POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH POMORSKA GRUPA SPRZEDAŻOWA SP. Z O.O.

1. CELE POLITYKI

1. Polityka Bezpieczeństwa Danych Osobowych, zwana dalej Polityką, określa zasady przetwarzania danych osobowych w Pomorskiej Grupie Sprzedażowej spółce z ograniczoną odpowiedzialnością z siedzibą w Gdańsku (dalej: PGS) w celu ich zabezpieczenia adekwatnie do ryzyka i zidentyfikowanych zagrożeń oraz uzyskania zgodności z wymaganiami przepisów prawa i wytycznych w obszarze ochrony danych osobowych, w szczególności Rozporządzenia 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 (dalej: RODO).

2. TERMINOLOGIA

termin	znaczenie
zgoda podmiotu danych	dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych
administrator danych	podmiot, który ustala cele i środki przetwarzania danych osobowych
podmiot przetwarzający	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu i na rzecz administratora danych
dane osobowe	jakiekolwiek informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej
przetwarzanie danych osobowych	operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez

	przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie
naruszenie ochrony danych osobowych	naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych
profilowanie	dowolna forma zautomatyzowanego 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
pseudonimizacja	przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, np. szyfrowanie z kluczem tajnym, funkcja skrótu, tokenizacja
szczególne kategorie danych	dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby

3. POSTANOWIENIA OGÓLNE

1. PGS sp. z o.o. uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne w celu skutecznego zabezpieczenia przetwarzanych danych oraz spełnienia wymogów, o których mowa w RODO.
2. Środkiem ochrony organizacyjnej jest niniejsza Polityka, która definiuje mechanizmy ochrony danych osobowych stosowane przez PGS, a także inne procedury i zasady ochrony danych osobowych ustanowione w ramach obowiązujących regulacji wewnętrznych.
3. Wszystkie osoby przetwarzające dane osobowe w PGS są zobowiązane do stosowania niniejszych reguł. Szczegółowe procedury przetwarzania danych osobowych powinny być zgodne z niniejszą Polityką oraz wymaganiami przepisów prawa, w szczególności z RODO i przepisami krajowymi w zakresie ochrony danych osobowych.
4. Zasady określone w niniejszej Polityce włącza się do programów szkoleniowych jako obligatoryjny obszar wiedzy, z którym powinni być zapoznawani wszyscy pracownicy i współpracownicy PGS oraz w stosownych przypadkach pracownicy stron trzecich.

4. ODPOWIEDZIALNOŚĆ

- Sprawuje nadzór nad systemem ochrony danych osobowych w PGS, w związku z tym jest uprawniony do przeglądu wszystkich mechanizmów ustanowionych w celu ochrony danych osobowych, weryfikowania ich skuteczności i adekwatności.
- Sprawuje nadzór nad wymaganiami prawnymi ochrony danych osobowych.

Inspektor Ochrony Danych	• Pełni funkcję punktu kontaktowego dla organu nadzorczego ochrony danych osobowych oraz osób, których dane są przetwarzane. • Prowadzi rejestr obowiązujących wzorów zgód na przetwarzanie danych osobowych i obowiązków informacyjnych. • Zapewnia aktualność rejestrów czynności przetwarzania na podstawie informacji przekazywanych przez poszczególne komórki organizacyjne. • Koordynuje realizację praw osób, których dane są przetwarzane. • Nadzoruje proces nadawania upoważnień do przetwarzania danych osobowych i prowadzi ewidencję osób upoważnionych.
Inspektor Ochrony Danych wspólnie z firmą zewnętrzną prowadzącą obsługę kadrową	• Odpowiadają za bezpieczeństwo danych osobowych pracowników lub osób zatrudnionych na innej podstawie prawnej oraz kandydatów do pracy. • Odpowiadają za realizację praw pracowników w zakresie ochrony danych osobowych.
Administrator Systemów Informatycznych	• Wdraża środki ochrony bezpieczeństwa teleinformatycznego ustanowione w ramach systemu ochrony danych osobowych.
Zewnętrzna Kancelaria Prawna	• Nadzoruje proces powierzania przetwarzania danych osobowych. • Odpowiada za weryfikację implementacji środków ochrony danych osobowych w ramach umów z podmiotami przetwarzającymi. • Wspiera Inspektora Ochrony Danych w zakresie wymagań prawnych ochrony danych osobowych.
Wszystkie osoby przetwarzające dane osobowe w PGS sp. z o.o.	• Dbają o bezpieczeństwo przetwarzanych danych osobowych. • Niezwłocznie zgłaszają wszelkie naruszenia ochrony danych osobowych zgodnie z Procedurą zarządzania incydentami bezpieczeństwa. • Identyfikują powierzenie przetwarzania danych osobowych w ramach umów zawieranych z podmiotami zewnętrznymi i dobierają odpowiednie do przedmiotu zamówienia i stosowanych środków przetwarzania, mechanizmy ochrony danych. • Realizują prawa osób, których dane są przetwarzane.

5. ZASADY OCHRONY DANYCH OSOBOWYCH

1. Osoby przetwarzające dane osobowe w PGS są zobowiązane do ochrony przetwarzanych danych osobowych oraz realizacji praw osób, których dane są przetwarzane.
2. Dane osobowe przetwarzane przez PGS muszą być:
   a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
   b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
   c) adekwatne, stosowne oraz ograniczone do tego, co jest niezbędne dla realizacji celów, dla których są przetwarzane;
   d) prawidłowe i w razie potrzeby uaktualniane;
   e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
   f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.
3. Przetwarzanie danych osobowych jest możliwe jedynie gdy spełniona jest przynajmniej jedna z następujących przesłanek:

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na PGS;
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym;
f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

4. Każda osoba, której dane są przetwarzane, ma szereg praw, w tym:
   - prawo dostępu do danych
   - prawo do sprostowania danych
   - prawo do usunięcia danych („prawo do bycia zapomnianym")
   - prawo do ograniczenia przetwarzania
   - prawo do przenoszenia danych
   - prawo do sprzeciwu.

   Zasady realizacji powyższych praw zostały opisane w Załączniku nr 1 do niniejszej Polityki – Zasadach realizacji praw osób, których dane dotyczą.
5. W celu ewidencjonowania procesów przetwarzania danych osobowych Inspektor Ochrony Danych prowadzi w postaci elektronicznej Rejestr czynności przetwarzania administratora danych, którego wzór stanowi Załącznik nr 2 oraz Rejestr czynności przetwarzania podmiotu przetwarzającego, którego wzór stanowi Załącznik nr 3 i na żądanie udostępnia je organowi nadzorczemu.
6. W celu ewidencjonowania podmiotów przetwarzających Inspektor Ochrony Danych prowadzi w postaci elektronicznej rejestr umów, w ramach których powierzono przetwarzanie danych osobowych.
7. Zabronione jest przekazywanie danych do państwa trzeciego (poza Europejski Obszar Gospodarczy) lub organizacji międzynarodowej. Odstępstwo od tej zasady możliwe jest tylko i wyłącznie po uzyskaniu zgody Inspektora Ochrony Danych, który dokonuje weryfikacji spełnienia przesłanek, o których mowa w Rozdziale V RODO.
8. Wszyscy pracownicy i współpracownicy PGS zobowiązani są do przestrzegania zasad bezpieczeństwa fizycznego pomieszczeń, w których przetwarzane są dane osobowe.

6. UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Inspektor Ochrony Danych, w imieniu Administratora danych nadaje upoważnienia do przetwarzania danych osobowych wszystkim osobom, które przetwarzają dane osobowe w PGS. Dotyczy to osób zatrudnionych na podstawie umowy o pracę, umów cywilno-prawnych, praktykantów i stażystów.
2. Wzór upoważnienia stanowi Załącznik nr 4.
3. Upoważnione mogą zostać jedynie osoby, które zostały przeszkolone i zapoznane z zasadami ochrony danych osobowych w PGS.
4. Oryginał upoważnienia przekazywany jest osobie, której dokument dotyczy, zaś kopia jest przechowywana w ewidencji osób upoważnionych, prowadzonej przez Inspektora Ochrony Danych w formie elektronicznej.
5. Upoważnienie ustaje w momencie rozwiązania lub wygaśnięcia umowy, która była podstawą relacji pomiędzy PGS sp. z o.o. a osobą upoważnioną lub odwołania przedmiotowego upoważnienia.

7. IDENTYFIKACJA ZMIAN W CZYNNOŚCIACH PRZETWARZANIA DANYCH OSOBOWYCH

1. Wszystkie czynności przetwarzania danych osobowych w PGS są ewidencjonowane w postaci rejestrów czynności przetwarzania: administratora danych i podmiotu przetwarzającego, którego wzory stanowią odpowiednio - Załącznik nr 2 i Załącznik nr 3.
2. Inspektor Ochrony Danych, na podstawie informacji przekazywanych od poszczególnych komórek organizacyjnych, uzupełnia przedmiotowe rejestry i nadzoruje ich aktualność.
3. Osoby przetwarzające dane osobowe w PGS zobowiązane są do niezwłocznego informowania Inspektora Ochrony Danych o jakichkolwiek zmianach w zakresie procesów przetwarzania danych osobowych w ramach poszczególnych zbiorów lub identyfikacji nowych zbiorów danych osobowych.
4. W przypadku wątpliwości czy nowe czynności przetwarzania powinny skutkować utworzeniem nowego zbioru danych należy skonsultować się z Inspektorem Ochrony Danych.

8. INFORMACJE PODAWANE OSOBIE, KTÓREJ DANE DOTYCZĄ (OBOWIĄZEK INFORMACYJNY)

1. W przypadku zbierania danych od osób, których te dane dotyczą, najpóźniej w momencie ich pozyskiwania, podmiot danych należy poinformować o:
   a) nazwie administratora i jego danych kontaktowych;
   b) celach przetwarzania danych osobowych i podstawie prawnej przetwarzania;
   c) prawnie uzasadnionym interesie realizowanym przez PGS (jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO);
   d) odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
   e) zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych (jeśli dotyczy);
   f) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu;
   g) prawie do żądania od PGS dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
   h) prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem (jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO);
   i) prawie wniesienia skargi do organu nadzorczego;
   j) tym, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
   k) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą (jeżeli dotyczy).
2. W przypadku zbierania danych z innych źródeł niż od osób, których te dane dotyczą, należy niezwłocznie (najpóźniej w ciągu 30 dni) poinformować podmiot danych o:
   a) nazwie administratora i jego danych kontaktowych;
   b) celach przetwarzania danych osobowych i podstawie prawnej przetwarzania;
   c) kategoriach danych osobowych;

d) odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
e) zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych (jeśli dotyczy);
f) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu;
g) prawnie uzasadnionym interesie realizowanym przez PGS (jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO);
h) prawie do żądania od PGS dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
i) prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem (jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO);
j) prawie wniesienia skargi do organu nadzorczego;
k) źródle pochodzenia danych osobowych;
l) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą (jeżeli dotyczy).

3. Inspektor Ochrony Danych prowadzi rejestr obowiązujących wzorów zgód na przetwarzanie danych osobowych i obowiązków informacyjnych.

9. ZASADY WYRAŻANIA ZGODY NA PRZETWARZANIE DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych na podstawie zgody jest możliwe tylko i wyłącznie wtedy, kiedy możliwe jest wykazanie, że osoba wyraziła tę zgodę.
2. Przedmiotowe zgody należy przechowywać w taki sposób, aby możliwe było wykazanie ich wyrażenia (rozliczalność).
3. Dozwolone jest wykorzystywanie formuł zgody zawartych w rejestrze obowiązujących wzorów zgód na przetwarzanie danych osobowych i obowiązków informacyjnych, prowadzonym przez Inspektora Ochrony Danych. W przypadku, gdy treść zgody wyrażonej przez Podmiot danych odbiega od zatwierdzonego wzoru należy zweryfikować czy otrzymana treść zgody jest poprawna i zbieżna z celem, dla którego została wyrażona. W przypadku wątpliwości należy skonsultować się z Inspektorem Ochrony Danych.
4. Za zamieszczenie klauzuli zgody w ramach mechanizmu gromadzącego dane oraz skuteczne jej pobranie, odpowiedzialna jest osoba nadzorująca proces, w ramach którego przetwarzane są dane.
5. Zgoda musi być przedstawiona w jasny i prosty sposób, wskazując na konkretny cel przetwarzania. Musi być wyodrębniona od pozostałej treści.
6. Zgoda nie może być wymuszona. Nie może być od niej uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy (dobrowolność wyrażenia zgody).
7. W przypadkach, gdy jest to podyktowane wykorzystaniem technologii informatycznych zgoda może być wyrażona w sposób elektroniczny, należy przy tym pamiętać, że PGS jest zobowiązana do udowodnienia, że konkretna zgoda została wyrażona w sposób zgody z powszechnie obowiązującymi przepisami prawa.
8. W przypadku zbierania danych osobowych od osób poniżej 16 roku życia należy pobrać zgodę od jej rodzica lub opiekuna prawnego.
9. Osoba, której dane przetwarzane są na podstawie zgody, ma prawo do jej cofnięcia w dowolnym momencie, o czym należy ją poinformować w momencie pobierania zgody.

10. Wycofanie zgody musi być równie łatwe jak jej wyrażenie, z zastrzeżeniem, że należy skorzystać z wszelkich rozsądnych środków w celu zweryfikowania tożsamości osoby wnioskującej.

10. ZARZĄDZANIE PODMIOTAMI PRZETWARZAJĄCYMI

1. Jeżeli przetwarzanie ma być dokonywane w imieniu PGS, należy korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO oraz niniejszej Polityki, a także chroniło prawa osób, których dane dotyczą. W tym celu właściciel biznesowy umowy, w ramach której będzie miało miejsce powierzenie przetwarzania danych osobowych, określa kryteria wyboru podmiotu, które z uwzględnieniem specyfiki danego procesu przetwarzania, zapewnią przedmiotowe gwarancje.
2. Właściciel biznesowy umowy zobowiązany jest uwzględnić konieczność weryfikacji podmiotu przetwarzającego w zakresie jego zgodności z wymaganiami ochrony danych osobowych, w porozumieniu z Inspektorem Ochrony Danych.
3. Dodatkowo, Właściciel biznesowy umowy, jeśli jest to zasadne, wyznacza kryteria wyboru podmiotu przetwarzającego uwzględniające ocenę w zakresie bezpieczeństwa danych osobowych, np. posiadanie przez podmiot przetwarzający odpowiednich certyfikatów bezpieczeństwa.
4. Powierzenie danych osobowych odbywa się na podstawie:
   - umowy powierzenia lub
   - klauzuli w umowie głównej, z zastrzeżeniem uwzględnienia wszystkich wymagań zawartych w umowie powierzenia.
5. Właściciel biznesowy umowy zobowiązany jest wskazać w umowie powierzenia opis środków bezpieczeństwa, które podmiot przetwarzający wdraża w celu zapewnienia poufności, integralności i dostępności danych osobowych.
6. Umowy powierzenia podlegają ewidencjonowaniu przez Inspektora Ochrony Danych w rejestrze umów powierzenia przetwarzania, z zastrzeżeniem konieczności wskazania relacji pomiędzy umową powierzenia a umową główną.
7. Przekazanie jakichkolwiek danych osobowych podmiotowi zewnętrznemu, w ramach zawartej umowy, możliwe jest dopiero w momencie zawarcia umowy powierzenia.
8. Współpraca z podmiotem przetwarzającym realizowana jest zgodnie z zawartą umową powierzenia oraz Zasadami bezpieczeństwa w kontaktach z podmiotami zewnętrznymi, stanowiącymi Załącznik nr 5 do niniejszej Polityki.
9. PGS sp. z o.o. i podmiot przetwarzający współpracują ze sobą w celu realizacji praw osób, których dane są przetwarzane.

11. OCHRONA DANYCH OSOBOWYCH W PROJEKTACH I NOWYCH OPERACJACH PRZETWARZANIA DANYCH OSOBOWYCH

1. Wszystkie osoby przetwarzające dane w PGS zobowiązane są do uwzględniania ochrony danych osobowych w fazie projektowania nowych rozwiązań technicznych / procesów lub wprowadzania znaczących modyfikacji w już istniejących. Należy wdrażać odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności.
2. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikającego z przetwarzania, osoba projektująca rozwiązanie techniczne

/ proces wdraża odpowiednie środki techniczne i organizacyjne (np. pseudonimizacja), zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak, by spełnić wymogi przepisów prawa oraz chronić prawa osób, których dane dotyczą.

3. Jeżeli dany rodzaj przetwarzania 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 należy dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych (PIA), w szczególności w przypadku:
    a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
    b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa lub
    c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.
4. Identyfikując operacje mogące powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych należy kierować się wytycznymi opublikowanymi przez polski organ nadzoru.

12. ZASADY AKTUALIZACJI

Inspektor Ochrony Danych odpowiada za przeprowadzenie przeglądu dokumentu co najmniej raz w roku. W przypadku konieczności wprowadzenia zmian dokonuje aktualizacji zapisów.

13. ARCHIWIZACJA DOKUMENTU

Archiwizacja odbywa się na zasadach określonych w przepisach i regulacjach wewnętrznych obowiązujących w przedmiotowym zakresie.

14. POSTANOWIENIA KOŃCOWE

Niewywiązywanie się z powyższych zaleceń może skutkować wyciągnięciem konsekwencji służbowych zgodnie z odrębnymi uregulowaniami.

15. ZAŁĄCZNIKI

Załącznik nr 1 – Zasady realizacji praw osób, których dane dotyczą

Załącznik nr 1 do Polityki Bezpieczeństwa Danych Osobowych
PGS Sp. z o.o.

ZASADY REALIZACJI PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

1. Zasady realizacji praw osób, których dane dotyczą, obejmują:
   - prawo dostępu do danych,
   - prawo do sprostowania danych,
   - prawo do usunięcia danych (prawo do bycia zapomnianym),
   - prawo do ograniczenia przetwarzania,
   - prawo do przenoszenia danych,
   - prawo do sprzeciwu,
   - prawo by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

2. Zasady ogólne realizacji praw:

2.1 Wszystkie wnioski oraz udzielone odpowiedzi, o których mowa w niniejszych Zasadach podlegają ewidencjonowaniu w Rejestrze realizacji praw osób, których dane dotyczą. Przedmiotowa ewidencja nadzorowana jest przez Inspektora Ochrony Danych.

2.2 Każdy wniosek powinien mieć formę pisemną. Dopuszczalna jest forma elektroniczna, z zastrzeżeniem, że musi ona umożliwiać zweryfikowanie tożsamości osoby wnioskującej, np. w przypadku pracownika wysłanie wiadomości elektronicznej z firmowej, imiennej skrzynki, w przypadku osoby spoza organizacji, poprzez wykorzystanie podpisu cyfrowego, użycie profilu zaufanego lub potwierdzenie za pomocą innego kanału komunikacji lub przez wskazanie w wiadomości danych umożliwiających identyfikację podmiotu danych.

2.3 Wszelka korespondencja prowadzona z podmiotem danych powinna być prowadzona w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

2.4 Wszystkie wnioski są wolne od opłat, chyba że Zarząd PGS sp. z o.o. (dalej: PGS) podejmie inną decyzję wskazując wysokość opłaty do pobrania, uwzględniając administracyjne koszty obsługi żądania.

2.5 W przypadku gdy osobą wnioskującą jest pracownik lub osoba zatrudniona na innej podstawie prawnej w PGS, realizuje go firma zewnętrzna świadcząca na rzecz PGS obsługę kadrową we współpracy z Inspektorem Ochrony Danych. W pozostałych przypadkach osobą odpowiedzialną za wskazanie komórki organizacyjnej realizującej wniosek jest Inspektor Ochrony Danych.

2.6 Odpowiedź jest udzielana tym samym kanałem, którym wpłynął wniosek lub innym, zgodnie ze wskazaniem osoby wnioskującej, w terminie 30 dni od dnia wpłynięcia wniosku.

2.7 PGS informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania każdego odbiorcę, któremu ujawniono dane osobowe, chyba że w wyjątkowych przypadkach okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. PGS informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli tego zażąda.

2.8 Inspektor Systemów Informatycznych zobowiązany jest do współpracy z osobą odpowiedzialną za rozpatrzenie wniosku w celu jego sprawnej i kompletnej realizacji.

2.9 Realizacja przedmiotowych praw nie może niekorzystnie wpływać na prawa i wolności innych osób, nie może także naruszać tajemnicy przedsiębiorstwa, własności intelektualnej czy praw autorskich.

3. **Prawo dostępu do danych** jest realizowane zgodnie z następującymi zasadami:

3.1 Każda osoba, której dane dotyczą, może zwrócić się do PGS z wnioskiem o dostęp do danych jej dotyczących.

3.2 W ramach przedmiotowego prawa osoba wnioskująca jest uprawniona do uzyskania dostępu do danych oraz następujących informacji:

a) cele przetwarzania;
b) kategorie danych osobowych;
c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych oraz podjętych w związku z tym zabezpieczeniach;
d) planowany okres przechowywania danych osobowych;
e) informacje o prawie do żądania od PGS sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
f) informacje o prawie wniesienia skargi do organu nadzorczego;
g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;

h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą (jeżeli dotyczy).

3.3 Jeżeli PGS przetwarza duże ilości informacji o osobie, której dotyczy zapytanie, przed podaniem informacji może zwrócić się do wnioskodawcy z prośbą o sprecyzowanie informacji lub czynności przetwarzania, których dotyczy żądanie.

3.4 Załącznikiem do udzielanej odpowiedzi jest kopia danych osobowych podlegających przetwarzaniu.

4. **Prawo do sprostowania danych** jest realizowane zgodnie z następującymi zasadami:

4.1 Każda osoba, której dane dotyczą, może zwrócić się do PGS z wnioskiem o sprostowanie swoich danych.

4.2 Poprzez sprostowanie należy rozumieć:

- poprawienie nieprawidłowych danych,
- uzupełnienie niekompletnych danych.

4.3 Prawo do sprostowania danych jest realizowane w ramach standardowych procesów obsługi danych w poszczególnych zbiorach, zgodnie z regulacjami wewnętrznymi PGS.

5. **Prawo do usunięcia danych („prawo do bycia zapomnianym")** jest realizowane zgodnie z następującymi zasadami:

5.1 Każda osoba, której dane dotyczą, może zwrócić się do PGS z wnioskiem o usunięcie swoich danych.

5.2 Osoba realizująca wniosek wskazuje zakres danych możliwych do usunięcia, z zastrzeżeniem, że usunięcie danych osoby możliwe jest tylko w przypadku wystąpienia jednej z przesłanek:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;

c) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania na mocy art. 21 RODO i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;

d) dane osobowe były przetwarzane niezgodnie z prawem;

e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego;
f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 RODO.

5.3 Odmowa uwzględnienia całości lub części wniosku może wynikać przede wszystkim z faktu, że dalsze przetwarzanie danych osobowych jest niezbędne:
a) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy przepisów prawa;
b) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych;
c) do ustalenia, dochodzenia lub obrony roszczeń.

5.4 Po ustaleniu zakresu danych możliwych do usunięcia dane te są niezwłocznie usuwane ze wszystkich nośników, na których się znajdują, niezależnie od ich formy.

5.5 W celach dowodowych zachowuje się wniosek osoby oraz treść odpowiedzi, co nie rodzi niezgodności z obowiązującymi przepisami w zakresie ochrony danych osobowych.

6. **Prawo do ograniczenia przetwarzania** rozumiane jest jako oznaczenie przechowywanych danych osobowych, zarówno w postaci elektronicznej, jak i w postaci papierowej, w celu ograniczenia ich przyszłego przetwarzania (nakaz przechowywania przez administratora dotychczas zebranych danych oraz brak możliwości dokonywania na nich innych operacji niż przechowywanie), jest ono realizowane zgodnie z następującymi zasadami:

6.1 Każda osoba, której dane dotyczą, może zwrócić się do PGS z wnioskiem o ograniczenie przetwarzania swoich danych.

6.2 Osoba, której dane dotyczą, ma prawo żądania ograniczenia przetwarzania w następujących przypadkach:
a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający PGS sprawdzić prawidłowość tych danych;
b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
c) PGS nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
d) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie PGS są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

6.3 W przypadku, gdy w ramach prowadzonego przez organ nadzorczy postępowania w sprawie naruszenia przepisów o ochronie danych osobowych, wnosi on o ograniczenie przetwarzania, wskazuje jednocześnie dopuszczalny zakres przetwarzania oraz okres ograniczenia.

6.4 Przed uchyleniem ograniczenia przetwarzania PGS informuje o tym osobę wnioskującą.

7. **Prawo do przenoszenia danych** jest realizowane zgodnie z następującymi zasadami:

7.1 Każda osoba, której dane dotyczą, może zwrócić się do PGS z wnioskiem o udostępnienie lub przesłanie swoich danych do innego administratora.

7.2 Wniosek jest rozpatrywany pozytywnie, gdy przetwarzanie odbywa się w sposób zautomatyzowany na podstawie zgody osoby lub zawartej umowy. Przeniesieniu podlegają dane, które podmiot danych sam dostarczył PGS (dane przekazane aktywnie i świadomie przez osobę, której dane dotyczą, oraz wygenerowane poprzez jej działanie – zaobserwowane w związku z korzystaniem przez nią z usług lub urządzeń). Prawo do przenoszenia danych nie obejmuje danych wytworzonych przez PGS, czyli uzyskanych w wyniku wtórnego przetwarzania danych pozyskanych.

7.3 Osoba realizująca wniosek przygotowuje plik z danymi osoby wnioskującej i zapisuje go z zachowaniem obowiązujących w PGS zasad bezpieczeństwa teleinformatycznego, wskazanych w Polityce Bezpieczeństwa Teleinformatycznego.

7.4 Zależnie od treści wniosku dane są przekazywane osobie, której dane dotyczą lub wskazanemu przez nią administratorowi danych.

7.5 Przekazanie lub przesłanie pliku do innego administratora realizowane jest w sposób zapewniający bezpieczeństwo danych, zgodnie z zasadami wskazanymi w Polityce Bezpieczeństwa Teleinformatycznego.

7.6 Realizacja przedmiotowego prawa nie oznacza automatycznego usunięcia danych osoby, które przetwarzane są przez PGS.

8. **Prawo do sprzeciwu** jest realizowane zgodnie z następującymi zasadami:

8.1 Każda osoba, której dane dotyczą, może złożyć wniosek, w którym sprzeciwia się przetwarzaniu swoich danych, w tym profilowaniu.

8.2 Realizacja przedmiotowego prawa jest możliwa gdy przetwarzanie jest realizowane w związku z prawnie uzasadnionym interesem realizowanym przez PGS, który nie jest nadrzędny wobec interesów, praw i wolności osoby, której dane dotyczą. W związku z tym, PGS może odmówić zaprzestania przetwarzania danych osobowych, powołując się na:

- istnienie ważnych, prawnie uzasadnionych podstaw do przetwarzania danych, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub
- istnienie podstaw do ustalenia, dochodzenia lub obrony roszczeń.

8.3 Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść skutecznie sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

9. **Prawo by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa** jest realizowane zgodnie z następującymi zasadami:

9.1 Realizacja przedmiotowego prawa nie będzie miała miejsca w sytuacji, w której przetwarzanie:
- nie jest w pełni zautomatyzowane, tj. finalną decyzję podejmuje człowiek na podstawie wyników zautomatyzowanego przetwarzania oraz innych czynników,
- nie rodzi wobec osoby skutków prawnych, ani też znacząco na nią nie wpływa.

9.2 Realizacja przedmiotowego prawa nie będzie również możliwa w sytuacji gdy:
- przetwarzanie to jest niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą a PGS;
- przetwarzanie to jest dozwolone przepisami prawa i przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub
- opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

9.3 W ramach każdej operacji przetwarzania, opartej wyłącznie na zautomatyzowanym podejmowaniu decyzji, rodzącej wobec osoby skutki prawne lub w inny sposób znacząco na nią wpływającej, osobie zapewnia się możliwość odwołania od decyzji PGS.

9.4 W ramach realizacji przedmiotowego wniosku (odwołania) należy dokonać indywidualnej analizy zgromadzonych danych i weryfikacji czy stosowany algorytm zautomatyzowanego przetwarzania uwzględnił wszystkie istotne czynniki mające wpływ na podjętą decyzję (w ramach prawa do interwencji ludzkiej).

9.5 Decyzję w zakresie realizacji przedmiotowego prawa w ramach realizowanych operacji przetwarzania danych osobowych podejmuje Inspektor Ochrony Danych na podstawie analizy tych operacji i wykorzystywanych mechanizmów przetwarzania.