awaze

DIGITAL SERVICES ACT

Transparency Report

for Reporting Period ending December 2025
Report Published: 17 February 2026

1. Introduction

This transparency report has been prepared in accordance with Article 15 of Regulation (EU) 2022/2065, the Digital Services Act (DSA). It outlines our content moderation practices and enforcement decisions relating to specific product areas and aims to provide clear, accessible, and comprehensive information on how we manage and moderate content on our platform.

This report specifically covers moderation actions and procedures applied to the following products: Awaze Group's online platforms and digital services that facilitate the listing, discovery, and booking of short-term holiday accommodation, including user-generated content such as property listings, descriptions, images, reviews, and related communications.

This report is part of our ongoing commitment to transparency, accountability, and compliance with the obligations set forth in the DSA.

Name of service provider	This report covers the following Awaze Group legal entities: Novasol, Fincallorca, Ardennes Étape and SandyBlue - Collectively the "Awaze Group"
Date of publication of the report	17 February 2026
Date of publication of the latest previous report	17 February 2025
Starting date of reporting period	1 January 2025
Ending date of reporting period	31 December 2025

2. Orders received from EU Member State authorities

In accordance with Articles 9 and 10 of the DSA, this section provides information on orders received from competent authorities of EU Member States during the reporting period. These orders relate to illegal content and requests for information.

2.1. Orders to action illegal content from Member State authorities

Type of illegal content	No. of orders received	Member State issuing order	Median time to confirm receipt	Median time to give effect to the order
Animal Welfare	0	N/A	N/A	N/A
Consumer information infringements	0	N/A	N/A	N/A
Cyber violence	0	N/A	N/A	N/A
Data protection and privacy violations	0	N/A	N/A	N/A
Illegal or harmful speech	0	N/A	N/A	N/A
Intellectual property infringements	0	N/A	N/A	N/A
Negative effects on civic discourse or elections	0	N/A	N/A	N/A
Protection of minors	0	N/A	N/A	N/A
Risk for public security	0	N/A	N/A	N/A
Scams/fraud	0	N/A	N/A	N/A
Self-harm	0	N/A	N/A	N/A
Unsafe, non-compliant or prohibited products	0	N/A	N/A	N/A
Violence	0	N/A	N/A	N/A
Type of illegal content not specified by the authority	0	N/A	N/A	N/A
All other types	0	N/A	N/A	N/A
Total:	0	N/A	N/A	N/A

2.2 Order to provide information on recipients of the service from Member State authorities

Report reason/Type of illegal content	No. of notices received	No. of notices received by trusted flaggers	No. of actions taken on foot of notices	No. processed solely by automated means	Median time to take action
Animal Welfare	0	N/A	N/A	N/A	N/A
Consumer information infringements	0	N/A	N/A	N/A	N/A
Data protection and privacy violations	0	N/A	N/A	N/A	N/A
Illegal or harmful speech	0	N/A	N/A	N/A	N/A
Intellectual property infringements	0	N/A	N/A	N/A	N/A
Negative effects on civic discourse or elections	0	N/A	N/A	N/A	N/A
Protection of minors	0	N/A	N/A	N/A	N/A
Risk for public security	0	N/A	N/A	N/A	N/A
Scams/fraud	0	N/A	N/A	N/A	N/A
Self-harm	0	N/A	N/A	N/A	N/A
Unsafe, non-compliant or prohibited products	0	N/A	N/A	N/A	N/A
Violence	0	N/A	N/A	N/A	N/A
Type of illegal content not specified by the authority	0	N/A	N/A	N/A	N/A
All other types	0	N/A	N/A	N/A	N/A
Total:	0	N/A	N/A	N/A	N/A

3. User reports/notices

This section outlines the number and nature of reports submitted by users, other individuals and entities regarding the content they believe to be illegal or in breach of our platform's terms and conditions. Additionally, it outlines how we handle content moderation actions in response to user reports.

Reports received from users

Report reason/Type of illegal content	No. of notices received	No. of notices received by trusted flaggers	No. of actions taken on foot of notices	No. processed solely by automated means	Median time to take action
Animal Welfare	0	N/A	N/A	N/A	N/A
Consumer information infringements	0	N/A	N/A	N/A	N/A
Data protection and privacy violations	0	N/A	N/A	N/A	N/A
Illegal or harmful speech	0	N/A	N/A	N/A	N/A
Intellectual property infringements	0	N/A	N/A	N/A	N/A
Negative effects on civic discourse or elections	0	N/A	N/A	N/A	N/A
Protection of minors	0	N/A	N/A	N/A	N/A
Risk for public security	0	N/A	N/A	N/A	N/A
Scams/fraud	0	N/A	N/A	N/A	N/A
Self-harm	0	N/A	N/A	N/A	N/A
Unsafe, non-compliant or prohibited products	0	N/A	N/A	N/A	N/A
Violence	0	N/A	N/A	N/A	N/A
Type of illegal content not specified by the authority	0	N/A	N/A	N/A	N/A
All other types	0	N/A	N/A	N/A	N/A
Total:	0	N/A	N/A	N/A	N/A

4. Content moderation engaged in at Awaze's own initiative

Awaze is committed to maintaining a safe, secure, and abuse-free environment for both our customers and their end users. As a provider of customer service platform, our platform enables businesses to engage users via messaging, email, and integrations – all of which carry potential for abuse if not properly safeguarded.

We use a layered approach to content moderation, combining automated detection systems, internal admin tooling, and manual review processes. This section provides an overview of content moderation actions undertaken on our own initiative, without the prompt of any legal obligation or third-party notice.

Moderation carried out on our own initiative includes both proactive detections using automated systems and manual review by content moderators. We are committed to ensuring that all staff involved in content moderation are equipped with the necessary skills, knowledge, and resources to carry out their responsibilities fairly, accurately, and in line with applicable laws and internal policies.

Own-initiative content moderation

Type of illegal content or other violation of the AUP	No. of items moderated	No. of those items detected using solely automated means	Type of restriction applied
Scams/fraud	Inbound emails filtered: 2,691,775 (annualised; includes 52,046 impersonation detections) Malicious links found: 1,135 unsafe URL clicks detected (email) + 98,262 DNS protection events blocked (web, incl. 7,165 phishing) Malicious uploads found: 1,010 inbound malware detections (email)	Inbound emails filtered: 2,691,775 Malicious links found: 1,135 (email) + 98,262 (web) Malicious uploads found: 1,010	Visibility restriction: E-mails are quarantined/ blocked; web requests are blocked by DNS filtering / firewall policy. Content removal: Inbound emails can be rejected (not delivered) when they match spam/ malware/impersonation controls. Account suspension: Not used by these controls (handled via separate HR/IT processes where required).
Other type of violations of the platform's terms and conditions	Total spam complaints: 96,665 (Spam Rejection – secure email gateway; annualised steady-state estimate)	Automated spam complaints: 96,665 (automated spam detection at the secure email gateway)	Suspend platform permissions: Not applicable. These are email gateway rejections, not platform enforcement actions.
Total:	191,072	197,072	N/A

4. Qualitative description of the automated means

Awaze uses automated security controls to reduce scams, phishing, impersonation and malware across email and web access.

Email protections: We use a secure email gateway (Mimecast) to inspect inbound email before it is delivered. The gateway uses automated checks (reputation, authentication, content analysis, malware scanning, and impersonation detection) to reject or quarantine messages associated with scams/fraud, impersonation or malware. We also use email authentication controls across our domains (SPF, DKIM and DMARC). These controls help receiving systems verify that messages claiming to come from Awaze domains are authorised and have not been altered, and they reduce domain spoofing and impersonation attempts.

Web protections: We use a managed SD-WAN security service (Cato) that applies DNS filtering, firewall policy and intrusion prevention. This blocks access to known malicious domains, phishing infrastructure, and command-and-control destinations, and it blocks high-risk traffic patterns at the network edge.

Reporting note: Annual figures are estimated using vendor reporting windows (Mimecast Aug–Dec 2025; Cato 12 Oct–31 Dec 2025) and assume steady state with no policy or volume change.

Precise purposes

The automated tools aim to protect inbound and outbound messaging activity, prevent abuse, maintain sender reputation, and ensure compliance with guidelines and legislation (e.g. email sending guidelines, CAN-SPAM compliance). Specific purposes include:

- **Detecting suspicious activity and patterns during signup;**
- **Evaluating content at creation and access across links, uploads and other user generated content;**
- **Monitoring rate limits and usage thresholds for key features;**
- **Scoring risk based on historical data;**
- **Prevent delivery of phishing, impersonation and malware via email by rejecting or quarantining inbound messages that match automated threat controls;**
- **Prevent access to malicious web destinations by blocking DNS resolution and/or web traffic for domains and categories associated with malware, phishing, DGAs and command-and-control; and**
- **Detect and block network-based attacks (for example brute force attempts, reputation-based blocks, vulnerability scanning and exploit patterns) using IPS signatures and firewall policy.**

Use of SPF/DKIM/DMARC email authentication to reduce spoofing of Awaze domains and improve detection and rejection of impersonation and phishing emails.

Indicators of accuracy and possible rate of error

Confidence in our tooling is strong, with a low false positive rate. However, customers can appeal with our support team if they believe there has been a false positive in our content moderation processes or anti-abuse tooling.

Email: Detections are driven by automated threat intelligence, authentication checks, content analysis and malware scanning. False positives can occur (for example, legitimate bulk senders or newly registered domains) and are mitigated through allowlisting, policy tuning and review of quarantined/rejected messages.

Web/DNS: DNS and firewall blocks rely on threat feeds, categorisation, behavioural indicators (for example DGA detection) and IPS signatures. False positives can occur (for example miscategorised domains or shared infrastructure) and are managed via exceptions/allowlists and periodic rule tuning.

Awaze reviews trends and adjusts policies when needed to reduce false positives while maintaining protection.

- **Workspaces must pass an anti-abuse assessment before they can avail of many features, especially those which allow outbound communication.**
- **Rate limiting, content scanning and spam pattern detection are in place across many channels of our product**
- **If content is not against our terms but a customer wishes to administrate their workspace according to their own terms, they can remove content or block users as they see fit.**
- **Manual overrides by Customer Support (CS) are available for automated blocks.**
- **Awaze employees (e.g. Customer Support) have tools to approve or deny reinstatement for blocked email attempts.**
- **We apply layered controls (email gateway + DNS filtering + firewall + IPS) so no single control is solely relied upon.**
- **We use allowlisting/exceptions (where justified), and we tune policies based on operational impact and security risk.**
- **We keep audit logs and security event reporting to support investigation and incident response.**
- **Security policies and detection capabilities are maintained through vendor updates and internal review**

We apply domain-level email authentication (SPF, DKIM and DMARC) as an additional safeguard to reduce spoofing and improve the reliability of automated email filtering decisions.

6. Complaints received

Number of complaints we received through our internal complaint-handling systems

Internal complaints mechanism

No. of complaints submitted	0
Basis of complaint	N/A
Decisions taken following a complaint	N/A
Median time to address complaint	N/A