LEGGE SUI SERVIZI DIGITALI

Rapporto sulla trasparenza

per il periodo di riferimento che termina a dicembre 2025

Rapporto pubblicato: 17 febbraio 2026

1. Introduzione

Il presente rapporto sulla trasparenza è stato redatto in conformità all'articolo 15 del Regolamento (UE) 2022/2065, il Digital Services Act (DSA). Descrive le nostre pratiche di moderazione dei contenuti e le decisioni di applicazione relative a specifiche aree di prodotto e mira a fornire informazioni chiare, accessibili e complete su come gestiamo e moderiamo i contenuti sulla nostra piattaforma.

Il presente rapporto riguarda in particolare le azioni e le procedure di moderazione applicate ai seguenti prodotti: le piattaforme online e i servizi digitali di Awaze Group che facilitano l'inserimento, la scoperta e la prenotazione di alloggi per vacanze di breve durata, inclusi contenuti generati dagli utenti quali annunci di proprietà, descrizioni, immagini, recensioni e comunicazioni correlate.

Il presente rapporto rientra nel nostro impegno costante verso la trasparenza, la responsabilità e il rispetto degli obblighi stabiliti dal DSA.

Nome del fornitore del servizio	Il presente rapporto riguarda le seguenti entità legali del Gruppo Awaze: Novasol, Fincallorca, Ardennes Étape e SandyBlue - Collettivamente il "Gruppo Awaze"
Data di pubblicazione del rapporto	**17 febbraio 2026**
Data di pubblicazione dell'ultimo rapporto precedente	**17 febbraio 2025**
Data di inizio del periodo di riferimento	**1 gennaio 2025**
Data di fine del periodo di riferimento	**31 dicembre 2025**

2. Ordini ricevuti dalle autorità degli Stati membri dell'UE

Ai sensi degli articoli 9 e 10 del DSA, la presente sezione fornisce informazioni sugli ordini ricevuti dalle autorità competenti degli Stati membri dell'UE durante il periodo di riferimento. Tali ordini riguardano contenuti illeciti e richieste di informazioni.

2.1. Ordini di azione contro i contenuti illegali da parte delle autorità degli Stati membri

Tipo di contenuto illegale	Numero di ordini ricevuti	Stato membro che emette l'ordine	Tempo medio per confermare la ricezione	Tempo mediano per dare effetto all'ordine
Benessere degli animali	0	N / A	N / A	N / A
Violazioni delle informazioni dei consumatori	0	N / A	N / A	N / A
violenza informatica	0	N / A	N / A	N / A
Violazioni della protezione dei dati e della privacy	0	N / A	N / A	N / A
Discorso illegale o dannoso	0	N / A	N / A	N / A
Violazioni della proprietà intellettuale	0	N / A	N / A	N / A
Effetti negativi sul discorso civico o sulle elezioni	0	N / A	N / A	N / A
Tutela dei minori	0	N / A	N / A	N / A
Rischio per la sicurezza pubblica	0	N / A	N / A	N / A
Truffe/frodi	0	N / A	N / A	N / A
Autolesionismo	0	N / A	N / A	N / A
Prodotti non sicuri, non conformi o proibiti	0	N / A	N / A	N / A
Violenza	0	N / A	N / A	N / A
Tipo di contenuto illegale non specificato dall'autorità	0	N / A	N / A	N / A
Tutti gli altri tipi	0	N / A	N / A	N / A
Totale:	0	N / A	N / A	N / A

2.2 Ordine di fornire informazioni sui destinatari del servizio da parte delle autorità degli Stati membri

Segnala motivo/tipo di contenuto illegale	Numero di notifiche ricevute	Numero di notifiche ricevute da segnalatori attendibili	Numero di azioni intraprese a seguito di notifiche	No. trattati esclusivamente con mezzi automatizzati significa	Tempo medio per agire
Benessere degli animali	0	N / A	N / A	N / A	N / A
Violazioni delle informazioni dei consumatori	0	N / A	N / A	N / A	N / A
Violazioni della protezione dei dati e della privacy	0	N / A	N / A	N / A	N / A
Discorso illegale o dannoso 0		N / A	N / A	N / A	N / A
Violazioni della proprietà intellettuale	0	N / A	N / A	N / A	N / A
Effetti negativi sul discorso civico o sulle elezioni	0	N / A	N / A	N / A	N / A
Tutela dei minori	0	N / A	N / A	N / A	N / A
Rischio per la sicurezza pubblica 0		N / A	N / A	N / A	N / A
Truffe/frodi	0	N / A	N / A	N / A	N / A
Autolesionismo	0	N / A	N / A	N / A	N / A
Prodotti non sicuri, non conformi o proibiti	0	N / A	N / A	N / A	N / A
Violenza	0	N / A	N / A	N / A	N / A
Tipo di contenuto illegale non specificato dall'autorità	0	N / A	N / A	N / A	N / A
Tutti gli altri tipi	0	N / A	N / A	N / A	N / A
Totale:	0	N / A	N / A	N / A	N / A

3. Segnalazioni/avvisi degli utenti

Questa sezione descrive il numero e la natura delle segnalazioni inviate da utenti, altri individui ed entità in merito a contenuti che ritengono illegali o in violazione dei termini e delle condizioni della nostra piattaforma. Inoltre, descrive come gestiamo le azioni di moderazione dei contenuti in risposta alle segnalazioni degli utenti.

Segnalazioni ricevute dagli utenti

Segnala motivo/tipo di contenuto illegale	Numero di notifiche ricevute	Numero di notifiche ricevute da segnalatori attendibili	Numero di azioni intraprese a seguito di notifiche	No. trattati esclusivamente con mezzi automatizzati	Tempo medio per agire significa
Benessere degli animali	0	N / A	N / A	N / A	N / A
Violazioni delle informazioni dei consumatori	0	N / A	N / A	N / A	N / A
Violazioni della protezione dei dati e della privacy	0	N / A	N / A	N / A	N / A
Discorso illegale o dannoso	0	N / A	N / A	N / A	N / A
Violazioni della proprietà intellettuale	0	N / A	N / A	N / A	N / A
Effetti negativi sul discorso civico o sulle elezioni	0	N / A	N / A	N / A	N / A
Tutela dei minori	0	N / A	N / A	N / A	N / A
Rischio per la sicurezza pubblica	0	N / A	N / A	N / A	N / A
Truffe/frodi	0	N / A	N / A	N / A	N / A
Autolesionismo	0	N / A	N / A	N / A	N / A
Prodotti non sicuri, non conformi o proibiti	0	N / A	N / A	N / A	N / A
Violenza	0	N / A	N / A	N / A	N / A
Tipo di contenuto illegale non specificato dall'autorità	0	N / A	N / A	N / A	N / A
Tutti gli altri tipi	0	N / A	N / A	N / A	N / A
Totale:	0	N / A	N / A	N / A	N / A

4. Moderazione dei contenuti effettuata su iniziativa di Awa

Awaze si impegna a mantenere un ambiente sicuro, protetto e privo di abusi, sia per i nostri clienti che per i loro utenti finali. In qualità di fornitore di una piattaforma di assistenza clienti, la nostra piattaforma consente alle aziende di interagire con gli utenti tramite messaggistica, e-mail e integrazioni, tutti strumenti potenzialmente pericolosi se non adeguatamente protetti.

Utilizziamo un approccio a più livelli alla moderazione dei contenuti, combinando sistemi di rilevamento automatizzati, strumenti di amministrazione interna e processi di revisione manuale. Questa sezione fornisce una panoramica delle azioni di moderazione dei contenuti intraprese di nostra iniziativa, senza alcun obbligo legale o notifica da parte di terzi.

La moderazione effettuata su nostra iniziativa include sia rilevamenti proattivi tramite sistemi automatizzati sia la revisione manuale da parte dei moderatori dei contenuti. Ci impegniamo a garantire che tutto il personale coinvolto nella moderazione dei contenuti sia dotato delle competenze, delle conoscenze e delle risorse necessarie per svolgere le proprie responsabilità in modo equo, accurato e in linea con le leggi applicabili e le policy interne.

Moderazione dei contenuti su iniziativa propria

Tipo di contenuto illegale o altra violazione dell'AUP	Numero di elementi moderati	Numero di quegli elementi rilevati utilizzando esclusivamente l'automazione significa	Tipo di restrizione applicata
Truffe/frodi	Email in entrata filtrate: 2.691.775 (annualizzato; include 52.046 rilevamenti di impersonificazione) Link dannosi rilevati: 1.135 clic su URL non sicuri rilevati (e-mail) + 98.262 eventi di protezione DNS bloccati (web, incl. 7.165 phishing) Caricamenti dannosi rilevati: 1.010 rilevamenti di malware in entrata (e-mail)	Email in entrata filtrate: 2.691.775 Link dannosi trovati: 1.135 (e-mail) + 98.262 (web) Caricamenti dannosi trovati: 1.010	Limitazione della visibilità: le e-mail vengono messe in quarantena/ bloccato; le richieste web sono bloccate dal filtro DNS/criterio firewall. Rimozione dei contenuti: le email in entrata possono essere rifiutate (non recapitate) quando corrispondono a spam/ Controlli anti-malware/ impersonificazione. Sospensione dell'account: non utilizzata da questi controlli (gestita tramite processi HR/IT separati, ove necessario).
Altri tipi di violazioni dei termini e delle condizioni della piattaforma	Totale reclami per spam: 96.665 (Rifiuto spam – gateway di posta elettronica sicuro; stima annualizzata dello stato stazionario)	Segnalazioni automatiche di spam: 96.665 (rilevamento automatico dello spam sul gateway di posta elettronica sicuro)	Sospendi autorizzazioni piattaforma: non applicabile. Si tratta di rifiuti del gateway di posta elettronica, non di azioni di imposizione della piattaforma.
Totale:	191.072	197.072	N / A

4. Descrizione qualitativa dei mezzi automatizzati

Awaze utilizza controlli di sicurezza automatizzati per ridurre truffe, phishing, impersonificazione e malware nell'accesso tramite e-mail e web.

Protezioni e-mail: utilizziamo un gateway e-mail sicuro (Mimecast) per ispezionare la posta in arrivo prima che venga recapitata. Il gateway utilizza controlli automatizzati (reputazione, autenticazione, Analisi dei contenuti, scansione malware e rilevamento di impersonificazione) per rifiutare o mettere in quarantena i messaggi associati a truffe/frodi, impersonificazione o malware. Utilizziamo inoltre controlli di autenticazione email su tutti i nostri domini (SPF, DKIM e DMARC). Questi controlli aiutano i sistemi di ricezione a verificare che i messaggi che dichiarano di provenire da domini Awaze siano autorizzati e non siano stati alterati, riducendo al contempo i tentativi di spoofing e impersonificazione del dominio.

Protezioni web: utilizziamo un servizio di sicurezza SD-WAN gestito (Cato) che applica filtri DNS, policy firewall e prevenzione delle intrusioni. Questo blocca l'accesso a domini dannosi noti, infrastrutture di phishing e destinazioni di comando e controllo, e blocca modelli di traffico ad alto rischio ai margini della rete.

Nota di reporting: le cifre annuali sono stimate utilizzando le finestre di reporting dei fornitori (Mimecast agosto-dicembre 2025; Cato 12 ottobre-31 dicembre 2025) e presuppongono uno stato stabile senza modifiche di politica o volume.

Scopi precisi

Gli strumenti automatizzati mirano a proteggere l'attività di messaggistica in entrata e in uscita, prevenire abusi, preservare la reputazione del mittente e garantire la conformità alle linee guida e alla legislazione (ad esempio, linee guida per l'invio di e-mail, conformità CAN-SPAM). Gli scopi specifici includono:

- **Rilevamento di attività e modelli sospetti durante la registrazione;**
- **Valutazione del contenuto in fase di creazione e accesso tramite link, caricamenti e altri contenuti generati dagli utenti;**
- **Monitoraggio dei limiti di velocità e delle soglie di utilizzo per le funzionalità chiave;**
- **Valutazione del rischio basata sui dati storici;**
- **Impedisci la distribuzione di phishing, impersonificazione e malware tramite e-mail rifiutando o mettendo in quarantena messaggi in entrata che corrispondono ai controlli automatizzati delle minacce;**
- **Impedisci l'accesso a destinazioni web dannose bloccando la risoluzione DNS e/o il traffico web per domini e categorie associati a malware, phishing, DGA e comando e controllo; e**
- **Rilevare e bloccare gli attacchi basati sulla rete (ad esempio tentativi di forza bruta, blocchi basati sulla reputazione, scansione delle vulnerabilità e modelli di exploit) utilizzando firme IPS e policy firewall.**

Utilizzo dell'autenticazione e-mail SPF/DKIM/DMARC per ridurre lo spoofing dei domini Awaze e migliorare il rilevamento e il rifiuto di e-mail di impersonificazione e phishing.

Indicatori di accuratezza e possibile tasso di errore

La fiducia nei nostri strumenti è elevata, con un basso tasso di falsi positivi. Tuttavia, i clienti possono presentare ricorso al nostro team di supporto se ritengono che si sia verificato un falso positivo nei nostri processi di moderazione dei contenuti o nei nostri strumenti anti-abuso.

Email: i rilevamenti sono basati su intelligence automatizzata sulle minacce, controlli di autenticazione, analisi dei contenuti e scansione antimalware. Possono verificarsi falsi positivi (ad esempio, mittenti legittimi di massa o domini di nuova registrazione) e vengono mitigati tramite l'inserimento in liste consentite, l'ottimizzazione delle policy e la revisione dei messaggi in quarantena/rifiutati.

Web/DNS: i blocchi DNS e firewall si basano su feed di minacce, categorizzazione, indicatori comportamentali (ad esempio, rilevamento DGA) e firme IPS. Possono verificarsi falsi positivi (ad esempio, domini non categorizzati correttamente o infrastrutture condivise) e vengono gestiti tramite eccezioni/liste consentite e ottimizzazione periodica delle regole.

Awaze esamina le tendenze e, quando necessario, adegua le policy per ridurre i falsi positivi mantenendo al contempo la protezione.

- **Gli spazi di lavoro devono superare una valutazione anti-abuso prima di poter usufruire di numerose funzionalità, in particolare quelli che consentono la comunicazione in uscita.**
- **La limitazione della velocità, la scansione dei contenuti e il rilevamento dei modelli di spam sono in atto su molti canali di il nostro prodotto**
- **Se il contenuto non viola i nostri termini ma un cliente desidera amministrare il proprio spazio di lavoro secondo i propri termini, può rimuovere il contenuto o bloccare gli utenti come ritiene opportuno.**
- **Per i blocchi automatizzati sono disponibili sostituzioni manuali da parte del Supporto Clienti (CS).**
- **I dipendenti di Awaze (ad esempio l'assistenza clienti) dispongono di strumenti per approvare o negare il ripristino per gli utenti bloccati tentativi di invio di e-mail.**
- **Applichiamo controlli a strati (gateway di posta elettronica + filtro DNS + firewall + IPS) in modo che non sia necessario un singolo controllo su cui fare affidamento esclusivamente.**
- **Utilizziamo elenchi consentiti/eccezioni (ove giustificato) e adattiamo le policy in base alle esigenze operative impatto e rischio per la sicurezza.**
- **Conserviamo registri di controllo e report sugli eventi di sicurezza per supportare le indagini e la risposta agli incidenti.**
- **Le policy di sicurezza e le capacità di rilevamento vengono mantenute tramite aggiornamenti dei fornitori e controlli interni revisione**

Applichiamo l'autenticazione e-mail a livello di dominio (SPF, DKIM e DMARC) come ulteriore misura di sicurezza per ridurre lo spoofing e migliorare l'affidabilità delle decisioni di filtraggio automatico delle e-mail.

6. Reclami ricevuti

Numero di reclami ricevuti tramite i nostri sistemi interni di gestione dei reclami

Meccanismo di reclamo interno

Numero di reclami presentati	**0**
Base del reclamo	**N / A**
Decisioni prese a seguito di un reclamo	**N / A**
Tempo medio per rispondere al reclamo	**N / A**