Polityka prywatności

Samorząd Pod Lupą z inicjatywy Nowej Nadziei

1. Administrator i kontakt

Administratorem danych osobowych przetwarzanych w związku z działaniem serwisu **Samorząd Pod Lupą z inicjatywy Nowej Nadziei**, dalej „Serwis”, jest **partia polityczna „Nowa Nadzieja”**, ul. Piękna 3/8, 00-539 Warszawa, NIP 7011300979, REGON 544041673, dalej „Administrator”.

Kontakt w sprawach ochrony danych i realizacji praw: **kontakt@wolnosc.pl** lub korespondencyjnie na powyższy adres, z dopiskiem „Ochrona danych”. Serwis działa pod adresem **https://samorzadpodlupa.pl/**.

Polityka opisuje przetwarzanie danych związane ze zgłoszeniami, weryfikacją spraw, publikowaniem ustaleń, korespondencją, obsługą techniczną i pracą zespołu. RODO oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.

2. Zgłoszenie bez ujawniania tożsamości

Formularz nie wymaga imienia, nazwiska, adresu e-mail, telefonu ani konta zgłaszającego. Ma to ułatwiać przekazywanie informacji osobom obawiającym się lokalnych konsekwencji i ograniczać zakres gromadzonych danych. Administrator nie zbiera dodatkowych informacji wyłącznie po to, aby ustalić tożsamość zgłaszającego.

Zgłoszenie i dołączenie plików są dobrowolne. Opis sprawy oraz wymagane informacje o jej obszarze są potrzebne do przyjęcia i obsługi zgłoszenia. Brak wystarczających informacji może uniemożliwić weryfikację. Niepodanie danych kontaktowych nie blokuje zgłoszenia.

Anonimowy sposób wysłania nie oznacza, że materiał nie zawiera danych osobowych. Treść, zdjęcie lub dokument mogą identyfikować zgłaszającego albo inne osoby. Oczyszczanie plików nie usuwa danych widocznych na obrazie. Kontakt przez e-mail ujawnia dane wynikające z użytej poczty. Dane techniczne połączenia opisano w pkt 8.

Status sprawdza się przy użyciu kodu sprawy i tajnego kodu dostępu otrzymanych po przyjęciu zgłoszenia. Należy je zachować i chronić. Serwis nie odtwarza ich na podstawie tożsamości, nie udostępnia komunikatora i nie pozwala ponownie pobrać przesłanych plików.

3. Zakres i źródła danych

- **Zgłoszenia i ich obsługa:** opis sprawy, wskazany obszar, załączniki, informacje potrzebne do sprawdzania statusu, przebieg obsługi oraz ustalenia zespołu.
- **Osoby opisane w materiałach:** dane identyfikacyjne, informacje o funkcji, działalności i zdarzeniach związanych ze sprawą, a także dane świadków i zgłaszającego, jeżeli znalazły się w treści lub korespondencji. Zakres jest ograniczany do danych niezbędnych i dopuszczalnych prawem.
- **Korespondencja i reklamacje:** treść wiadomości, dobrowolnie podane dane nadawcy i kontakt potrzebny do odpowiedzi.
- **Korzystanie z Serwisu i praca zespołu:** dane techniczne połączenia i zdarzeń bezpieczeństwa, dane kont członków zespołu, ich upoważnień oraz czynności związanych z obsługą spraw.

Źródłami są zgłoszenia i załączniki, korespondencja, legalnie dostępne źródła publiczne, w tym Biuletyn Informacji Publicznej i rejestry, odpowiedzi na wnioski o informację publiczną oraz wyjaśnienia osób i instytucji. Dane mogą więc pochodzić od osoby, której dotyczą, od zgłaszającego lub z innych wskazanych źródeł.

4. Cele i podstawy prawne

Przyjmowanie i weryfikacja zgłoszeń. Podstawą dla zwykłych danych osobowych jest art. 6 ust. 1 lit. f RODO. Prawnie uzasadnionym interesem jest obywatelska kontrola spraw publicznych, wyjaśnianie sygnałów o nieprawidłowościach i wspieranie rzetelnej debaty. Administrator ocenia niezbędność przetwarzania i równowagę między tym interesem a prawami osób.

Kontakt, reklamacje, organizacja pracy i bezpieczeństwo. Podstawą jest art. 6 ust. 1 lit. f RODO, a interesem sprawna obsługa spraw i korespondencji, ochrona przed nadużyciami oraz rozliczalność dostępu. Dane związane z umową z członkiem zespołu są przetwarzane także na podstawie art. 6 ust. 1 lit. b RODO w zakresie niezbędnym do jej wykonania.

Obowiązki prawne i roszczenia. Art. 6 ust. 1 lit. c RODO stanowi podstawę wypełniania obowiązków wynikających z RODO, w tym realizacji praw osób i reagowania na naruszenia, oraz wiążących żądań właściwych organów opartych na przepisach prawa. Niezbędne dane mogą być zachowane dla ustalenia, dochodzenia lub obrony roszczeń na podstawie art. 6 ust. 1 lit. f RODO.

Publikowanie ustaleń. Publikacja danych identyfikujących osobę wymaga odrębnej oceny podstawy prawnej, niezbędności i proporcjonalności. Przy zastosowaniu art. 6 ust. 1 lit. f RODO interesem jest informowanie o zweryfikowanych sprawach publicznych, z uwzględnieniem praw osób. Przyjęcie zgłoszenia nie oznacza automatycznej publikacji; zbędne dane prywatne są usuwane lub anonimizowane.

Dane ze zgłoszeń nie są wykorzystywane do marketingu, profilowania wyborców, reklamy politycznej ani rekrutacji do partii. Akceptacja Regulaminu nie zastępuje podstawy prawnej. Jeżeli dodatkowa czynność wymaga zgody, jest ona uzyskiwana odrębnie, dla wskazanego celu.

5. Dane wymagające szczególnej ochrony

Nie należy przesyłać zbędnych danych o zdrowiu, poglądach politycznych, przekonaniach, przynależności związkowej, życiu intymnym ani innych szczególnych kategorii danych. Ich wykorzystanie wymaga podstawy z art. 6 RODO oraz odpowiedniej przesłanki z art. 9 ust. 2 RODO. Sama zgoda zgłaszającego lub ogólne powołanie się na interes społeczny nie uprawniają do przetwarzania takich danych innej osoby.

Przesłanka szczególna jest ustalana dla konkretnej sytuacji, np. gdy osoba sama w sposób oczywisty upubliczniła dane albo są one niezbędne dla roszczeń. Sama dostępność informacji w Internecie nie oznacza jej upublicznienia przez tę osobę. Przepisy dotyczące działalności partii wobec członków lub osób utrzymujących z nią stałe kontakty nie obejmują automatycznie wszystkich osób wymienionych w zgłoszeniach.

Dane dotyczące wyroków skazujących i czynów zabronionych, objęte art. 10 RODO, wymagają podstawy przewidzianej prawem; sam art. 6 ust. 1 lit. f RODO nie wystarcza. Jeżeli brak właściwej podstawy dalszego przetwarzania danych szczególnie chronionych, są one usuwane lub skutecznie anonimizowane i nie są w tym zakresie dalej analizowane ani publikowane. Można nadal weryfikować fakty niewymagające ich przetwarzania.

6. Załączniki i poufność zgłoszeń

Załączniki są kontrolowane i oczyszczane ze zbędnych metadanych, np. informacji o autorze lub lokalizacji zapisanych poza widoczną treścią. Oryginał jest przetwarzany przejściowo w celu przygotowania zabezpieczonej kopii, a następnie usuwany wraz z niepotrzebnymi plikami pośrednimi. Oryginały nie są archiwizowane ani zachowywane w kopiach bezpieczeństwa. Przy braku możliwości bezpiecznego przetworzenia plik jest odrzucany i usuwany.

Oczyszczanie nie zasłania danych widocznych w dokumencie lub na zdjęciu. Może też usuwać właściwości oryginalnego pliku, w tym możliwość weryfikacji podpisu elektronicznego. Zgłaszający powinien ograniczyć zbędne informacje przed wysłaniem i zachować własny oryginał, jeżeli legalnie go posiada.

Treść zgłoszeń i oczyszczone załączniki są przechowywane z zastosowaniem szyfrowania. Połączenie z Serwisem jest szyfrowane. Administrator ogranicza uprawnienia do danych, weryfikuje dostęp i zobowiązuje upoważnione osoby do poufności. Materiały są wykorzystywane wyłącznie w zakresie niezbędnym do zgodnych z prawem zadań.

Zabezpieczenia ograniczają ryzyko nieuprawnionego dostępu, lecz nie oznaczają gwarancji pełnej anonimowości. Tożsamość może wynikać z samego materiału, a bezpieczeństwo zależy również od urządzenia i połączenia użytkownika. Anonimowy formularz nie wyklucza przetwarzania danych osobowych zawartych w zgłoszeniu.

7. Dostęp do danych i ich odbiorcy

W ramach Administratora dostęp mają upoważnione osoby obsługujące i weryfikujące sprawy, osoby sprawujące nadzór oraz osoby wykonujące niezbędne zadania techniczne. Zakres dostępu odpowiada zadaniom. Sprawa może wymagać konsultacji z innym upoważnionym członkiem zespołu. Samo członkostwo w partii nie daje dostępu do zgłoszeń.

Dane mogą być przekazywane następującym kategoriom odbiorców, wyłącznie w niezbędnym i zgodnym z prawem zakresie:

- **Dostawcy usług technicznych:** hosting, utrzymanie strony, zabezpieczenia, kopie bezpieczeństwa i poczta elektroniczna. Podmioty działające w imieniu Administratora przetwarzają dane na podstawie wymaganych umów powierzenia.
- **Radcowie prawni i adwokaci:** w celu konsultacji lub obsługi prawnej, z zachowaniem właściwej podstawy przetwarzania i tajemnicy zawodowej.
- **Właściwe organy:** gdy ujawnienie wynika z obowiązku prawnego lub istnieje inna odpowiednia podstawa przekazania danych w konkretnej sprawie.
- **Odbiorcy publikacji:** tylko w zakresie informacji, których publikacja została odrębnie uznana za zgodną z prawem i konieczną. Nie uzyskują dostępu do bazy zgłoszeń.

Wyjaśnianie sprawy z osobą lub instytucją, której ona dotyczy, odbywa się z ograniczeniem ujawnianych danych i ochroną źródła. Dane identyfikujące zgłaszającego nie są publikowane bez jego odrębnej, świadomej zgody, chyba że ujawnienie wynika z obowiązku prawnego.

8. Dane techniczne i cookies

Do zestawienia połączenia, ochrony Serwisu i diagnostyki infrastruktura obsługująca stronę może przetwarzać adres IP, czas połączenia oraz dane o przeglądarce i urządzeniu. Dane te nie są wymaganymi danymi identyfikacyjnymi w formularzu. Ich przetwarzanie ogranicza się do zakresu potrzebnego dla działania i bezpieczeństwa Serwisu.

W ścieżce zgłoszeniowej stosowane są wyłącznie mechanizmy cookies lub pamięci przeglądarki niezbędne do transmisji, świadczenia zamówionej usługi i jej bezpieczeństwa. Nie stosuje się reklamowych pikseli śledzących ani profilowania marketingowego.

Mechanizmy opcjonalne, jeżeli zostaną wprowadzone, wymagają wcześniejszej informacji i zgody zgodnie z art. 399 ustawy z dnia 12 lipca 2024 r. - Prawo komunikacji elektronicznej. Informacja obejmie cel, dostawcę, czas działania oraz sposób wycofania zgody. Ustawienia cookies można zmienić w przeglądarce; zablokowanie mechanizmów niezbędnych może uniemożliwić działanie formularza lub sesji.

9. Narzędzia pomocnicze i decyzje automatyczne

Serwis nie ma modułu AI automatycznie analizującego zgłoszenia. Ocenę materiałów, dalsze działania i publikację zatwierdzają upoważnione osoby. Kontrola techniczna plików nie stanowi decyzji wywołującej skutki prawne lub podobnie istotnie wpływającej na osobę. Nie są podejmowane takie decyzje oparte wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu.

Zespół może korzystać wyłącznie z zatwierdzonych narzędzi pomocniczych, z zachowaniem poufności i ograniczenia danych. Wprowadzenie danych osobowych do usługi zewnętrznej wymaga odpowiedniej podstawy prawnej, zabezpieczeń i wykonania obowiązku informacyjnego. Zgłoszenia nie są automatycznie przekazywane do publicznych narzędzi AI.

10. Przekazywanie danych poza EOG

Przekazanie danych poza Europejski Obszar Gospodarczy, także przez dostęp zagranicznego dostawcy, wymaga spełnienia warunków rozdziału V RODO. Podstawą może być właściwa decyzja Komisji Europejskiej albo odpowiednie zabezpieczenia, np. standardowe klauzule umowne wraz ze środkami uzupełniającymi, jeżeli są potrzebne.

Przed rozpoczęciem takiego przetwarzania Administrator udostępnia informację o faktycznym transferze, odbiorcy, państwie, zakresie danych i podstawie przekazania. Informacje o zastosowanych zabezpieczeniach i sposobie uzyskania ich kopii można otrzymać pod adresem kontaktowym wskazanym w pkt 1. Postanowienie to nie stanowi zgody na przekazanie danych dowolnemu dostawcy.

11. Okresy przechowywania

Dane są usuwane lub nieodwracalnie anonimizowane po ustaniu celu i podstawy przetwarzania. Obowiązują następujące okresy i kryteria:

Rodzaj danych	Okres lub kryterium przechowywania
Oryginały załączników	Wyłącznie przez czas potrzebny do kontroli i przygotowania zabezpieczonej kopii; następnie są usuwane. Pliki odrzucone są usuwane. Oryginały nie są archiwizowane.
Sprawy w toku	Przez okres niezbędny do weryfikacji i zgodnych z prawem dalszych działań. Potrzeba zachowania danych jest oceniana okresowo i przy zmianie etapu sprawy.
Sprawy zamknięte	Do 12 miesięcy od zamknięcia. Dłuższe zachowanie wymaga konkretnej podstawy, np. trwającego postępowania lub potrzeby ochrony roszczeń, oraz ponownej oceny niezbędności.

Rodzaj danych	Okres lub kryterium przechowywania
Dane i kopie zbędne	Są usuwane bez zbędnej zwłoki po stwierdzeniu ich nieprzydatności albo po zakończeniu zadania, do którego były potrzebne.
Kontakt i reklamacje	Do zakończenia obsługi, a następnie przez czas niezbędny do wykazania udzielonej odpowiedzi lub ochrony roszczeń, stosownie do ich charakteru i terminów przedawnienia.
Dane techniczne	Przez czas niezbędny do diagnostyki, ochrony przed nadużyciami i wyjaśnienia incydentów. Okres zależy od rodzaju zdarzenia i potrzeby zabezpieczenia dowodów; nie oznacza bezterminowego przechowywania.
Dane zespołu	Przez czas współpracy, a następnie w zakresie niezbędnym do wykonania obowiązków prawnych, rozliczenia czynności lub ochrony roszczeń.
Opublikowane ustalenia	Tak długo, jak publikacja jest zgodna z prawem, aktualna i uzasadniona interesem publicznym. Nowe informacje lub uzasadnione żądanie powodują ponowną ocenę.

Zasady usuwania obejmują również kopie bezpieczeństwa. Dane usunięte z bieżącego systemu nie są dalej wykorzystywane operacyjnie i są usuwane z kopii w cyklu zastępowania ich kolejnymi kopiami. Kopie nie służą bezterminowemu archiwizowaniu spraw; odtworzenie danych nie uchyla wcześniejszego obowiązku ich usunięcia.

12. Prawa osób i sposób ich realizacji

W granicach określonych przez RODO przysługuje prawo dostępu do swoich danych i uzyskania ich kopii, sprostowania, usunięcia, ograniczenia przetwarzania oraz wniesienia skargi do **Prezesa Urzędu Ochrony Danych Osobowych**. Informacje o składaniu skarg: **https://uodo.gov.pl/**.

Sprzeciw. Wobec przetwarzania na podstawie art. 6 ust. 1 lit. f RODO można wnieść sprzeciw z przyczyn związanych ze szczególną sytuacją danej osoby. Administrator zaprzestaje przetwarzania, chyba że wykaże ważne prawnie uzasadnione podstawy nadrzędne wobec jej praw i wolności albo podstawy związane z roszczeniami.

Zgoda i przenoszenie danych. Zgodę można wycofać w dowolnym momencie bez wpływu na zgodność wcześniejszego przetwarzania z prawem. Prawo do przenoszenia dotyczy danych dostarczonych przez osobę, przetwarzanych automatycznie na podstawie zgody lub umowy, w warunkach określonych przez RODO.

Złożenie wniosku. Żądanie należy skierować na **kontakt@wolnosc.pl** lub adres Administratora, opisując sprawę i dane, których dotyczy. Nie należy przesyłać tajnego kodu dostępu ani zbędnego dokumentu tożsamości. Przy uzasadnionych wątpliwościach mogą być potrzebne minimalne dodatkowe informacje pozwalające bezpiecznie potwierdzić uprawnienie.

Brak możliwości identyfikacji. Administrator nie ma obowiązku zbierać dodatkowych danych wyłącznie po to, aby ustalić tożsamość osoby. Gdy nie potrafi przyporządkować do niej danych, informuje o tym, jeśli jest to możliwe. Osoba może dostarczyć informacje umożliwiające rozpatrzenie żądania zgodnie z art. 11 RODO.

Termin odpowiedzi. Informacja o realizacji żądania jest udzielana bez zbędnej zwłoki, zasadniczo w ciągu miesiąca. Przy skomplikowaniu lub liczbie żądań termin można przedłużyć o dwa miesiące, informując o przyczynie w pierwszym miesiącu. Odmowa wymaga uzasadnienia i informacji o dostępnych środkach ochrony.

Ochrona innych osób. Dostęp do własnych danych nie oznacza automatycznego wydania całego zgłoszenia. Przy udzielaniu informacji i kopii uwzględnia się prawa innych osób oraz poufność źródła, w granicach dozwolonych prawem. Usunięcie danych osobowych nie zawsze oznacza zakończenie badania faktów publicznych.

13. Dane pozyskane od innych osób

Jeżeli danych nie pozyskano bezpośrednio od osoby, której dotyczą, lecz np. od zgłaszającego lub ze źródła publicznego, Administrator realizuje obowiązek z art. 14 RODO. Informuje tę osobę co do zasady najpóźniej w ciągu miesiąca, a przy wcześniejszym kontakcie lub udostępnieniu danych odpowiednio najpóźniej przy pierwszej takiej czynności. Informacja obejmuje kategorie i źródło danych.

Odstąpienie od indywidualnego zawiadomienia wymaga konkretnej przesłanki z art. 14 ust. 5 RODO i zastosowania wymaganych zabezpieczeń. Nie następuje automatycznie z uwagi na anonimowy charakter zgłoszenia. Publiczne udostępnienie tej Polityki nie zastępuje indywidualnej informacji, gdy jest ona wymagana.

14. Naruszenia ochrony danych i zmiany Polityki

Administrator reaguje na naruszenia ochrony danych i wykonuje obowiązki wynikające z art. 33 i 34 RODO. Jeżeli naruszenie może powodować wysokie ryzyko dla praw lub wolności osoby, zawiadamia ją bez zbędnej zwłoki, z uwzględnieniem wyjątków przewidzianych prawem.

Polityka jest aktualizowana przy zmianach sposobu przetwarzania, funkcji Serwisu lub przepisów. Jej aktualna treść jest dostępna w Serwisie. Nowy cel lub sposób przetwarzania wymaga odpowiedniej podstawy prawnej i wcześniejszego przekazania wymaganych informacji. Sama zmiana dokumentu nie oznacza zgody osoby.

Polityka jest stosowana od dnia jej udostępnienia przez Administratora w Serwisie. W sprawach ochrony danych należy korzystać z kontaktu wskazanego w pkt 1.