



REGULAMIN I POLITYKA PRYWATNOŚCI DOTYCZĄCY PLATFORMY ALERT-WHISTLEBLOWING

Niniejszy Regulamin określa zasady korzystania z Platformy ALERT Whistleblowing osadzonej w ramach serwisu internetowego www.osuma.pl i stanowi uzupełnienie Regulaminów i Polityki Prywatności osadzonych na stronie głównej serwisu www.osuma.pl.

Regulamin ma na celu realizację wymogów wynikających z Dyrektywy Parlamentu Europejskiego i Rady UE o ochronie sygnalistów (UE) 2019/1937, która weszła w życie na terenie RP weszła w życie **25 września 2024 r.** Realizacja uzgodnionego umownie przetwarzania danych co do zasady odbywa się na terytorium państwa członkowskiego Unii Europejskiej lub innego państwa będącego stroną Porozumienia o Europejskim Obszarze Gospodarczym.

Ponad to obsługa spraw zgłoszonych w ramach Platformy podlega ustawie o ochronie danych osobowych zgodnie z postanowieniem 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 jako „**RODO**”).

§1. Postanowienia ogólne

1. Firma OSUMA Sp. z o.o. z siedzibą przy. Ul. Czyżówka 14/2.11, 30-526 Kraków, NIP: 6793368122, zwana dalej OSUMA zobowiązuje się do udostępnienia narzędzia służącego do rejestracji naruszeń wynikających z Dyrektywy (UE) 2019/1937. Narzędziem udostępnianym do rejestracji naruszeń jest Platforma o nazwie ALERT- Whistleblowing, zwanej niżej Platformą.
2. Platforma jest udostępniana jedynie pracownikom i współpracownikom Klienta, z którym OSUMA podpisała umowę na świadczenie tej Usługi.
3. Platforma jest osadzona na subdomenie serwisu www.osuma.pl.
4. Użytkownik pragnący skorzystać z Platformy ma obowiązek zapoznania się z osadzonymi na stronie www.osuma.pl regulaminami oraz Polityką Prywatności, a rejestrując zgłoszenie na Platformie tym samym akceptuje ich zapisy i nie wnosi żadnych uwag.
5. Platforma służy do zgłaszania:
 - naruszeń prawa
 - nieprawidłowości powiązanych z pracodawcą lub współpracownikiem
6. Użytkownik Platformy zobowiązany jest do korzystania z Platformy zgodnie z jej przeznaczeniem i niniejszym Regulaminem.
7. Użytkownicy Platformy nie mogą przekazywać haseł, loginów, kopiować ani w jakikolwiek sposób przekazywać informacji powiązanych z zarejestrowanym incydentem stronom trzecim, za wyjątkiem sytuacji dozwolonych przepisami prawa.



8. Firma OSUMA podpisując umowę z Klientem zobowiązuje go oraz osoby odpowiedzialne za obsługę administracyjną platformy stojące po stronie Klienta, do przestrzegania zasad regulaminów oraz ochrony prywatności zgodnie z RODO.
9. OSUMA nie ponosi odpowiedzialności za zakłócenia, w tym przerwy w funkcjonowaniu Platformy wynikające z problemów technicznych Użytkownika, wynikające między innymi z braku dostępu do Internetu, przerwami w dostępie do Internetu, innymi problemami technicznymi Użytkownika uniemożliwiającymi rejestrację zgłoszenia. W szczególności nie odpowiada za problemy z rejestracją wynikające z siły wyższej czy przerwach w dostawie serwisu wynikających z planowanych aktualizacji oprogramowania.
10. Dane mogą być przetwarzane przez podmiot technicznie obsługujący system zgłoszeń, z którym OSUMA zawarła umowę, zwany dalej Podmiotem Technicznym.
OSUMA występuje jako podmiot umożliwiający zbieranie danych w oparciu o podpisane umowy z Klientami. Podmiot Techniczny odpowiedzialny za utrzymanie Platformy może przetwarzać dane na podstawie umowy powierzenia danych. Zakres przetwarzania danych sprowadza się do zabezpieczenia technicznych i organizacyjnych środków bezpieczeństwa zgodnie z Załącznikiem do Regulaminu.

§2. Zgłoszenia

1. Zgłoszenia na Platformie mogą być:
 - a. imienne – Użytkownik podaje dane umożliwiające identyfikację jak adres email, w polu widocznym dla Administratora
 - b. częściowo anonimowe – Użytkownik podaje prywatny adres email w polu niewidocznym dla Administratora
 - c. w pełni anonimowe – Użytkownik nie podaje żadnych danych identyfikacyjnych (zgłoszenie będzie w pełni anonimowe pod warunkiem, że w załączonych dokumentach do sprawy dane identyfikacyjne nie widnieją)
2. Zgłoszenia muszą być składane w dobrej wierze.
3. Użytkownik akceptując ten Regulamin potwierdza, że jest świadomym tego, że składanie fałszywych zgłoszeń może wiązać się z odpowiedzialnością karną.
4. Użytkownik Platformy przyjmuje do wiadomości, że podanie przez niego danych osobowych oznacza początek przetwarzania przez Administratora i jest dobrowolne.
5. Dane osobowe Użytkowników powiązanych z Klientami firmy OSUMA są przetwarzane zgodnie z Polityką Prywatności dostępną na stronie www.osuma.pl. Przez Klienta należy rozumieć Firmę/Instytucję, z którą OSUMA podpisała umowę na realizację usługi.
6. Dane osobowe Użytkowników Platformy są równocześnie przetwarzane zgodnie z polityką prywatności Klienta oraz w oparciu o Techniczne i organizacyjne środki bezpieczeństwa zapewnione przez Klienta oraz Podmiot Techniczny.
7. Administratorem danych osobowych Użytkownika po dokonaniu rejestracji sprawy/naruszenia staje się dedykowany operator subdomeny wyznaczony po stronie Klienta, zwany niżej Administratorem.
8. Administrator zobowiązany jest do przestrzegania przepisów RODO oraz ustawy o ochronie sygnalistów.



9. Dane przetwarzane są w celu obsługi zgłoszeń naruszeń prawa. Podanie danych jest dobrowolne.
10. Dane mogą być przetwarzane przez Podmiot Techniczny zgodnie z klauzulą informacyjną stanowiącą Załącznik nr 1.
11. OSUMA rości sobie prawo do usunięcia dostępu Użytkownika do Platformy w razie naruszeń Regulaminu lub Polityki Prywatności i tym samym rości sobie prawo do skierowania sprawy dotyczącej naruszeń do organów ścigania. Wszelkie próby złamania stosowanych zabezpieczeń będą podstawą do pociągnięcia do odpowiedzialności karnej.
12. Kontakt z Administratorem danych osobowych jest możliwy za pośrednictwem poczty elektronicznej: biuro@osuma.pl lub drogą pocztową na adres siedziby spółki OSUMA Sp. z o.o. z zapiskiem „Ochrona Danych Osobowych”. Korzystając z tej opcji Użytkownik przekazuje dobrowolnie dane osobowe do OSUMA celem przekazania do właściwego Administratora. Tym samym, Użytkownik zgadza się na przetwarzanie tych danych zgodnie z Polityką Prywatności OSUMA, udostępnioną w ramach serwisu www.osuma.pl oraz w oparciu o niniejszy Regulamin.
13. W ramach świadczonej usługi stosowane są następujące środki bezpieczeństwa:
 - a. szyfrowanie transmisji (TLS)
 - b. kontrola dostępu
 - c. anonimizacja danych
 - d. regularne testy bezpieczeństwa

§3. Procedura obsługi zgłoszeń

1. Klient zobowiązany jest do ustanowienia procedury zgłoszeń nieprawidłowości w firmie, zwanej dalej Procedurą. Obowiązująca u Klienta Procedura określa zasady zgłaszania naruszeń prawa oraz ochrony sygnalistów.
2. Użytkownik zgłaszając naruszenie rejestruje na Platformie sprawę, która ma nadany unikalny numer.
3. Platforma umożliwia wprowadzenie załączników potwierdzających zaistnienie nieprawidłowości.
4. Po zarejestrowaniu sprawy, Użytkownik będzie w stanie uzupełnić swój wniosek, ale nie będzie w stanie usunąć żadnych elementów, które wcześniej załączył czy przekazał w zgłoszeniu.
5. Dedykowany Administrator analizuje zgłoszenie i procesuje zgodnie z procedurą udostępnioną w regulaminie Firmy/Instytucji, której sprawa dotyczy.
6. Komunikacja zwrotna oraz status zgłoszenia będzie udostępniana w ramach Platformy, po zalogowaniu się do numeru sprawy, który zostanie jej nadany.
7. Administrator zobowiązany jest do potwierdzenia przyjęcia zgłoszenia oraz odpowiedzi, w terminie określonym w ustawie o Ochronie Sygnalistów.
8. Użytkownik Platformy dokonujący rejestracji zgłoszenia zobowiązany jest do zapisania lub zapamiętania danych do logowania oraz numeru sprawy, celem weryfikacji postępów prowadzonego postępowania. Utrata tych danych w przypadku zgłoszeń anonimowych uniemożliwi weryfikację postępów sprawy, w tym informacji i odpowiedzi załączonych do sprawy przez Administratora.



9. Użytkownik zapamięta dane użyte do logowania w momencie rejestracji sprawy oraz numer jej przypisany, pod rygorem możliwości utraty dostępu do zgłoszonej sprawy.
 10. Dane powiązane z zarejestrowaną sprawą będą przechowywane przez okres:
 - niezbędny do rozpatrzenia zgłoszenia
 - oraz przez czas wymagany przepisami prawa
-

§4. Ochrona danych

1. Dane osobowe zbierane są w celu:
 - przyjmowania i weryfikacji zgłoszeń
 - umożliwienia prowadzenia postępowań wyjaśniających
 - realizacji obowiązków prawnych związanych z ochroną sygnalistów
2. Dane mogą być przekazywane:
 - upoważnionym pracownikom Klienta
 - podmiotom wspierającym (np. dostawcy systemu IT)
 - organom publicznym – jeśli wymagają tego przepisy
3. Administratorem danych osobowych rejestrowanych na Platformie jest Firma/Instytucja (zwana Klientem) wskazana przez Użytkownika Platformy w momencie rejestracji sprawy/incydentu.
4. Pracownicy lub współpracownicy Klienta widocznego na liście obsługiwanych podmiotów (Klientów) udostępnionej w ramach Portalu ALERT-Whistleblowing są jedynymi Użytkownikami, którzy mogą rejestrować na Platformie sprawy.
5. Użytkownik, który zarejestrował sprawę przekazuje swoje dane Klientowi do weryfikacji i tym samym Klient, którego wskazał staje się Administratorem jego danych osobowych, zgodnie z Polityką Prywatności Klienta.
6. Lista obsługiwanych podmiotów dostępna na Portalu ALERT Whistleblowing jest aktualizowana na bieżąco w oparciu o aktywne umowy podpisane z Klientami na udostępnienie tej usługi.
7. Klienci oraz wyznaczeni przez nich Administratorzy podlegają obowiązkowi wynikającemu z art. 26 RODO i zobowiązują się w szczególności do:
 - a) zapewnienia zgodności przetwarzania z obowiązującymi przepisami (w szczególności RODO oraz Ustawy o Ochronie Sygnalistów);
 - b) regularnego monitorowania procesów oraz środków technicznych i organizacyjnych celem zapewnienia poufności;
 - c) zapewnienia realizacji praw osób, których dane dotyczą, oraz obowiązków informacyjnych (art. 13 i 14 RODO);
 - d) współpracy z organem nadzorczym w razie zaistnienia takiej konieczności
8. Przetwarzane kategorie danych osobowych to dane osobowe przekazane przez Klientów, które pochodzą bezpośrednio od nich. OSUMA wymaga jedynie



tych danych, które pozwalają na realizację stosownej Umowy z Klientem przy zachowaniu przepisów RODO.

9. Kategorie osób, których dotyczy przetwarzanie danych, obejmują:

- osoby pełniące funkcję Operatorów Subdomeny(Administratorów) wskazane przez Klienta
- osoby przekazujące informacje;
- osoby, których dotyczy zgłoszenie;
- członkowie komisji weryfikacyjnych
- inne osoby zaangażowane
- świadkowie;
- pracowników Klienta;
- pracowników tymczasowych zatrudnionych obecnie lub wcześniej przez Klienta;
- osoby trzecie, jeżeli ma to zastosowanie.

10. Kategorie danych jakie mogą podlegać przetwarzaniu:

- a. Informacje dotyczące tożsamości sygnalistów oraz dane kontaktowe, o ile zgłoszenie nie zostało dokonane anonimowo,
- b. Dane osób, których dotyczy zgłoszenie lub które są w inny sposób zaangażowane (np. nazwisko, imię, stanowisko, dane kontaktowe, kontekst zatrudnienia),
- c. Dane zawarte w zgłoszeniach;
- d. Dane powstałe w związku z analizą i obsługą zgłoszeń oraz działaniami następczymi,
- e. Dane dotyczące planowania i kontroli,
- f. Adresy IP, pliki logów, typy przeglądarek.

11. Użytkownik, który przekazał Administratorowi swoje dane osobowe, ma prawo do:

- a. dostępu do swoich danych -art.5 RODO (GDPR),
- b. prawo do sprostowania (poprawiania) swoich danych- art.16.GDPR, przy czym w ramach Portalu nie będzie w stanie usuwać załączników, a jedynie uzupełniać sprawę o dodatkowe załączniki czy informacje
- c. usunięcia danych –art.17 GDPR, co będzie równoznaczne z zamknięciem sprawy i rezygnacją z jej procedowania
- d. ograniczenia przetwarzania danych osobowych, co umożliwia wybór kategorii zgłoszenia;
- e. wycofania zgody w dowolnym momencie – art. 7 ust3 GDPR (RODO), przy czym będzie to równoznaczne z decyzją o zamknięciu sprawy na etapie pośrednim i rezygnację z dalszego procesowania;
- f. wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy Użytkownik uzna, że przetwarzanie danych osobowych narusza przepisy RODO.

Realizacja praw może być ograniczona w zakresie niezbędnym do ochrony sygnalisty.



12. Zagubienie danych do logowania oraz numeru sprawy w ramach opcji w pełni anonimowej uniemożliwi Użytkownikowi dostęp do sprawy ze względu na jej szyfrowanie.
 13. Dane Użytkownika są usuwane po zamknięciu sprawy ramach Portalu.
 14. W razie naruszenia postanowień RODO, Użytkownikowi przysługuje prawo do wniesienia skargi do organów nadzoru, w tym do Prezesa Urzędu Ochrony Danych Osobowych.
-

§5. Odpowiedzialność użytkownika

1. Użytkownika rejestrującego sprawę obowiązuje zakaz składania fałszywych zgłoszeń.
 2. Użytkownik ponosi odpowiedzialność za nadużycia powiązane z zarejestrowaną sprawą, w tym odpowiedzialność karną.
-

§6. Wymagania techniczne

Do korzystania z Platformy niezbędne są:

- a) urządzenie z dostępem do sieci Internet i przeglądarką internetową typu Microsoft Internet Explorer, Google Chrome,
- b) aktywne konto poczty elektronicznej (e-mail),
- c) aktywne konto Klienta (Firmy/Instytucji), której zgłoszenie ma dotyczyć (widoczne w ramach listy rozwijalnej na Platformie ALERT Whistleblowing)





Załącznik nr 1 do REGULAMINU I POLITYKI PRYWATNOŚCI DOTYCZĄCY PLATFORMY ALERT-WHISTLEBLOWING

Techniczne i organizacyjne środki bezpieczeństwa zapewnione przez Podmiot Techniczny

1. Poufność (art. 32 ust. 1 lit. b RODO)

2. Integralność (art. 32 ust. 1 lit. b RODO)

Kontrola przekazywania danych

Zapobieganie nieuprawnionemu odczytowi, kopiowaniu, modyfikowaniu lub usuwaniu danych podczas ich elektronicznego przesyłania lub transportu.

- szyfrowanie danych.

Kontrola wprowadzania danych

Możliwość ustalenia, czy, kiedy i przez kogo dane osobowe zostały wprowadzone, zmienione lub usunięte w systemach przetwarzania danych.

- prowadzenie rejestrów i logów systemowych.

3. Dostępność i odporność systemów (art. 32 ust. 1 lit. b RODO)

Kontrola dostępności

Ochrona danych przed przypadkowym lub celowym zniszczeniem albo utratą.

- strategia wykonywania kopii zapasowych (online/offline, w lokalizacji i poza lokalizacją),
- ochrona antywirusowa,
- zapory sieciowe (firewall).

Szybkie przywracanie dostępności danych i dostępu do nich
(art. 32 ust. 1 lit. c RODO)

4. Procedury regularnego testowania, mierzenia i oceniania skuteczności środków bezpieczeństwa (art. 32 ust. 1 lit. d oraz art. 25 ust. 1 RODO)

- system zarządzania ochroną danych,
- procedury reagowania na incydenty bezpieczeństwa,
- domyślna ochrona danych (privacy by default) zgodnie z art. 25 ust. 2 RODO.

Kontrola przetwarzania na zlecenie

Przetwarzanie danych osobowych przez podmiot przetwarzający wyłącznie na podstawie udokumentowanych poleceń administratora, zgodnie z art. 28 RODO.

- jednoznaczne uregulowanie zasad współpracy w umowie,
- sformalizowany proces zarządzania zleceniami,
- staranny dobór podmiotów przetwarzających,



- obowiązek uprzedniej weryfikacji podmiotu przetwarzającego,