POLSKIE STOWARZYSZENIE TŁUMACZY KONFERENCYJNYCH

POLITYKA OCHRONY DANYCH OSOBOWYCH

Niniejszy dokument określa zasady ochrony i przetwarzania danych osobowych przez Polskie Stowarzyszenie Tłumaczy Konferencyjnych w Warszawie („**PSTK**").
Przykładamy dużą wagę do ochrony prywatności, traktując dane osobowe z należytą starannością i uwzględnieniem zasad wynikających z przepisów dotyczących ochrony danych osobowych.
Niniejszy dokument określa, w jaki sposób zbieramy, wykorzystujemy i chronimy zasoby stanowiące dane osobowe w rozumieniu obowiązujących przepisów, a także wskazuje cele wykorzystywania takich danych oraz okres ich przechowywania. Znajdują się tu również informacje o uprawnieniach przysługujących w związku z przetwarzaniem przez PSTK danych osobowych.

Administrator danych osobowych

Jako administrator danych osobowych PSTK jest odpowiedzialne za zbieranie i przetwarzanie danych osobowych w związku z prowadzeniem swojej działalności.
Pełne dane administratora danych osobowych:
Polskie Stowarzyszenie Tłumaczy Konferencyjnych
00-029 Warszawa, ul. Nowy Świat 33/13
KRS: 0000626849, REGON: 364953956, NIP: 5272774592
e-mail: kontakt@pstk.org.pl
We wszelkich sprawach dotyczących ochrony danych osobowych można się z nami kontaktować pisemnie na adres siedziby lub elektronicznie na ww. adres e-mail.
W przypadku braku wyznaczenia inspektora ochrony danych osobowych domniemanymi osobami odpowiedzialnymi za ochronę danych osobowych są członkowie zarządu PSTK oraz osoby upoważnione do przetwarzania danych osobowych.

Podstawy prawne ochrony danych osobowych

Ochrona danych osobowych jest ważnym elementem działalności każdego podmiotu funkcjonującego na obszarze Polski i Unii Europejskiej.
Zasady tej ochrony określa:

- *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* („RODO") oraz
- *ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych* (Dz. U. 2018 poz. 1000).

Zasady przetwarzania danych osobowych

PSTK dokłada starań, aby dane osobowe były przetwarzane w sposób zgodny z prawem, rzetelny, przejrzysty i bezpieczny.

Naczelne zasady, jakimi się kierujemy, są następujące:

- zbieramy dane osobowe w minimalnym zakresie, niezbędnym do realizacji celów, dla których są zbierane;
- cele zbierania danych osobowych mają oparcie w przepisach prawa i są jasno określone;
- dbamy o aktualność i poprawność danych osobowych i niezwłocznie reagujemy na wnioski o sprostowanie czy aktualizację danych;
- realizujemy prawa do: dostępu do danych osobowych oraz ich poprawiania, usunięcia danych osobowych, wycofania zgody na przetwarzanie, ograniczenia przetwarzania, przenoszenia danych, wniesienia sprzeciwu wobec przetwarzania danych oraz niepodlegania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu danych, w tym profilowaniu;
- ograniczamy przechowywanie danych osobowych do okresu niezbędnego dla realizacji celów, dla których są zbierane (o ile nie zachodzą okoliczności mogące wydłużyć okres przechowywania danych);
- chronimy dane osobowe przed utratą, dostępem osób niepowołanych, przypadkową utratą, uszkodzeniem, zniszczeniem lub zmianą oraz innymi bezprawnymi formami przetwarzania;
- jeżeli dane osobowe są udostępniane innym podmiotom, następuje to w sposób zgodny z obowiązującymi przepisami prawa;
- jesteśmy w stanie wykazać (w wymagany prawem sposób), że w odniesieniu do danych osobowych działamy zgodnie z przepisami prawa;
- uwzględniamy ochronę danych w fazie projektowania (np. nowej usługi) oraz zapewniamy domyślną ochronę danych osobowych.

Cele przetwarzania danych osobowych

PSTK przetwarza dane osobowe wyłącznie w określonych, zgodnych z prawem celach, do których przede wszystkim należą:

- sprawy członkostwa (w tym jego procedowania) i bezpośrednio z nimi związane – na podstawie art. ust. 1 lit. a RODO;
- podjęcie działań zmierzających do zawarcia umowy (w tym obsługa kierowanych zgłoszeń, np. przez formularz kontaktowy) – na podstawie art. 6 ust. 1 lit. f RODO;
- realizacja zawartej umowy (w tym kontaktowanie się w celach związanych ze świadczeniem usług) – na podstawie art. 6 ust. 1 lit. b RODO;
- wypełnienie obowiązków prawnych wynikających z obowiązujących przepisów prawa, w tym w szczególności przepisów podatkowych, o rachunkowości oraz ustaw regulujących prowadzoną działalność – na podstawie art. 6 ust. 1 lit. c RODO;

- ochrona żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej – na podstawie art. 9 ust. 2 lit. c RODO;
- dochodzenie i obrona przed ewentualnymi roszczeniami (np. windykacja należności, prowadzenie postępowań sądowych, arbitrażowych i mediacyjnych) – na podstawie art. 6 ust. 1 lit. f RODO;
- marketing usług własnych – na podstawie art. 6 ust. 1 lit. f RODO;
- przechowywanie danych dla celów archiwizacyjnych oraz zapewnienia rozliczalności (wykazania spełnienia przez nas obowiązków wynikających z przepisów prawa) – na podstawie art. 6 ust. 1 lit. f RODO.

Jeżeli zachodzi potrzeba przetwarzania danych w innych celach niż wyżej określone, informujemy o tym oraz w razie takiej potrzeby występujemy o stosowną zgodę.

Sposób zbierania danych osobowych

Dane osobowe otrzymujemy przede wszystkim od naszych członków oraz od osób chcących skorzystać lub korzystających z naszych świadczeń. Mogą się one pojawić także w wyniku realizacji zawartych przez nas umów. Nie kupujemy ani nie handlujemy w żaden sposób danymi osobowymi.

Możemy również gromadzić informacje dotyczące osób, które nie mają bezpośrednich relacji z nami. Może to mieć miejsce nie tylko w wyniku realizacji zawartych przez nas umów, lecz także w sytuacji, gdy dane są przekazywane przez jednego z naszych członków, jeżeli jest np. członkiem rodziny, pełnomocnikiem, kontrahentem, udziałowcem, przedstawicielem podmiotu prawnego, pracownikiem usługodawcy lub partnera handlowego.

Jeżeli zbieramy dane bezpośrednio od osoby, której dane dotyczą, przekazujemy taką informację od razu. Gdy dane pochodzą z innego źródła, przekazujemy je osobie, której dotyczą:

- w rozsądnym terminie, nie później jednak niż w ciągu miesiąca od pozyskania danych;
- najpóźniej przy pierwszej komunikacji z osobą, której dane dotyczą,

chyba, że udzielenie informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku.

Ochrona danych osobowych w fazie projektowania oraz domyślna ochrona danych osobowych

Wdrażamy odpowiednie środki organizacyjne i techniczne celem skutecznej realizacji zasad ochrony danych, nadania przetwarzaniu danych niezbędnych zabezpieczeń oraz zapewnieniu ochrony praw osób, których dane dotyczą.

Wdrażając odpowiednie środki organizacyjne i techniczne uwzględniamy:

- stan wiedzy technicznej,
- koszt wdrażania,
- charakter, zakres, kontekst i cele przetwarzania danych,

- ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania.

Wdrażamy takie środki organizacyjne i techniczne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia określonego celu przetwarzania, biorąc pod uwagę: ilość zbieranych danych osobowych, ich zakres, okres ich przechowywania oraz ich dostępność dla innych osób.

Stosowane środki zapewniają, by domyślnie dane osobowe nie były udostępniane nieokreślonej liczbie osób.

W pierwszej kolejności rozważamy, czy cel, jakiemu ma służyć projektowane rozwiązanie, jest możliwy do osiągnięcia bez konieczności przetwarzania danych osobowych, a jeżeli tak, to wybieramy takie rozwiązanie.

Ocena skutków dla ochrony danych

W przypadku, jeżeli określony rodzaj przetwarzania (w szczególności z wykorzystaniem nowych technologii) ze względu na swój charakter, zakres, kontekst i cele, z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, przed rozpoczęciem przetwarzania dokonujemy oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

Kategorie przetwarzanych danych osobowych

Przetwarzamy dane osobowe w niezbędnym zakresie w ramach prowadzonej przez nas działalności, przede wszystkim identyfikacyjne i kontaktowe:

- dla celów członkostwa (członkowie, kandydaci): imię, nazwisko, adres (korespondencyjny/zamieszkania), adres e-mail, numer telefonu, pary językowe;
- dla zawierania i realizacji umów z nami, w tym ewentualnego dochodzenia związanych z tym roszczeń oraz wypełniania obowiązków prawnych (kontrahenci): imię, nazwisko, adres (korespondencyjny/zamieszkania), PESEL/NIP, adres e-mail, numer telefonu;
- dla celów korespondencyjnych/marketingowych (newsletter): imię, nazwisko, adres e-mail.

Podanie danych jest dobrowolne, jednak jeżeli ich nie otrzymamy, nie będziemy mogli dokonać przyjęcia w poczet członków, zawrzeć lub wykonać umowy lub skierować korespondencji do osób nią zainteresowanych, a w konsekwencji możliwa jest sytuacja, iż nie będzie można skorzystać ze świadczenia, którym dana osoba jest zainteresowana.

Nie przetwarzamy danych osobowych w sposób zautomatyzowany ani też nie dokonujemy na ich podstawie profilowania.

Analiza ryzyka (identyfikacja zagrożeń)

FORMA PRZETWARZANIA DANYCH: ZAGROŻENIA:

Dane przetwarzane w sposób tradycyjny:	- oszustwo, kradzież, sabotaż; - zdarzenia losowe (pożar); - zaniedbania osobowe (niedyskrecja, udostępnienie danych osobie nieupoważnionej); - niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; - pokonanie zabezpieczeń fizycznych; - podsłuchy, podglądy; - brak rejestrowania udostępniania danych; - niewłaściwe miejsce i sposób przechowywania dokumentacji.
Dane przetwarzane w systemach informatycznych:	- oszustwo, kradzież, sabotaż; - zaniedbania osobowe (niedyskrecja, udostępnienie danych osobie nieupoważnionej); - niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; - pokonanie zabezpieczeń informatycznych; - podsłuchy, podglądy; - pozostawienie sprzętu bez wylogowania się.

Bezpieczeństwo danych osobowych

PSTK podejmuje techniczne i organizacyjne środki służące ochronie danych osobowych przed nieuprawnionym dostępem lub wykorzystaniem, jak również przed przypadkowym zniszczeniem, utratą lub naruszeniem integralności. Względy bezpieczeństwa uwzględniamy na poziomie planowania, infrastruktury IT, standardów i praktyki biznesowej. Nasze standardy bezpieczeństwa obejmują w szczególności: zabezpieczenie dostępu (indywidualne hasłowanie systemów i/lub urządzeń, zamykane pomieszczenia i/lub szafy z ograniczonym dostępem), system kopii zapasowych, przegląd, utrzymanie i zarządzanie incydentami bezpieczeństwa. Korzystamy wyłącznie z licencjonowanego oprogramowania, zabezpieczenia przed wyciekiem danych są realizowane zgodnie z zabezpieczeniami producentów oprogramowania oraz przez zabezpieczenia wdrożone i kontrolowane przez administratora sieci. Sieci wewnętrzne i zewnętrzne są zabezpieczone przez administratora sieci oraz dostawcę Internetu, zgodnie z obowiązującymi zasadami bezpieczeństwa. Kopie zapasowe są tworzone na bieżąco, zasady tworzenia kopii zapasowych są zgodne z licencjami oprogramowania. Kopie zapasowe są przechowywane na chronionym serwerze

zabezpieczonym przez administratora sieci. Indywidualne stanowiska komputerowe są chronione unikalnymi loginami i okresowo zmienianymi hasłami.
W ramach zapewniania bezpieczeństwa przetwarzanych danych osobowych uwzględniane są wymogi:

- poufności – dane są chronione przed nieuprawnionym lub przypadkowym ujawnieniem osobom trzecim;
- integralności – dane są chronione przed nieuprawnioną modyfikacją;
- dostępności – zapewniany jest dostęp upoważnionych osób do danych osobowych, jeżeli pojawia się taka potrzeba.

Dane osobowe mogą być przetwarzane przez osoby trzecie jedynie w przypadku, gdy taki podmiot zobowiąże się do zapewnienia właściwych technicznych i organizacyjnych środków gwarantujących zapewnienie bezpieczeństwa przetwarzania danych osobowych, jak również do zachowania poufności tych danych. Każda osoba mająca dostęp do danych osobowych dysponuje odpowiednim upoważnieniem i jest zobowiązana do zachowania poufności.

Zasady bezpieczeństwa

- Dostęp do danych osobowych mogą mieć tylko osoby posiadające upoważnienie do ich przetwarzania.
- Obecność osób nieuprawnionych do przetwarzania danych w pomieszczeniu, w którym przetwarzane są dane osobowe jest możliwa tylko w obecności osoby upoważnionej do ich przetwarzania, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
- Osoby mające dostęp do danych osobowych nie mogą ich ujawniać w sposób wykraczający poza czynności związane z ich przetwarzaniem, w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
- Osoby przechowujące dane osobowe zobowiązane są do zabezpieczenia materiałów zawierających dane w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym.
- Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia.
- Nie wolno udostępniać indywidualnych haseł i identyfikatorów do systemów informatycznych.
- Wysyłanie seryjnych wiadomości e-mail wymaga zastosowania opcji „kopia ukryta”.
- Niedopuszczalne jest udzielanie informacji dotyczących danych osobowych innym podmiotom na podstawie prośby o takie dane skierowanej w formie zapytania telefonicznego.
- W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej należy stosować zasadę tzw. „czystego biurka”, oznaczającej niepozostawianie materiałów

zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Nie należy pozostawiać danych osobowych w miejscach ogólnodostępnych.

- Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe powinno odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści (np. z wykorzystaniem niszczarek).
- Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze indywidualną odpowiedzialność ponosi przede wszystkim każda osoba mająca dostęp do danych.
- W czasie chwilowej nieobecności w pomieszczeniach należy zamykać w sposób uniemożliwiający dostęp osobom nieuprawnionym (np. na klucz) pomieszczenia lub budynki wchodzące w skład obszarów, w których przetwarzane są dane osobowe.
- Przed opuszczeniem pomieszczenia, w którym przechowywane są dane osobowe należy upewnić się, że zostało ono odpowiednio zabezpieczone (np. zamknięte okna, drzwi).
- Po zakończeniu pracy w systemie informatycznym, w którym przechowywane są dane osobowe, należy wylogować się z systemu.
- Osoba użytkująca komputer przenośny zawierający dane osobowe zobowiązana jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania oraz użytkowania poza obszarem, w którym przetwarzane są dane osobowe.
- Na osobie pracującej zdalnie spoczywa obowiązek odpowiedniego zabezpieczenia danych tak, aby osoby trzecie nie miały dostępu do danych osobowych.
- Dane osobowe przesyłane elektronicznie powinny być zabezpieczone hasłem wysyłanym oddzielnym kanałem telekomunikacyjnym.

Okres przechowywania danych osobowych

Dane osobowe przechowujemy przez okres członkostwa, realizacji zawartej umowy, a po ich ustaniu/wykonaniu przez okres konieczny dla zabezpieczenia dochodzenia ewentualnych roszczeń oraz spełnienia obowiązków wynikających z przepisów prawa.

W przypadku przetwarzania danych osobowych na podstawie zgody – do momentu jej wycofania lub złożenia sprzeciwu.

W sytuacji, w której przetwarzanie danych osobowych odbywa się na podstawie przepisów prawa, dane przechowywane są przez okres wynikający z przepisów szczególnych.

Po upływie okresów przechowywania dane osobowe są usuwane lub zostają zanonimizowane.

Udostępnianie danych osobowych innym podmiotom

Możemy udostępniać dane osobowe podmiotom przetwarzającym:

- firmom lub osobom świadczącym usługi na nasze zlecenie lub w naszym imieniu, którym zlecimy czynności wymagające przetwarzania danych, np. w zakresie księgowości, usług IT, działalności pocztowej lub kurierskiej;
- uprawnionym organom i instytucjom państwowym lub samorządowym (np. sądom, prokuraturze) na ich pisemne żądanie i w zakresie dozwolonym przez prawo;
- niektórym osobom wykonującym regulowane zawody, takim jak np. adwokaci, radcowie prawni, notariusze, biegli rewidenci;
- w zakresie dozwolonym przez obowiązujące przepisy możemy także udostępniać dane osobowe instytucjom zajmującym się dochodzeniem należności, w tym przedsiębiorcom zajmującym się windykacją i obrotem wierzytelnościami oraz ich pełnomocnikom.

Od podmiotów trzecich wymagamy zachowania poufności i bezpieczeństwa informacji oraz wykorzystania ich jedynie do zapewnienia celu przekazania.

Podczas pracy i świadczenia usług korzystamy z nowoczesnych narzędzi i rozwiązań informatycznych, w tym m.in największych na świecie firm z sektora IT. Większość tego rodzaju firm ma siedzibę poza Europejskim Obszarem Gospodarczym, najczęściej w USA. Pomimo że nikt poza nami nie ma dostępu do danych, które za pomocą tych narzędzi informatycznych przetwarzamy, według RODO oznacza to, że w ten sposób może dochodzić do przekazywania danych osobowych poza Europejski Obszar Gospodarczy (bo firmy dostarczające tego rodzaju narzędzi i rozwiązań posiadają nieraz serwery zlokalizowane także poza EOG). Informujemy więc o tym fakcie – a więc, że z punktu widzenia RODO dane mogą być przekazywane do tzw. państw trzecich. Takie działania zawsze jednak odbywają się zgodnie z RODO – jeżeli dane państwo nie zostało uznane przez Komisję Europejską za zapewniające odpowiedni poziom ochrony danych, ze wszystkimi podmiotami, z których produktów lub usług korzystamy, w wyniku czego może dojść do przekazywania danych do państw trzecich w rozumieniu RODO, mamy zawarte umowy w przedmiocie przetwarzania danych osobowych zawierające standardowe klauzule umowne dotyczące ochrony danych przyjęte przez Komisję Europejską, o których mowa w art. 46 ust. 2 lit. c) RODO.

Przypadek naruszenia ochrony danych osobowych

W przypadku powzięcia przez jakąkolwiek osobę po stronie PSTK informacji o jakimkolwiek incydencie, który może doprowadzić do naruszenia ochrony danych osobowych (lub podejrzeniu takiego naruszenia), osoba ta niezwłocznie informuje o tym członka zarządu PSTK. Ww. incydentem może być każde zdarzenie, które zagraża bezpośrednio lub pośrednio bezpieczeństwu przetwarzania danych osobowych, w tym np. naruszenie bezpieczeństwa fizycznego pomieszczeń lub sprzętów (np. podejrzenie włamania, zalania, zagubienia nośnika z danymi osobowymi).

W przypadku stwierdzenia naruszenia ochrony danych osobowych, po przeprowadzeniu analizy bez zbędnej zwłoki (w miarę możliwości, nie później niż w terminie 72 godzin po

stwierdzeniu naruszenia) podlega ono zgłoszeniu organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Zgłoszenie organowi nadzorczemu powinno:

- opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, jak również kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- zawierać imię i nazwisko oraz dane kontaktowe osoby, od której można uzyskać więcej informacji;
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
- opisywać środki zastosowane lub proponowane w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Dokumentujemy naruszenia ochrony danych osobowych, w tym jego okoliczności, skutki oraz podjęte działania zaradcze.

Zawiadamianie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, bez zbędnej zwłoki zawiadamiana jest osoba, której dane dotyczą, o takim naruszeniu.

Zawiadomienie jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera co najmniej:

- imię i nazwisko oraz dane kontaktowe osoby, od której można uzyskać więcej informacji;
- wskazanie możliwych konsekwencji naruszenia ochrony danych osobowych;
- wskazanie środków zastosowanych lub proponowanych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Zawiadomienie nie jest wymagane w następujących przypadkach:

- wdrożono odpowiednie techniczne i organizacyjne środki ochrony (w szczególności takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do danych osobowych) i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie;
- zastosowano środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
- zawiadomienie wymagałoby niewspółmiernie dużego wysiłku; w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Prawa przysługujące w związku z przetwarzaniem danych osobowych

Przestrzegamy realizacji uprawnień związanych z przetwarzaniem danych osobowych (prawa te wynikają w szczególności z art. 16-21 RODO).

Osoba, której dane przetwarzamy ma prawo do:

- Cofnięcia zgody na przetwarzanie danych osobowych
  W przypadkach, w których przetwarzanie danych odbywa się na podstawie zgody przysługuje prawo do cofnięcia zgody w dowolnym momencie. Cofnięcie zgody nie ma wpływu na zgodność z prawem przetwarzania danych, którego dokonano przed jej cofnięciem.
- Dostępu do danych osobowych
  Można otrzymać od potwierdzenie, czy dane osobowe są przez przetwarzane i w jaki sposób.
- Sprostowania danych osobowych
  Nieaktualne lub niedokładne dane osobowe mogą zostać w każdej chwili sprostowane, a także uzupełnione w przypadku, gdy są niekompletne.
- Sprzeciwu wobec przetwarzania danych osobowych
  Jeżeli przetwarzamy dane osobowe w oparciu o nasz uzasadniony interes (np. cele dowodowe, archiwizacyjne), wówczas w razie sprzeciwu będziemy musieli zaprzestać przetwarzania tych danych (chyba, że wykażemy istnienie istotnych, uzasadnionych podstaw dla przetwarzania, które obiektywnie powinny mieć pierwszeństwo nad ochroną lub polegają na obronie naszych roszczeń, np. w postępowaniu sądowym). W przypadku wniesienia sprzeciwu wobec przetwarzania danych osobowych na potrzeby marketingu bezpośredniego zaprzestajemy go niezwłocznie.
- Usunięcia danych osobowych
  Tzw. „prawo do bycia zapomnianym" polega co do zasady (nie jest ono bowiem bezwzględne) na możliwości żądania od administratora niezwłocznego usunięcia danych osobowych dotyczących osoby zgłaszającej takie żądanie.
- Ograniczenia przetwarzania danych osobowych
  Może to polegać np. na czasowym zablokowaniu dostępu do danych lub przeniesieniu danych do innego systemu, np. na okres pozwalający nam sprawdzić prawidłowość danych lub np. ustalenie, czy prawnie uzasadnione podstawy po naszej stronie są nadrzędne wobec podstawy zgłoszonego sprzeciwu.
- Przenoszenia danych osobowych
  Jeżeli przetwarzanie odbywa się w oparciu o udzieloną zgodę lub na podstawie umowy, oraz w sposób zautomatyzowany, osoba której dane przetwarzamy ma prawo do otrzymania kopii danych osobowych, które nam dostarczyła.

- Złożenia skargi do organu nadzorczego
  W związku z przetwarzaniem przez nas danych osobowych osoba, której dane dotyczą może złożyć skargę do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

Wszelkie wnioski dotyczące danych osobowych, w tym realizacji przysługujących praw, można przesyłać nam pisemnie na adres naszej siedziby lub elektronicznie, na adres e-mail: kontakt@pstk.org.pl

Wnioski rozpatrujemy i realizujemy niezwłocznie, dokładając starań, aby nastąpiło to nie później niż w ciągu miesiąca. W razie uzasadnionej potrzeby, z uwagi na skomplikowany charakter żądania lub liczbę zgłoszonych żądań, termin realizacji żądania może zostać przedłużony o kolejne dwa miesiące, o czym niezwłocznie powiadomimy.

Cookies

Pliki cookies to niewielkie informacje tekstowe, wysyłane przez portal i zapisywane na komputerze użytkownika (bądź innym urządzeniu, z którego korzysta osoba odwiedzająca stronę internetową).

W związku z korzystaniem ze strony internetowej możliwe jest gromadzenie danych zawartych w logach systemowych. W logach systemowych mogą być gromadzone informacje o adresach IP (numer interfejsu sieciowego), jednakże dane te nie pozwalają nam na jednoznaczne zidentyfikowanie użytkownika (wskazanie konkretnej osoby fizycznej korzystającej z komputera czy innego urządzenia podłączonego do Internetu).

Przeglądarka internetowa może przechowywać pliki cookies na dysku komputera. W plikach cookies znajdują się informacje niezbędne do prawidłowego funkcjonowania portalu.

Zawartość plików cookies nie pozwala na identyfikację użytkownika.

Za pomocą plików cookies nie są przetwarzane lub przechowywane dane osobowe użytkowników portalu (za ich pomocą nie przetwarzamy ani nie przechowujemy danych osobowych).

Mechanizm cookies nie jest wykorzystywany do pozyskiwania informacji o Użytkownikach, za wyjątkiem informacji o ich zachowaniu na portalu.

Pliki cookies mogą być przechowywane na komputerach użytkowników w celu:

- właściwego dopasowania portalu do potrzeb użytkowników oraz optymalizacji korzystania ze strony internetowej;
- zapamiętania preferencji i indywidualnych ustawień użytkownika;
- tworzenia statystyk oglądalności portalu pomagających zrozumieć, w jaki sposób użytkownicy korzystają ze stron internetowych, co umożliwia ich ulepszanie;
- utrzymania sesji użytkownika (w przypadku logowania), dzięki której użytkownik nie musi na każdej podstronie ponownie wpisywać loginu i hasła;

Z uwagi na „czas życia” cookies i innych podobnych technologii, stosowane mogą być pliki:

- „sesyjne” (session cookies), czyli pliki tymczasowe, przechowywane w urządzeniu końcowym użytkownika do czasu wylogowania, opuszczenia strony internetowej lub wyłączenia oprogramowania (przeglądarki internetowej);

- „stałe” (persistent cookies), 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 cookies i inne podobne technologie, stosowane mogą być następujące rodzaje plików:

- „niezbędne” – pliki cookies umożliwiające korzystanie z usług dostępnych w ramach portalu, np. uwierzytelniające pliki cookies wykorzystywane do usług wymagających uwierzytelniania;
- służące do zapewnienia bezpieczeństwa – pliki cookies wykorzystywane do wykrywania nadużyć w zakresie uwierzytelniania w ramach portalu;
- „wydajnościowe” – pliki cookies umożliwiające zbieranie informacji o sposobie korzystania ze stron internetowych;
- „funkcjonalne” – pliki cookies umożliwiające „zapamiętanie” wybranych przez użytkownika ustawień i personalizację interfejsu użytkownika, np. w zakresie wybranego języka lub regionu, rozmiaru czcionki, wyglądu strony internetowej itp.;
- „reklamowe” – pliki cookies umożliwiające dostarczanie użytkownikom treści reklamowych optymalnie dostosowanych do ich zainteresowań.

Jeżeli nie chcesz otrzymywać plików cookies, które nie są bezwzględnie konieczne do działania podstawowych funkcjonalności naszej strony internetowej, możesz nie wyrazić zgody, odpowiednio zmieniając ustawienia swojej przeglądarki.

Dodatkowe informacje o plikach cookies i o tym, jak je wyłączyć, dostępne są na stronie internetowej http://wszystkoociasteczkach.pl. Znajdują się tam również informacje, jak usunąć pliki cookies ze swojego komputera.

Odrzucenie wszystkich plików cookies może oznaczać niemożność korzystania w pełni ze wszystkich funkcjonalności strony internetowej.

Zmiany

Okresowo aktualizujemy i możemy dokonywać zmian w niniejszej polityce, co może wynikać w szczególności z potrzeby dostosowania się do zmian w przepisach prawa czy obowiązujących standardach prywatności, zmian technologicznych, jak też poszerzania naszej działalności.

Prawa autorskie

Niniejsza polityka, jak również wszelkie treści i elementy graficzne naszej strony internetowej są chronione przepisami prawa, w szczególności ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (tekst jednolity Dz.U. z 2017 r., poz. 880, z późn. zm.) oraz ustawy z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji (tekst jednolity Dz.U z 2018 r., poz. 419). Jakiekolwiek nieuprawnione wykorzystywanie, w tym kopiowanie lub powielanie, wiąże się z narażeniem na odpowiedzialność prawną z tego tytułu.