

Polityka ochrony danych osobowych w Polskiej Izbie Paliw Płynnych

1. Niniejszy dokument zatytułowany „Polityka ochrony danych osobowych” (dalej: **Polityka**) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w Polskiej Izbie Paliw Płynnych (dalej: **PIPP**) z siedzibą w Warszawie zarejestrowaną w Krajowym Rejestrze Sądowym – rejestrze stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000120987, NIP 5260307979

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s.1).

2. Polityka zawiera :
 - a) opis zasad ochrony danych obowiązujących w PIPP,
 - b) odwołania do załączników uszczegóławiających (wzorce procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach).
3. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Zarząd Rady Izby PIPP, a w ramach Zarządu:
 - a) Członek Zarządu, któremu powierzono nadzór nad obszarem ochrony danych osobowych.
 - b) Osoba wyznaczona przez Zarząd do zapewnienia zgodności z ochrony danych osobowych;

za nadzór i monitorowanie przestrzegania Polityki odpowiadają;

- c) Inspektor Ochrony Danych, jeżeli został powołany w PIPP,
- d) Komórka audytu wewnętrznego, jeżeli funkcjonuje w PIPP,

za stosowanie niniejszej Polityki odpowiedzialni są:

- e) PIPP,
- f) komórka organizacyjna odpowiedzialna za obszar bezpieczeństwa informacji,
- g) komórki organizacyjne przetwarzające dane osobowe w dużym rozmiarze,
- h) wszyscy członkowie personelu PIPP.

PIPP powinna też zapewnić zgodność postępowania kontrahentów PIPP z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych w PIPP.

4. SKRÓTY I DEFINICJE:

Polityka oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.

RODO oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s.1).

Dane oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.

Dane szczególnych kategorii oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

Dane karne oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.

Dane dzieci oznaczają dane osób poniżej 16. roku życia.

Osoba oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.

Podmiot przetwarzający oznacza organizację lub osobę, której PIPP powierzyła przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna Księgowość).

Profilowanie oznacza dowolną formę zautomatyzowania przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, 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.

Eksport danych oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.

IOD lub Inspektor oznacza Inspektora Ochrony Danych Osobowych.

RCPD lub Rejestr oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

PIPP oznacza Polską Izbę Paliw Płynnych

5. OCHRONA DANYCH OSOBOWYCH W PIPP - ZASADY OGÓLNE

5.1. Filary ochrony danych osobowych w PIPP:

a) **Legalność** - PIPP dba o ochronę prywatności i przetwarzanie danych zgodnie z prawem.

- b) **Bezpieczeństwo** - PIPP zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie.
- c) **Prawa jednostki** - PIPP umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
- d) **Rozliczalność** - PIPP dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

5.2. Zasady ochrony danych:

PIPP przetwarza dane osobowe z poszanowaniem następujących zasad:

- a) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
- b) rzetelnie i uczciwie (rzetelność);
- c) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
- d) w konkretnych celach i nie „na zapas” (minimalizacja);
- e) nie więcej niż potrzeba (adekwatność);
- f) z dbałością o prawidłowość danych (prawidłowość);
- g) nie dłużej niż potrzeba (czasowość);
- h) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

5.3. System ochrony danych

System ochrony danych osobowych w PIPP składa się z następujących elementów:

1. **Inwentaryzacja danych.** PIPP dokonuje identyfikacji zasobów danych osobowych, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystywanych (inwentaryzacja), w tym:
 - a) przypadków przetwarzania danych szczególnych kategorii i danych karnych;
 - b) przypadków przetwarzania danych osób, których PIPP nie identyfikuje (dane niezidentyfikowane);
 - c) przypadków przetwarzania danych dzieci;
 - d) profilowania;
 - e) współadministrowania danymi.

2. Rejestr.

PIPP opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną w PIPP.

3. Podstawy prawne.

PIPP zapewnia, identyfikuje, weryfikuje postawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:

- a) utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,
- b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy PIPP przetwarza dane na podstawie prawnie uzasadnionego interesu PIPP.

4. Obsługa praw jednostki.

PIPP spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

- a) **obowiązki informacyjne.** PIPP przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków;
- b) **możliwość wykonywania żądań.** PIPP weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających;
- c) **obsługa żądań.** PIPP zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO i dokumentowane;
- d) **zawiadomienie o naruszeniach.** PIPP stosuje procedury pozwalające na ustalenie konieczności zawiadamiania osób dotkniętych zidentyfikowanymi naruszeniem ochrony danych.

5. Minimalizacja.

PIPP posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:

- a) zasady zarządzania **adekwatnością** danych;
- b) zasady reglamentacji i zarządzania **dostępem** do danych;
- c) zasady zarządzania okresem **przechowywania** danych i weryfikacji dalszej przydatności.

6. Bezpieczeństwo.

PIPP zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

- a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
- b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
- c) dostosowuje środki ochrony danych do ustalonego ryzyka;
- d) posiada system zarządzania bezpieczeństwem informacji;
- e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych – zarządza incydentami.

7. Przetwarzający.

PIPP posiada zasady doboru przetwarzających dane na jego rzecz, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.

8. Eksport danych.

PIPP posiada zasady weryfikacji, czy PIPP nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.

9. *Privacy by design.*

PIPP zarządza zmianami wpływającymi na prywatności. W tym celu procedury uruchamiania nowych projektów i inwestycji uwzględniają konieczność oceny wpływu zmiany na ochronę danych, analizę ryzyka, zapewnienie prywatności (a w tym zgodność celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

10. Przetwarzanie transgraniczne.

PIPP posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

6. INWENTARYZACJA

6.1 Dane szczególnych kategorii i dane karne

PIPP identyfikuje przypadki, w których przetwarza lub może przetwarzać dane szczególnych kategorii lub dane karne oraz utrzymuje dedykowane mechanizmy zapewniania zgodności z prawem przetwarzania takich danych. W przypadku zidentyfikowania przypadków przetwarzania danych szczególnych kategorii lub danych karnych PIPP postępuje zgodnie z przyjętymi zasadami w tym zakresie.

6.2 Dane niezidentyfikowane

PIPP identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane, i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.

6.3 Profilowanie

PIPP identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych, i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji PIPP postępuje zgodnie z przyjętymi zasadami w tym zakresie.

6.4 Współadministrowanie

PIPP identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.

7. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH

7.1 RCPD stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

7.2 PIPP prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

7.3 Rejestr jest jednym z podstawowych narzędzi umożliwiających PIPP rozliczanie większości obowiązków ochrony danych.

7.4 W Rejestrze dla każdej czynności przetwarzania danych, którą PIPP uznała za odrębną dla potrzeb Rejestru, PIPP odnotowuje co najmniej:

- a) nazwę czynności,
- b) cel przetwarzania,
- c) opis kategorii osób,
- d) opis kategorii danych,
- e) podstawę prawną przetwarzania wraz z wyszczególnieniem kategorii uzasadnianego interesu PIPP, jeśli podstawa jest uzasadniony interes,
- f) sposób zbierania danych,
- g) opis kategorii odbiorców danych (w tym przetwarzających),
- h) informacje o przekazywaniu poza EU/EOG;
- i) ogólny opis technicznych i organizacyjnych środków ochrony danych.

7.5 **Wzór Rejestru stanowi Załącznik nr 1** do Polityki - „Wzór Rejestru Czynności Przetwarzania Danych”. Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych PIPP rejestruje informację w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczanie się z niej.

8. PODSTAWY PRZETWARZANIA

8.1 PIPP dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

8.2 Wskazując w dokumentach ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadania publiczne/ władza publiczna, uzasadniony cel PIPP), PIPP dookreśla podstawę w precyzyjny i czytelny sposób, gdy jest to potrzebne. Np. dla zgody - wskazując jej zakres, gdy podstawą jest prawo - wskazując konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy - wskazujące kategorie zdarzeń, w których się zmaterializują, uzasadniony cel - wskazując konkretny cel, np. marketing własny, dochodzenie roszczeń.

8.3 PIPP wdraża metody zarządzania zgodami umożliwiające rejestracje i weryfikacje posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikacje na odległość (e-mail, telefon, SMS itp.) oraz rejestracje odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

8.4 Kierownik komórki organizacyjnej PIPP ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes PIPP, kierownik komórki ma obowiązek znać konkretny interes PIPP, który dzięki temu przetwarzaniu jest realizowany.

9. SPOSÓB OBSŁUGI PRAW JEDNOSTKI I OBOWIĄZKÓW INFORMACYJNYCH

9.1 PIPP dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

- 9.2 PIPP ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronach internetowych Polskiej Izby Paliw Płynnych informacji lub odwołań (linków) do informacji o prawach osób, o sposobie skorzystania z nich, w tym wymaganiach dotyczących identyfikacji, metod kontaktu z PIPP w tym celu, ewentualnym cenniku żądań „dodatkowych” itp.
- 9.3 PIPP dba o dotrzymanie prawnych terminów realizacji obowiązków względem osób.
- 9.4 PIPP wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw i jednostki i obowiązków informacyjnych.
- 9.5 W celu realizacji praw jednostki PIPP zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez PIPP, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,
- 9.6 PIPP dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

10.OBOWIĄZKI INFORMACYJNE

- 10.1 PIPP określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
- 10.2 PIPP informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie zadania tej osoby.
- 10.3 PIPP informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
- 10.4 PIPP informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.
- 10.5 PIPP określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam, gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).
- 10.6 PIPP informuje osobę o planowanej zmianie celu przetwarzania danych.
- 10.7 PIPP informuje osobę przed uchynieniem ograniczenia przetwarzania.
- 10.8 PIPP informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
- 10.9 PIPP informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
- 10.10 PIPP bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

11. Żądania osób

11.1. Prawa osób trzecich.

Realizując prawa osób, których dane dotyczą, PIPP wprowadza proceduralne gwarancje ochrony prawa i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste), PIPP może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową.

11.2. Nieprzetwarzanie

PIPP informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

11.3. Odmowa

PIPP informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

11.4. Dostęp do danych.

Na żądanie osoby dotyczące dostępu do jej danych PIPP informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych.

11.5. Kopie danych

Na żądanie PIPP wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. PIPP wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest na podstawie oszacowanego jednostkowego kosztu obsługi żądania wydania kopii danych.

11.6. Sprostowanie danych.

PIPP dokonuje sprostowania nieprawidłowych danych na żądanie osoby. PIPP ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowość danych, których sprostowania się domaga. W przypadku sprostowania danych PIPP informuje osobę o odbiorcach danych, na żądanie tej osoby.

11.7. Uzupełnienie danych.

PIPP uzupełnia i aktualizuje dane na żądanie osoby. PIPP ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. PIPP nie musi przetwarzać danych, które są zbędne). PIPP może polegać na oświadczeniu osoby co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez PIPP procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

11.8. Usunięcie danych.

Na żądanie osoby PIPP usuwa dane, gdy:

- a) Dane nie są niezbędne dla celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach;
- b) Zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania;
- c) Osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych;
- d) Dane były przetwarzane niezgodnie z prawem;
- e) Konieczność usunięcia wynika z obowiązku prawnego;
- f) Żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej).

PIPP określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17 ust. 3 RODO.

Jeżeli dane podlegające usunięciu zostały upublicznione, PIPP podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe o potrzebie usunięcia danych i dostępu do nich.

W przypadku usunięcia danych PIPP informuje osobę o odbiorcach danych, na żądanie tej osoby.

11.9. Ograniczenie przetwarzania

PIPP dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

- a) Osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość;
- b) Przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
- c) PIPP nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
- d) Osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie PIPP zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania PIPP przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.

PIPP informuje osobę przed uchyleniem ograniczenia przetwarzania.

W przypadku ograniczenia przetwarzania danych PIPP informuje osobę o odbiorcach danych, na żądanie tej osoby.

11.10 Przenoszenie danych.

Na żądanie osoby, PIPP wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona PIPP, przetwarzane na podstawie

zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej w systemach informatycznych.

11.11. Sprzeciw w szczególnej sytuacji.

Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez PIPP w oparciu o uzasadniony interes lub o powierzone zadanie w interesie publicznym, PIPP uwzględni sprzeciw, o ile nie zachodzą po jego stronie ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, prawa i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

11.12. Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych.

Jeżeli PIPP prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. PIPP uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

11.13. Sprzeciw względem marketingu bezpośredniego.

Jeżeli osoba zgłosi względem przetwarzania jej danych przez PIPP na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), PIPP uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

11.14. Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu.

Jeżeli PIPP przetwarza dane w sposób automatyczny, w tym w szczególności profiluje osoby i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na osobę, PIPP zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie PIPP, chyba że taka automatyczne decyzja:

- a) Jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą, a PIPP lub
- b) Jest wprost dozwolona przepisami prawa lub
- c) Opiera się na wyraźnej zgodzie odwołującej osoby

12. MINIMALIZACJA

PIPP dba o minimalizację przetwarzania danych pod kątem:

- a) Adekwatności danych do celów (ilości danych i zakresu przetwarzania);
- b) Dostępu danych;
- c) Czasu przechowywania danych.

12.1. Minimalizacja zakresu

PIPP zweryfikowała zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.

PIPP dokonuje okresowego przeglądu ilości przetwarzania danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.

PIPP przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (*privacy by design*).

12.2. Minimalizacja dostępu

PIPP stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).

PIPP stosuje kontrolę dostępu fizycznego.

PIPP dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających.

PIPP dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.

Szczegółowe zasady kontroli dostępu fizycznego i logicznego zwarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji PIPP.

12.3. Minimalizacja czasu.

PIPP wdraża mechanizmy kontroli cyklu życia danych osobowych w PIPP, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.

Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu, są usuwane z systemów produkcyjnych PIPP, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez PIPP. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

13. BEZPIECZEŃSTWO

PIPP zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez PIPP.

13.1. Analiza ryzyka i adekwatności środków bezpieczeństwa

PIPP przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

- a) PIPP zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnątrz lub ze wsparciem podmiotów wyspecjalizowanych.
- b) PIPP kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
- c) PIPP przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. PIPP analizuje możliwe

sytuacje i scenariusze ochrony danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

- d) PIPP ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym PIPP ustala przydatności i stosuje takie środki i podejście, jak:
- 1) Pseudonimizacja
 - 2) Szyfrowanie danych osobowych
 - 3) Inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania
 - 4) Środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego

13.2. Oceny skutków dla ochrony danych

PIPP dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.

PIPP stosuje metodykę oceny skutków przyjętą w PIPP.

13.3. Środki bezpieczeństwa

PIPP stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych.

Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w PIPP i są bliżej opisane w procedurach przyjętych przez PIPP obszarów.

13.4. Zgłaszanie naruszeń

PIPP stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych Osobowych w terminie niezwłocznym – nie dłuższym niż 72 h od ustalenia naruszenia.

14. PRZETWARZAJĄCY

PIPP posiada zasady doboru i weryfikacji przetwarzających dane na rzecz PIPP opracowane w celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na PIPP.

PIPP przyjęła minimalne wymagania co do umowy powierzania przetwarzania danych, której to wzór stanowi załącznik nr 2 – „Wzór umowy powierzenia przetwarzania danych”

PIPP rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia danych osobowych.

15. PLIKI COOKIES

15.1 Witryny internetowe PIPP używają cookies. Są to niewielkie pliki tekstowe wysyłane przez serwer www i przechowywane przez oprogramowanie komputera przeglądarki, są one zapisywane na dysku urządzenia użytkownika końcowego w celu ułatwienia nawigacji oraz dostosowania serwisu do preferencji użytkownika. Zablokowanie zapisywania plików cookies na urządzeniu końcowym lub ich usunięcie możliwe jest w po właściwym skonfigurowaniu ustawień przeglądarki internetowej, może jednak spowodować utrudnienia lub brak działania niektórych funkcji serwisu. Niedokonanie zmian ustawień przeglądarki internetowej na ustawienia blokujące zapisywanie plików cookies jest jednoznaczne z wyrażeniem zgody na ich zapisywanie.

15.2 Wiele stron internetowych zapisuje na Twoim komputerze, a dokładniej w schowku konkretnej przeglądarki (Firefox, Internet Explorer, Chrome i inne) na Twoim koncie użytkownika komputera lub telefonu, na którym łączysz się z Siecią, tzw. pliki cookie. Zazwyczaj pliki cookie są bardzo pożyteczne. Dzięki nim zapamiętywane są Twoje indywidualne ustawienia i dzięki nim możesz się zalogować np. do swojej poczty. Autorzy stron internetowych wiedzą dzięki nim, jak wielu użytkowników do nich zagląda i co konkretnie czytają, a co obchodzą z daleka. Informacje zbierane przy użyciu plików cookie mogą też służyć do zbierania informacji o Tobie w celach handlowych. Np. jeżeli często wchodzisz na strony o książkach, będziesz widział więcej reklam księgarni.

15.3 Podmiotem zamieszczającym na urządzeniu końcowym użytkownika pliki cookies oraz uzyskującym do nich dostęp jest operator serwisu www.targi.paliwa.pl.

15.4 Pliki cookies wykorzystywane są w celu:

- a) dostosowania zawartości stron internetowych do preferencji użytkownika oraz optymalizacji korzystania ze stron internetowych;
- b) w szczególności pliki te pozwalają rozpoznać urządzenie użytkownika i odpowiednio wyświetlić stronę internetową, dostosowaną do jego indywidualnych potrzeb;
- c) tworzenia statystyk, które pomagają zrozumieć, w jaki sposób użytkownicy korzystają ze stron internetowych, co umożliwia ulepszanie ich struktury i zawartości;

W ramach serwisu stosowane są dwa zasadnicze rodzaje plików cookies: „sesyjne” (session cookies) oraz „stałe” (persistent cookies). Cookies „sesyjne” to pliki tymczasowe, które przechowywane są w urządzeniu końcowym użytkownika do czasu wylogowania, opuszczenia strony internetowej lub zamknięcia przeglądarki internetowej. „Stale” pliki cookies przechowywane są w urządzeniu końcowym użytkownika przez czas określony w parametrach plików cookies lub do czasu ich usunięcia przez użytkownika.

15.5 W ramach serwisu mogą być stosowane następujące rodzaje plików cookies:

- „niezbędne” pliki cookies, umożliwiające korzystanie z usług dostępnych w ramach serwisu, np. uwierzytelniające pliki cookies wykorzystywane do usług wymagających uwierzytelniania (logowania);
- pliki cookies służące do zapewnienia bezpieczeństwa, np. wykorzystywane do wykrywania nadużyć w zakresie uwierzytelniania w ramach serwisu;

- „wydajnościowe” pliki cookies, umożliwiające zbieranie informacji o sposobie korzystania ze stron internetowych serwisu;
- „funkcjonalne” pliki cookies, umożliwiające „zapamiętanie” wybranych przez użytkownika ustawień i personalizację interfejsu użytkownika, np. w zakresie wybranego języka lub regionu, wyglądu strony internetowej itp.;
- „reklamowe” pliki cookies, umożliwiające dostarczanie użytkownikom treści reklamowych dostosowanych do ich zainteresowań.

15.6 Użytkownik w każdej chwili ma możliwość wyłączenia lub przywrócenia opcji gromadzenia cookies poprzez zmianę ustawień w przeglądarce internetowej. Instrukcja zarządzania plikami cookies jest dostępna na stronie.

15.7 Informacje zbierane i generowane przez Cookies nie pozwalają na identyfikację Użytkownika.

15.8 W wyniku wykorzystywania Cookies nie są przechowywane żadne dane osobowe Użytkownika. Cookies używane przez PIPP są bezpieczne i nie mają szkodliwego wpływu na komputer Użytkownika

16. EKSPORT DANYCH

PIPP rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy (EOG).

17. PROJEKTOWANIE PRYWATNOŚCI

PIPP zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania.

W tym celu zasady prowadzenia projektów i inwestycji przez PIPP odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowania bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.