LOI SUR LES SERVICES NUMÉRIQUES

Rapport de transparence

pour la période de référence se terminant en décembre 2025

Rapport publié le 17 février 2026

1. Introduction

Ce rapport de transparence a été établi conformément à l'article 15 du règlement (UE) 2022/2065, dit « loi sur les services numériques » (DSA). Il décrit nos pratiques de modération des contenus et les décisions d'application relatives à des domaines de produits spécifiques et vise à fournir des informations claires, accessibles et complètes sur la manière dont nous gérons et modérons les contenus sur notre plateforme.

Ce rapport porte spécifiquement sur les actions et procédures de modération appliquées aux produits suivants : les plateformes en ligne et les services numériques du groupe Awaze qui facilitent la mise en ligne, la découverte et la réservation d'hébergements de vacances de courte durée, y compris le contenu généré par les utilisateurs tel que les annonces immobilières, les descriptions, les images, les avis et les communications connexes.

Ce rapport s'inscrit dans le cadre de notre engagement continu en matière de transparence, de responsabilité et de respect des obligations énoncées dans le DSA.

Nom du prestataire de services	Ce rapport couvre les entités juridiques suivantes du groupe Awaze : Novasol, Fincallorca, Ardennes Étape et SandyBlue - Collectivement le « Groupe Awaze »
Date de publication du rapport	17 février 2026
Date de publication du dernier rapport précédent	17 février 2025
Date de début de la période de déclaration	1er janvier 2025
Date de fin de la période de reporting	31 décembre 2025

2. Commandes reçues des autorités des États membres de l'UE

Conformément aux articles 9 et 10 du règlement (UE) 2017/799 (RGPD), cette section présente des informations sur les injonctions reçues des autorités compétentes des États membres de l'UE au cours de la période considérée. Ces injonctions concernent des contenus illicites et des demandes de renseignements.

2.1. Ordres des autorités des États membres visant à lutter contre les contenus illégaux

Type de contenu illégal	Nombre de commandes reçues	État membre émettant l'ordre	Délai médian de confirmation de réception	Délai médian d'exécution de la commande
Bien-être animal	0	N / A	N / A	N / A
atteintes aux droits des consommateurs	0	N / A	N / A	N / A
cyberviolence	0	N / A	N / A	N / A
violations de la protection des données et de la vie privée	0	N / A	N / A	N / A
Discours illégal ou nuisible	0	N / A	N / A	N / A
Violations de la propriété intellectuelle	0	N / A	N / A	N / A
Effets négatifs sur le débat civique ou les élections	0	N / A	N / A	N / A
Protection des mineurs	0	N / A	N / A	N / A
Risque pour la sécurité publique	0	N / A	N / A	N / A
Escroqueries/fraudes	0	N / A	N / A	N / A
L'automutilation	0	N / A	N / A	N / A
Produits dangereux, non conformes ou interdits	0	N / A	N / A	N / A
Violence	0	N / A	N / A	N / A
Type de contenu illégal non spécifié par l'autorité compétente	0	N / A	N / A	N / A
Tous les autres types	0	N / A	N / A	N / A
Total:	0	N / A	N / A	N / A

2.2 Ordonnance relative à la communication d'informations sur les bénéficiaires du service par les autorités des États membres

Motif du signalement/Type de contenu illégal	Nombre d'avis reçus	Nombre de notifications reçues par les signaleurs de confiance	Nombre de mesures prises suite aux notifications	Non traité exclusivement par des moyens automatisés moyens	Délai médian de prise de décision
Bien-être animal	0	N / A	N / A	N / A	N / A
atteintes aux droits des consommateurs	0	N / A	N / A	N / A	N / A
violations de la protection des données et de la vie privée	0	N / A	N / A	N / A	N / A
Discours illégal ou nuisible 0		N / A	N / A	N / A	N / A
Violations de la propriété intellectuelle	0	N / A	N / A	N / A	N / A
Effets négatifs sur le débat civique ou les élections	0	N / A	N / A	N / A	N / A
Protection des mineurs	0	N / A	N / A	N / A	N / A
Risque pour la sécurité publique 0		N / A	N / A	N / A	N / A
Escroqueries/fraudes	0	N / A	N / A	N / A	N / A
L'automutilation	0	N / A	N / A	N / A	N / A
Produits dangereux, non conformes ou interdits	0	N / A	N / A	N / A	N / A
Violence	0	N / A	N / A	N / A	N / A
Type de contenu illégal non spécifié par l'autorité compétente	0	N / A	N / A	N / A	N / A
Tous les autres types	0	N / A	N / A	N / A	N / A
Total:	0	N / A	N / A	N / A	N / A

3. Signalements/notifications des utilisateurs

Cette section décrit le nombre et la nature des signalements effectués par les utilisateurs, d'autres personnes et entités concernant les contenus qu'ils jugent illégaux ou non conformes aux conditions d'utilisation de notre plateforme. Elle explique également comment nous gérons les mesures de modération de contenu suite à ces signalements.

Signalements reçus des utilisateurs

Motif du signalement/Type de contenu illégal	Nombre d'avis reçus	Nombre de notifications reçues par les signaleurs de confiance	Nombre de mesures prises suite aux notifications	Non traité exclusivement par des moyens automatisés moyens	Délai médian de prise de décision
Bien-être animal	0	N / A	N / A	N / A	N / A
atteintes aux droits des consommateurs	0	N / A	N / A	N / A	N / A
violations de la protection des données et de la vie privée	0	N / A	N / A	N / A	N / A
Discours illégal ou nuisible 0		N / A	N / A	N / A	N / A
Violations de la propriété intellectuelle	0	N / A	N / A	N / A	N / A
Effets négatifs sur le débat civique ou les élections	0	N / A	N / A	N / A	N / A
Protection des mineurs	0	N / A	N / A	N / A	N / A
Risque pour la sécurité publique 0		N / A	N / A	N / A	N / A
Escroqueries/fraudes	0	N / A	N / A	N / A	N / A
L'automutilation	0	N / A	N / A	N / A	N / A
Produits dangereux, non conformes ou interdits	0	N / A	N / A	N / A	N / A
Violence	0	N / A	N / A	N / A	N / A
Type de contenu illégal non spécifié par l'autorité compétente	0	N / A	N / A	N / A	N / A
Tous les autres types	0	N / A	N / A	N / A	N / A
Total:	0	N / A	N / A	N / A	N / A

4. Modération de contenu effectuée à l'initiative d'Awaze

Awaze s'engage à maintenir un environnement sûr et sécurisé, exempt d'abus, pour ses clients et leurs utilisateurs. En tant que fournisseur de plateforme de service client, notre plateforme permet aux entreprises d'interagir avec les utilisateurs par messagerie, e-mail et intégrations ; autant de canaux qui présentent un risque d'abus s'ils ne sont pas correctement protégés.

Nous utilisons une approche multicouche pour la modération des contenus, combinant des systèmes de détection automatisés, des outils d'administration internes et des processus de vérification manuelle. Cette section présente un aperçu des actions de modération menées de notre propre initiative, sans obligation légale ni notification de tiers.

La modération effectuée de notre propre initiative comprend à la fois la détection proactive par des systèmes automatisés et la vérification manuelle par des modérateurs de contenu. Nous nous engageons à ce que tous les membres du personnel impliqués dans la modération de contenu disposent des compétences, des connaissances et des ressources nécessaires pour s'acquitter de leurs responsabilités de manière équitable et précise, conformément aux lois applicables et aux politiques internes.

Modération de contenu à l'initiative de l'entreprise

Type de contenu illégal ou autre violation des conditions d'utilisation acceptables	Nombre d'éléments modérés	Nombre de ces éléments détectés uniquement par des méthodes automatisées moyens	Type de restriction appliquée
Escroqueries/fraudes	Courriels entrants filtrés : 2 691 775 (données annualisées ; incluant 52 046 détections d'usurpation d'identité) Liens malveillants détectés : 1 135 clics sur des URL non sécurisées (courriel) + 98 262 événements de protection DNS bloqués (Web, dont 7 165 tentatives d'hameçonnage) Téléchargements malveillants détectés : 1 010 détections de logiciels malveillants entrants (courriel)	Courriels entrants filtrés : 2 691 775 Liens malveillants détectés : 1 135 (courriel) + 98 262 (web) 1 010 téléchargements malveillants détectés	Restriction de visibilité : les courriels sont mis en quarantaine. Bloqués ; les requêtes web sont bloquées par le filtrage DNS/la politique de pare-feu. Suppression de contenu : les courriels entrants peuvent être rejetés (non distribués) s'ils correspondent à du spam. Contrôles anti-logiciels malveillants et anti-usurpation d'identité. Suspension de compte : non utilisée par ces contrôles (gérée par des processus RH/IT distincts le cas échéant).
Autres types de violations des conditions générales de la plateforme	Nombre total de plaintes pour spam : 96 665 (Rejet de spam – passerelle de messagerie sécurisée ; estimation annualisée à l'état d'équilibre)	Plaintes automatisées pour spam : 96 665 (Détection automatique de spam au niveau de la passerelle de messagerie sécurisée)	Suspension des autorisations de la plateforme : sans objet. Il s'agit de rejets de passerelle de messagerie, et non de mesures d'application de la plateforme.
Total:	191 072	197 072	N / A

4. Description qualitative des moyens automatisés

Awaze utilise des contrôles de sécurité automatisés pour réduire les escroqueries, le phishing, l'usurpation d'identité et les logiciels malveillants lors de l'accès au Web et par courrier électronique.

Protection du courrier électronique : Nous utilisons une passerelle de messagerie sécurisée (Mimecast) pour inspecter les courriels entrants avant leur distribution. Cette passerelle effectue des contrôles automatisés (réputation, authentification, etc.). Nous utilisons l'analyse de contenu, la détection de logiciels malveillants et la détection d'usurpation d'identité pour rejeter ou mettre en quarantaine les messages associés à des escroqueries, des fraudes, des usurpations d'identité ou des logiciels malveillants. Nous utilisons également des contrôles d'authentification des e-mails sur l'ensemble de nos domaines (SPF, DKIM et DMARC). Ces contrôles permettent aux systèmes de réception de vérifier que les messages prétendant provenir des domaines Awaze sont autorisés et n'ont pas été modifiés, et ils réduisent les tentatives d'usurpation de domaine et d'identité.

Protection web : Nous utilisons un service de sécurité SD-WAN géré (Cato) qui applique un filtrage DNS, une politique de pare-feu et une prévention des intrusions. Ce service bloque l'accès aux domaines malveillants connus, aux infrastructures d'hameçonnage et aux serveurs de commande et de contrôle, et bloque les schémas de trafic à haut risque en périphérie du réseau.

Note relative au rapport : Les chiffres annuels sont estimés à l'aide des fenêtres de rapport des fournisseurs (Mimecast août-décembre 2025 ; Cato 12 oct.-31 déc. 2025) et supposent un état stable sans changement de politique ni de volume.

Objectifs précis

Les outils automatisés visent à protéger les activités de messagerie entrantes et sortantes, à prévenir les abus, à préserver la réputation de l'expéditeur et à garantir la conformité aux directives et à la législation (par exemple, les directives d'envoi de courriels, la conformité à la loi CAN-SPAM). Leurs objectifs spécifiques incluent :

- Détection des activités et des schémas suspects lors de l'inscription ;
- Évaluation du contenu lors de sa création et de son accès via les liens, les téléchargements et autres contenus générés par les utilisateurs ;
- Surveillance des limites de débit et des seuils d'utilisation pour les fonctionnalités clés ;
- Évaluation du risque basée sur des données historiques ;
- Empêcher la diffusion de courriels d'hameçonnage, d'usurpation d'identité et de logiciels malveillants en les rejetant ou en les mettant en quarantaine. messages entrants correspondant aux contrôles automatisés des menaces ;
- Empêcher l'accès aux sites Web malveillants en bloquant la résolution DNS et/ou le trafic Web pour domaines et catégories associés aux logiciels malveillants, au phishing, aux DGA et au commandement et contrôle ; et
- Détecter et bloquer les attaques réseau (par exemple les tentatives par force brute, les blocages basés sur la réputation, l'analyse des vulnérabilités et les modèles d'exploitation) à l'aide des signatures IPS et de la politique de pare-feu.

Utilisation de l'authentification des e-mails SPF/DKIM/DMARC pour réduire l'usurpation des domaines Awaze et améliorer la détection et le rejet des e-mails d'usurpation d'identité et d'hameçonnage.

Indicateurs de précision et taux d'erreur possible

Nous avons une grande confiance en nos outils, avec un faible taux de faux positifs. Cependant, les clients peuvent faire appel auprès de notre équipe d'assistance s'ils estiment qu'un faux positif a été généré par nos processus de modération de contenu ou nos outils anti-abus.

Courriel : La détection repose sur l'analyse automatisée des menaces, les contrôles d'authentification, l'analyse du contenu et la détection de logiciels malveillants. Des faux positifs peuvent survenir (par exemple, des expéditeurs légitimes ou des domaines récemment enregistrés) ; ce problème est atténué par l'ajout de listes blanches, l'ajustement des politiques et l'examen des messages mis en quarantaine ou rejetés.

Web/DNS : Les blocages DNS et pare-feu s'appuient sur des flux de données de menaces, la catégorisation, des indicateurs comportementaux (par exemple, la détection DGA) et les signatures IPS. Des faux positifs peuvent survenir (par exemple, des domaines mal catégorisés ou une infrastructure partagée) et sont gérés par des exceptions/listes blanches et un ajustement périodique des règles.

Awaze analyse les tendances et ajuste ses politiques en conséquence afin de réduire les faux positifs tout en maintenant la protection.

• Les espaces de travail doivent réussir une évaluation anti-abus avant de pouvoir bénéficier de nombreuses fonctionnalités.
notamment celles qui permettent les communications sortantes.

• La limitation du débit, l'analyse du contenu et la détection des schémas de spam sont en place sur de nombreux canaux.
notre produit

• Si un contenu n'enfreint pas nos conditions générales, mais qu'un client souhaite administrer son espace de travail selon ses propres conditions,
il peut supprimer du contenu ou bloquer des utilisateurs à sa guise.

• Des dérogations manuelles par le service client (CS) sont disponibles pour les blocages automatisés.

• Les employés d'Awaze (par exemple, le service client) disposent d'outils pour approuver ou refuser la réactivation des comptes bloqués.
tentatives d'envoi d'e-mails.

• Nous appliquons des contrôles multicouches (passerelle de messagerie + filtrage DNS + pare-feu + IPS) afin qu'aucun contrôle unique ne soit
On s'y fiait exclusivement.

Nous utilisons des listes blanches et des exceptions (lorsque cela est justifié) et nous adaptons les politiques en fonction des besoins opérationnels.
impact et risque pour la sécurité.

• Nous conservons des journaux d'audit et des rapports d'événements de sécurité pour faciliter les enquêtes et la réponse aux incidents.

• Les politiques de sécurité et les capacités de détection sont maintenues grâce aux mises à jour des fournisseurs et aux processus internes.
revoir

Nous appliquons l'authentification des e-mails au niveau du domaine (SPF, DKIM et DMARC) comme mesure de protection supplémentaire afin de réduire l'usurpation d'identité et d'améliorer la fiabilité des décisions de filtrage automatisé des e-mails.

6. Plaintes reçues

Nombre de plaintes reçues par le biais de nos systèmes internes de traitement des plaintes

mécanisme de plaintes internes

Nombre de plaintes déposées	0
Motif de la plainte	N / A
Décisions prises suite à une plainte	N / A
Délai médian de traitement des réclamations	N / A