Ustawa o usługach cyfrowych

Raport przejrzystości

dla okresu sprawozdawczego kończącego się w grudniu 2025 r.

Raport opublikowano: 17 lutego 2026 r.

1. Wprowadzenie

Niniejszy raport przejrzystości został sporządzony zgodnie z artykułem 15 Rozporządzenia (UE) 2022/2065, Ustawy o usługach cyfrowych (DSA). Opisuje on nasze praktyki moderowania treści oraz decyzje egzekucyjne dotyczące określonych obszarów produktów i ma na celu dostarczenie jasnych, dostępnych i wyczerpujących informacji na temat sposobu zarządzania i moderowania treści na naszej platformie.

W niniejszym raporcie omówiono w szczególności działania i procedury moderacyjne stosowane w przypadku następujących produktów: platformy internetowe i usługi cyfrowe Awaze Group, które ułatwiają zamieszczanie ofert, wyszukiwanie i rezerwowanie krótkoterminowych miejsc zakwaterowania na wakacje, w tym treści tworzone przez użytkowników, takie jak oferty nieruchomości, opisy, zdjęcia, recenzje i powiązane komunikaty.

Niniejsze sprawozdanie stanowi część naszego stałego zobowiązania do przejrzystości, odpowiedzialności i przestrzegania obowiązków określonych w DSA.

Nazwa dostawcy usług	W niniejszym raporcie uwzględniono następujące podmioty prawne Grupy Awaze: Novasol, Fincallorca, Ardennes Étape i SandyBlue – zbiorowo „Grupa Awaze”
Data publikacji raportu	17 lutego 2026 r.
Data publikacji ostatniego poprzedniego raportu	17 lutego 2025
Data rozpoczęcia okresu sprawozdawczego	1 stycznia 2025 r.
Data końcowa okresu sprawozdawczego	31 grudnia 2025 r.

2. Zamówienia otrzymane od organów państw członkowskich UE

Zgodnie z art. 9 i 10 ustawy DSA, w niniejszym rozdziale zawarto informacje o nakazach otrzymanych od właściwych organów państw członkowskich UE w okresie sprawozdawczym. Nakazy te dotyczą treści niezgodnych z prawem oraz wniosków o udzielenie informacji.

2.1. Nakazy podjęcia działań w związku z treściami niezgodnymi z prawem wydane przez organy państw członkowskich

Rodzaj treści niezgodnych z prawem	Liczba otrzymanych zamówień	Państwo członkowskie wydające nakaz	Średni czas potwierdzenia odbioru	Średni czas realizacji zamówienia
Dobrostan zwierząt	0	Nie dotyczy	Nie dotyczy	Nie dotyczy
Naruszenia informacji konsumenckich	0	Nie dotyczy	Nie dotyczy	Nie dotyczy
Cyberprzemoc	0	Nie dotyczy	Nie dotyczy	Nie dotyczy
Ochrona danych i naruszenia prywatności	0	Nie dotyczy	Nie dotyczy	Nie dotyczy
Nielegalna lub szkodliwa mowa	0	Nie dotyczy	Nie dotyczy	Nie dotyczy
Naruszenia własności intelektualnej	0	Nie dotyczy	Nie dotyczy	Nie dotyczy
Negatywne skutki dla dyskursu obywatelskiego lub wyborów	0	Nie dotyczy	Nie dotyczy	Nie dotyczy
Ochrona nieletnich	0	Nie dotyczy	Nie dotyczy	Nie dotyczy
Ryzyko dla bezpieczeństwa publicznego	0	Nie dotyczy	Nie dotyczy	Nie dotyczy
Oszustwa/nadużycia	0	Nie dotyczy	Nie dotyczy	Nie dotyczy
Samookaleczenie	0	Nie dotyczy	Nie dotyczy	Nie dotyczy
Produkty niebezpieczne, niezgodne z normami lub zakazane	0	Nie dotyczy	Nie dotyczy	Nie dotyczy
Przemoc	0	Nie dotyczy	Nie dotyczy	Nie dotyczy
Rodzaj treści niezgodnych z prawem nie został określony przez organ	0	Nie dotyczy	Nie dotyczy	Nie dotyczy
Wszystkie inne typy	0	Nie dotyczy	Nie dotyczy	Nie dotyczy
Całkowity:	0	Nie dotyczy	Nie dotyczy	Nie dotyczy

2.2 Nakaz dostarczenia przez organy państw członkowskich informacji o odbiorcach usług

Zgłoś powód/rodzaj treści niezgodnych z prawem	Liczba otrzymanych powiadomień	Liczba powiadomień otrzymanych przez zaufanych sygnalistów	Liczba działań podjętych na podstawie zawiadomień	Nie. przetwarzane wyłącznie w sposób zautomatyzowany oznacza	Średni czas potrzebny na podjęcie działania
Dobrostan zwierząt	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Naruszenia informacji konsumenckich	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Ochrona danych i naruszenia prywatności	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Nielegalna lub szkodliwa mowa 0		Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Naruszenia własności intelektualnej	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Negatywne skutki dla dyskursu obywatelskiego lub wyborów	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Ochrona nieletnich	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Ryzyko dla bezpieczeństwa publicznego 0		Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Oszustwa/nadużycia	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Samookaleczenie	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Produkty niebezpieczne, niezgodne z normami lub zakazane	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Przemoc	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Rodzaj treści niezgodnych z prawem nie został określony przez organ	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Wszystkie inne typy	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Całkowity:	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy

3. Raporty/powiadomienia użytkowników

W tej sekcji opisano liczbę i charakter zgłoszeń przesłanych przez użytkowników, inne osoby i podmioty dotyczące treści, które ich zdaniem są nielegalne lub naruszają regulamin naszej platformy. Ponadto opisano w niej sposób, w jaki postępujemy z moderacją treści w odpowiedzi na zgłoszenia użytkowników.

Raporty otrzymane od użytkowników

Zgłoś powód/rodzaj treści niezgodnych z prawem	Liczba otrzymanych powiadomień	Liczba powiadomień otrzymanych przez zaufanych sygnalistów	Liczba działań podjętych na podstawie zawiadomień	Nie. przetwarzane wyłącznie w sposób zautomatyzowany oznacza	Średni czas potrzebny na podjęcie działania
Dobrostan zwierząt	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Naruszenia informacji konsumenckich	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Ochrona danych i naruszenia prywatności	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Nielegalna lub szkodliwa mowa 0		Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Naruszenia własności intelektualnej	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Negatywne skutki dla dyskursu obywatelskiego lub wyborów	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Ochrona nieletnich	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Ryzyko dla bezpieczeństwa publicznego 0		Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Oszustwa/nadużycia	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Samookaleczenie	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Produkty niebezpieczne, niezgodne z normami lub zakazane	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Przemoc	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Rodzaj treści niezgodnych z prawem nie został określony przez organ	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Wszystkie inne typy	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Całkowity:	0	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy

4. Moderacja treści przeprowadzana z własnej inicjatywy przez Awaze

Awaze dokłada wszelkich starań, aby zapewnić bezpieczne i wolne od nadużyć środowisko zarówno dla naszych klientów, jak i użytkowników końcowych. Jako dostawca platformy obsługi klienta, umożliwiamy firmom kontakt z użytkownikami za pośrednictwem wiadomości, e-maili i integracji – wszystkie te rozwiązania niosą ze sobą potencjalne nadużycia, jeśli nie są odpowiednio zabezpieczone.

Stosujemy wielowarstwowe podejście do moderacji treści, łącząc zautomatyzowane systemy wykrywania, wewnętrzne narzędzia administracyjne i ręczne procesy weryfikacji. Ta sekcja zawiera przegląd działań moderacyjnych podejmowanych z własnej inicjatywy, bez żadnych zobowiązań prawnych ani powiadomienia osób trzecich.

Moderacja prowadzona z własnej inicjatywy obejmuje zarówno proaktywne wykrywanie za pomocą systemów automatycznych, jak i ręczną kontrolę przez moderatorów treści. Dokładamy wszelkich starań, aby wszyscy pracownicy zaangażowani w moderację treści posiadali niezbędne umiejętności, wiedzę i zasoby, pozwalające im wykonywać swoje obowiązki uczciwie, dokładnie i zgodnie z obowiązującymi przepisami prawa oraz wewnętrznymi zasadami.

Moderacja treści z własnej inicjatywy

Rodzaj treści niezgodnych z prawem lub innego naruszenia AUP	Liczba moderowanych elementów	Liczba przedmiotów wykrytych wyłącznie za pomocą automatyzacji oznacza	Rodzaj zastosowanego ograniczenia
Oszustwa/nadużycia	Przefiltrowano wiadomości e-mail przychodzące: 2 691 775 (w ujęciu rocznym; w tym 52 046 wykrytych podszywania się) Znaleziono złośliwe linki: wykryto 1135 niebezpiecznych kliknięć adresów URL (e-mail) + zablokowano 98 262 zdarzeń ochrony DNS (sieć, w tym 7165 phishing) Znaleziono złośliwe pliki do przesłania: 1010 wykrytych złośliwych wiadomości przychodzących (e-mail)	Odfiltrowano wiadomości przychodzące: 2 691 775 Znaleziono złośliwe linki: 1135 (e-mail) + 98262 (sieć) Znaleziono złośliwe pliki: 1010	Ograniczenie widoczności: Wiadomości e-mail są poddawane kwarantannie/ Zablokowane; żądania sieciowe są blokowane przez filtrowanie DNS/zasady zapory sieciowej. Usuwanie treści: Wiadomości przychodzące mogą zostać odrzucone (niedostarczone), jeśli kwalifikują się jako spam/ Kontrola złośliwego oprogramowania/ podszywania się. Zawieszenie konta: Nieobsługiwane przez te kontrole (obsługiwane w ramach oddzielnych procesów HR/IT, jeśli jest to wymagane).
Inne rodzaje naruszeń regulaminu platformy	Łączna liczba skarg na spam: 96 665 (Odrzucanie spamu – bezpieczna bramka poczty e-mail; szacunkowa wartość stacjonarna w ujęciu rocznym)	Zautomatyzowane skargi na spam: 96 665 (automatyczne wykrywanie spamu na bezpiecznej bramce pocztowej)	Zawieszenie uprawnień platformy: Nie dotyczy. Dotyczy to odrzuceń bramy pocztowej, a nie działań egzekucyjnych platformy.
Całkowity:	191 072	197 072	Nie dotyczy

4. Opis jakościowy środków zautomatyzowanych

Awaze wykorzystuje zautomatyzowane mechanizmy kontroli bezpieczeństwa w celu ograniczenia oszustw, phishingu, podszywania się pod inne osoby i rozprzestrzeniania złośliwego oprogramowania w poczcie elektronicznej i dostępie do Internetu.

Zabezpieczenia poczty elektronicznej: Używamy bezpiecznej bramki pocztowej (Mimecast) do sprawdzania poczty przychodzącej przed jej dostarczeniem. Bramka korzysta z automatycznych kontroli (reputacji, uwierzytelniania, Analiza treści, skanowanie złośliwego oprogramowania i wykrywanie podszywania się) w celu odrzucania lub poddawania kwarantannie wiadomości związanych z oszustwami, podszywaniem się lub złośliwym oprogramowaniem. Stosujemy również mechanizmy uwierzytelniania wiadomości e-mail we wszystkich naszych domenach (SPF, DKIM i DMARC). Mechanizmy te pomagają systemom odbiorczym weryfikować, czy wiadomości podszywające się pod domeny Awaze są autoryzowane i nie zostały zmienione, a także ograniczają próby podszywania się pod domenę i podszywania się.

Zabezpieczenia sieciowe: Korzystamy z zarządzanej usługi bezpieczeństwa SD-WAN (Cato), która stosuje filtrowanie DNS, politykę zapory sieciowej i zapobieganie włamaniom. Blokuje ona dostęp do znanych złośliwych domen, infrastruktury phishingowej i miejsc docelowych typu command-and-control, a także blokuje wzorce ruchu wysokiego ryzyka na brzegu sieci.

Uwaga dotycząca sprawozdawczości: Roczne liczby oszacowano na podstawie okien sprawozdawczych dostawców (Mimecast sierpień–grudzień 2025 r.; Cato 12 października–31 grudnia 2025 r.) i przyjęto założenie o stałym stanie bez zmian polityki lub wolumenu.

Dokładne cele

Zautomatyzowane narzędzia mają na celu ochronę ruchu przychodzącego i wychodzącego, zapobieganie nadużyciom, dbanie o reputację nadawcy oraz zapewnienie zgodności z wytycznymi i przepisami (np. wytycznymi dotyczącymi wysyłania wiadomości e-mail, zgodnością z ustawą CAN-SPAM). Konkretne cele obejmują:

- Wykrywanie podejrzanych działań i wzorców podczas rejestracji;
- Ocenianie treści w momencie ich tworzenia i dostępu do nich za pośrednictwem łączy, przesłanych treści i innych treści generowanych przez użytkowników;
- Monitorowanie limitów szybkości i progów wykorzystania kluczowych funkcji;
- Ocena ryzyka na podstawie danych historycznych;
- Zapobiegaj dostarczaniu wiadomości e-mail zawierających phishing, podszywanie się pod inne osoby i złośliwe oprogramowanie, odrzucając je lub poddając kwarantannie wiadomości przychodzące, które odpowiadają automatycznym kontrolom zagrożeń;
- Zapobiegaj dostępowi do złośliwych stron internetowych, blokując rozpoznawanie nazw domen i/lub ruch sieciowy. domeny i kategorie związane ze złośliwym oprogramowaniem, phishingiem, DGA i kontrolą; oraz
- Wykrywanie i blokowanie ataków sieciowych (na przykład prób siłowych, blokad opartych na reputacji, skanowania podatności i wzorców wykorzystania luk) przy użyciu sygnatur IPS i zasad zapory sieciowej.

Użycie uwierzytelniania poczty e-mail SPF/DKIM/DMARC w celu ograniczenia podszywania się pod domeny Awaze oraz poprawy wykrywania i odrzucania wiadomości e-mail podszywających się pod inne osoby i prób phishingu.

Wskaźniki dokładności i możliwego współczynnika błędu

Zaufanie do naszych narzędzi jest duże, a wskaźnik fałszywych trafień jest niski. Klienci mogą jednak odwołać się do naszego zespołu wsparcia, jeśli uważają, że wystąpił fałszywy alarm w naszych procesach moderacji treści lub narzędziach zapobiegających nadużyciom.

E-mail: Wykrycia są oparte na automatycznych analizach zagrożeń, sprawdzaniu uwierzytelniania, analizie treści i skanowaniu w poszukiwaniu złośliwego oprogramowania. Mogą wystąpić fałszywe alarmy (na przykład w przypadku legalnych nadawców masowych lub nowo zarejestrowanych domen), a ich ryzyko jest minimalizowane poprzez dodawanie wiadomości do listy dozwolonych, dostosowywanie zasad i weryfikację wiadomości poddanych kwarantannie/odrzuconych.

Web/DNS: Blokady DNS i zapory sieciowej opierają się na źródłach zagrożeń, kategoryzacji, wskaźnikach behawioralnych (na przykład wykrywaniu DGA) oraz sygnaturach IPS. Mogą wystąpić fałszywe alarmy (na przykład błędnie skategoryzowane domeny lub współdzielona infrastruktura), a zarządzanie nimi odbywa się za pomocą wyjątków/list dozwolonych oraz okresowego dostrajania reguł.

Awaze analizuje trendy i w razie potrzeby dostosowuje zasady, aby ograniczyć liczbę fałszywych alarmów, jednocześnie zapewniając ochronę.

- Przestrzenie robocze muszą przejść ocenę antynadużyciową, zanim będzie można korzystać z wielu funkcji, zwłaszcza te, które umożliwiają komunikację wychodzącą.
- W wielu kanałach obowiązują ograniczenia przepustowości, skanowanie treści i wykrywanie wzorców spamu. nasz produkt
- Jeśli treść nie narusza naszych warunków, ale klient chce zarządzać swoją przestrzenią roboczą zgodnie z własnymi warunkami, może usunąć treść lub zablokować użytkowników według własnego uznania.
- W przypadku blokad automatycznych możliwe jest ręczne nadpisanie ustawień przez Dział Obsługi Klienta (CS).
- Pracownicy Awaze (np. Dział Obsługi Klienta) dysponują narzędziami umożliwiającymi zatwierdzanie lub odrzucanie przywrócenia zablokowanych kont próby wysłania wiadomości e-mail.
- Stosujemy kontrolę warstwową (bramka poczty e-mail + filtrowanie DNS + zapora sieciowa + IPS), dzięki czemu nie ma potrzeby stosowania pojedynczej kontroli. wyłącznie na nim polegać.
- Używamy listy dozwolonych/wyjątków (w uzasadnionych przypadkach) i dostosowujemy zasady na podstawie danych operacyjnych wpływ i ryzyko bezpieczeństwa.
- Prowadzimy dzienniki audytów i raporty dotyczące zdarzeń związanych z bezpieczeństwem, aby wspierać dochodzenia i reagowanie na incydenty.
- Zasady bezpieczeństwa i możliwości wykrywania są utrzymywane za pomocą aktualizacji dostawców i wewnętrznych recenzja

Jako dodatkowe zabezpieczenie ograniczające podszywanie się i zwiększające niezawodność zautomatyzowanych decyzji dotyczących filtrowania wiadomości e-mail stosujemy uwierzytelnianie poczty e-mail na poziomie domeny (SPF, DKIM i DMARC).

6. Otrzymane skargi

Liczba skarg, które otrzymaliśmy za pośrednictwem naszych wewnętrznych systemów obsługi skarg

Wewnętrzny mechanizm składania skarg

Liczba złożonych skarg	0
Podstawa skargi	Nie dotyczy
Decyzje podjęte po złożeniu skargi	Nie dotyczy
Średni czas rozpatrzenia skargi	Nie dotyczy