczeństwo danych Administrator zachęca do posługiwania się pełnomocnictwem w formie poświadczonej przez notariusza lub upoważnionego radcę prawnego bądź adwokata, co istotnie przyspieszy weryfikację autentyczności wniosku. Odpowiedź na zgłoszenie powinna zostać udzielona w ciągu miesiąca od jego otrzymania. W razie konieczności przedłużenia tego terminu Administrator informuje wnioskodawcę o przyczynach opóźnienia.

Odpowiedź udzielana jest za pośrednictwem poczty tradycyjnej, chyba że wniosek został złożony drogą e-mailową lub zażądano przekazania odpowiedzi w formie elektronicznej.

Zasady pobierania opłat
Postępowanie w sprawie składanych wniosków jest nieodpłatne.

Cele oraz podstawy prawne przetwarzania

Korespondencja e-mailowa i tradycyjna
W przypadku kierowania do Administratora za pośrednictwem poczty e-mail lub tradycyjnej korespondencji niezwiązanej z usługami świadczonymi na rzecz nadawcy lub inną zawartą z nim umową, dane osobowe zawarte w tej korespondencji są przetwarzane wyłącznie w celu komunikacji i rozwiązania sprawy, której dotyczy korespondencja.

Podstawą prawną przetwarzania jest uzasadniony interes Administratora (art. 6 ust. 1 lit f RODO) polegający na prowadzeniu korespondencji kierowanej do niego w związku z jego działalnością gospodarczą.

Administrator przetwarza jedynie dane osobowe istotne dla sprawy, której dotyczy korespondencja. Całość korespondencji jest przechowywana w sposób zapewniający bezpieczeństwo zawartych w niej danych osobowych (oraz innych informacji) i ujawniana jedynie osobom upoważnionym.

Kontakt telefoniczny
W przypadku kontaktowania się z Administratorem drogą telefoniczną, w sprawach niezwiązanych z zawartą umową lub świadczonymi usługami, Administrator może żądać podania danych osobowych tylko wówczas, gdy będzie to niezbędne do obsługi sprawy, której dotyczy kontakt. Podstawą prawną jest w takim wypadku uzasadniony interes Administratora (art. 6 ust. 1 lit f RODO) polegający na konieczności rozwiązania zgłoszonej sprawy związanej z prowadzoną przez niego działalnością gospodarczą.

Rozmowy telefoniczne mogą być także nagrywane – w takim wypadku na początku rozmowy przekazywana jest stosowna informacja. Rozmowy są rejestrowane w celu monitorowania jakości świadczonej usługi oraz weryfikacji pracy konsultantów, a także w celach statystycznych. Nagrania są dostępne wyłącznie dla pracowników Administratora oraz osób obsługujących infolinię Administratora.
Dane osobowe w postaci nagrania rozmowy są przetwarzane:

- **w celach związanych z obsługą klientów i interesantów za pośrednictwem infolinii, jeśli Administra- tor udostępnia taką usługę** – podstawą prawną przetwarzania jest niezbędność przetwarzania do świadczenia usługi (art. 6 ust. 1 lit. b RODO);

- **w celu monitorowania jakości obsługi i weryfikacji pracy konsultantów obsługujących infolinię, jak również w celach analitycznych i statystycznych** – podstawą prawną przetwarzania jest uzasadniony interes Administratora (art. 6 ust. 1 lit f RODO) polegający na

dbaniu o jak najwyższą jakość obsługi na rzecz klientów i interesantów, a także pracy konsultantów oraz prowadzenie analiz statystycznych dotyczących komunikacji telefonicznej.

Monitoring wizyjny oraz kontrola wstępu
W celu zapewnienia bezpieczeństwa osób i mienia Administrator stosuje monitoring wizyjny oraz kontroluje wstęp do lokali i na teren przez niego zarządzany. Zebrane w ten sposób dane nie są wykorzystywane do żadnych innych celów.

Dane osobowe w postaci nagrań z monitoringu oraz dane zbierane w rejestrze wejść i wyjść są przetwarzane w celu zapewnienia bezpieczeństwa i porządku na terenie obiektu oraz ewentualnie w celu obrony przed roszczeniami lub ich dochodzenia. Podstawą przetwarzania danych osobowych jest uzasadniony interes Administratora (art. 6 ust. 1 lit. f RODO) polegający na zapewnieniu bezpieczeń- stwa mienia Administratora oraz ochrony jego praw.

Rekrutacja
W ramach procesów rekrutacyjnych Administrator oczekuje przekazywania danych osobowych (np. w CV lub życiorysie) jedynie w zakresie określonym w przepisach prawa pracy. W związku z tym nie należy przekazywać informacji w szerszym zakresie. W razie, gdy przesłane aplikacje będą zawierać dodatkowe dane, nie będą one wykorzystywane ani uwzględniane w procesie rekrutacyjnym.

Dane osobowe są przetwarzane:

- w celu wykonania obowiązków wynikających z przepisów prawa, związanych z procesem zatrudnienia, w tym przede wszystkim Kodeksu pracy – podstawą prawną przetwarzania jest obowiązek prawny ciążący na Administratorze (art. 6 ust. 1 lit c RODO w związku z przepisami Kodeksu pracy);

- w celu przeprowadzenia procesu rekrutacji w zakresie danych niewymaganych przepisami prawa, a także dla celów przyszłych procesów rekrutacyjnych – podstawą prawną przetwarzania jest zgoda (art. 6 ust. 1 lit a RODO);

- w celu ustalenia lub dochodzenia ewentualnych roszczeń lub obrony przed takimi roszczeniami – podstawą prawną przetwarzania danych jest prawnie uzasadniony interes Administratora (art. 6 ust. 1 lit f RODO).

Zbieranie danych w związku ze świadczeniem usług lub wykonywaniem innych umów
W razie zbierania danych dla celów związanych z wykonaniem konkretnej umowy, Administrator przekazuje osobie, której dane dotyczą, szczegółowe informacje dotyczące przetwarzania jej danych osobowych w momencie zawierania umowy.

Zbieranie danych w innych przypadkach

W związku z prowadzoną działalnością Administrator zbiera dane osobowe także w innych przypadkach – np. podczas spotkań biznesowych, na eventach branżowych czy poprzez wymianę wizytówek – w celach związanych z inicjowaniem i utrzymywaniem kontaktów biznesowych. Podstawą prawną przetwarzania jest w tym wypadku uzasadniony interes Administratora (art. 6 ust. 1 lit f RODO) pole- gający na tworzeniu sieci kontaktów w związku z prowadzoną działalnością.

Dane osobowe zebrane w takich przypadkach przetwarzane są wyłącznie w celu, dla jakiego zostały zebrane, a Administrator zapewnia ich odpowiednią ochronę.

Bezpieczeństwo danych

W celu zapewnienia integralności i poufności danych Administrator wdrożył 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. Administrator stosuje rozwiązania organizacyjne i techniczne w celu zapewnienia, że wszystkie operacje na danych osobowych są rejestrowane i dokonywane tylko przez osoby uprawnione.

Administrator podejmuje ponadto wszelkie niezbędne działania, by także jego podwykonawcy i inne podmioty współpracujące dawały gwarancję stosowania odpowiednich środków bezpieczeństwa w każdym przypadku, gdy przetwarzają dane osobowe na zlecenie Administratora.
Administrator prowadzi na bieżąco analizę ryzyka i monitoruje adekwatność stosowanych zabezpie- czeń danych do identyfikowanych zagrożeń. W razie konieczności Administrator wdraża dodatkowe środki służące zwiększeniu bezpieczeństwa danych.

Profilowanie

Co to jest profilowanie?
Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycz nej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Profilowanie składa się z trzech elementów:

- forma przetwarzania jest zautomatyzowana (co najmniej w części);
- przetwarzanie dotyczy danych osobowych;
- celem przetwarzania jest ocena czynników osobowych, przypisanie określonych cech lub

przewidywanie zachowań.

Co to jest zautomatyzowane przetwarzanie danych?
O zautomatyzowanym przetwarzaniu danych mówimy wtedy, gdy dane przetwarzane są wyłącznie przez algorytm (komputer), tj. bez udziału człowieka.

Administrator danych osobowych ma obowiązek informowania o zautomatyzowanym przetwarzaniu, w tym o profilowaniu jeśli takie przetwarzanie wywołuje skutki prawne lub istotnie wpływa na daną osobę fizyczną. Osoba, której dane są przetwarzane ma natomiast prawo do sprzeciwu na zautomatyzowane przetwarzanie, w tym profilowanie. RODO gwarantuje również prawo, aby nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu.

Przykłady profilowania i zautomatyzowanego podejmowania decyzji
- reklama internetowa (web tracking) w celu dostosowania wyświetlanych reklam do oczekiwań użytkownika;
- marketing bezpośredni własnych produktów i usług;
- analiza szkodowości klientów na wewnętrzne potrzeby statystyczne.
- decyzje w oparciu o zautomatyzowane przetwarzanie:
- ocena ryzyka ubezpieczeniowego w celu wyliczenia składki;
- analiza stylu jazdy (telematyka) w celu indywidualizacji składki;
- automatyczne wzywanie pomocy w razie wypadku.

Inspektor Ochrony Danych (IOD)

W sprawach z zakresu ochrony danych osobowych Użytkownicy mogą kontaktować się z wyznaczonym przez danego Administratora Inspektorem Ochrony Danych.

Taki kontakt może się odbyć drogą elektroniczną na adres e-mail: IOD_cash@pzu.pl lub pisemnie na adres PZU Cash SA, IOD, Rondo Ignacego Daszyńskiego 4, 00-843 Warszawa.

Inne ujawniane informacje (pliki cookie)

Prawie każda strona internetowa wykorzystuje technologię plików cookie. Podczas wizyt na naszej stronie, na komputerze Użytkownika zapisywane są fragmenty kodu, w których zapisano ustawienia użytkownika.

Służą one do zapewnienia optymalnej obsługi podczas wizyty na naszej stronie oraz umożliwiają szybszy i łatwiejszy dostęp do informacji. Pliki cookie nie służą do przetwarzania danych osobowych a ich zawartość nie pozwala na identyfikację użytkownika. Przy następnej

wizycie z tego samego urzą- dzenia 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 plik cookie. Dzięki temu można rozpoznać, że dany Użytkownik odwiedził ją w przeszłości i w niektórych przypadkach dopasować prezentowaną treść do odbiorcy.

Okres przechowywania plików cookie
Z uwagi na czas życia cookie 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 cookie lub do czasu ich usunięcia przez Użytkownika.

Pliki cookie dzielimy na dwie kategorie.
Niezbędne pliki cookie to pliki potrzebne do prawidłowego funkcjonowania naszych stron i aplikacji. Służą one do zapewnienia bezpieczeństwa, podtrzymania sesji użytkownika logującego się do naszych serwisów internetowych, a także zapamiętywania preferencji. Nie udostępniamy możliwości wyłącze- nia tego typu plików cookie z poziomu okna "Zarządzanie prywatnością". Usunięcie lub zablokowanie umieszczania omawianych plików cookie możliwe jest z poziomu przeglądarki internetowej, ale może spowodować utrudnienia w korzystaniu z naszych stron i aplikacji, a w skrajnych przypadkach nawet uniemożliwić korzystanie z niektórych lub wszystkich opcji.

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

- **niezbędne do działania usługi i aplikacji** - umożliwiające korzystanie z naszych usług, np. uwierzytelniające pliki cookie 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 np. wykrywanie niektórych problemów technicznych;

- **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.

Opcjonalne pliki cookie to zestaw plików wykorzystywanych głównie przez systemy analityczne i reklamowe zaufanych partnerów. Nie są one potrzebne do korzystania z naszych usług. Podobnie jak niezbędne pliki cookie, tak i ta kategoria plików przechowuje anonimowe informacje. Użytkownik może w każdej chwili usunąć umieszczone pliki cookie lub zablokować umieszczanie ich za pomocą opcji dostępnych w jego przeglądarce internetowej lub z poziomu okna "Zarządzanie prywatnością".

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

- **analityczne i statystyczne** - umożliwiają zbieranie informacji o sposobie korzystania ze stron internetowych i aplikacji w odniesieniu do zachowania w tych serwisach np. przejść pomiędzy podstronami serwisu internetowego oraz analizowania źródeł ruchu – skąd Użytkownicy trafiają do nas;
- **służące do personalizacji i testów A/B** - zmian wyglądu serwisów internetowych i aplikacji w zależności od preferencji Użytkownika oraz dotychczasowych zachowań;
- **reklamowe** - umożliwiające dostarczanie Użytkownikom treści reklamowych bardziej dostosowanych do ich zainteresowań, są to nasz pliki cookies, jak i pliki cookie dostawców zewnętrznych, wykorzystywane w szczególności do prawidłowych rozliczeń z wydawcami lub dotarcia z reklamami do osób, które odwiedzały nasze witryny.

Zarządzanie i usuwanie plików cookie niezbędnych i opcjonalnych z poziomu przeglądarki internetowej 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 cookie jest możliwa poprzez konfigurację ustawień w przeglądarkach internetowych m.in.:

- w przeglądarce Chrome
- w przeglądarce Internet Explorer
- w przeglądarce Mozilla Firefox
- w przeglądarce Opera
- w przeglądarce Safari

Przekazywanie danych poza EOG

Poziom ochrony danych osobowych poza Europejskim Obszarem Gospodarczym (EOG) różni się od tego zapewnianego przez prawo europejskie. Z tego powodu Administrator przekazuje dane osobowe 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.

Administrator zawsze informuje o zamiarze przekazania danych osobowych poza EOG na etapie ich zbierania.