awaze

GESETZ ÜBER DIGITALE DIENSTE

Transparenzbericht

für den Berichtszeitraum, der im Dezember 2025 endet

Bericht veröffentlicht: 17. Februar 2026

1. Einleitung

Dieser Transparenzbericht wurde gemäß Artikel 15 der Verordnung (EU) 2022/2065, dem Gesetz über digitale Dienste (Digital Services Act, DSA), erstellt. Er beschreibt unsere Vorgehensweise bei der Inhaltsmoderation und unsere Durchsetzungsentscheidungen in Bezug auf bestimmte Produktbereiche und soll klare, zugängliche und umfassende Informationen darüber bereitstellen, wie wir Inhalte auf unserer Plattform verwalten und moderieren.

Dieser Bericht behandelt insbesondere Moderationsmaßnahmen und -verfahren, die auf die folgenden Produkte angewendet werden: Die Online-Plattformen und digitalen Dienste der Awaze Group, die das Auflisten, Auffinden und Buchen von kurzfristigen Ferienunterkünften ermöglichen, einschließlich nutzergenerierter Inhalte wie Immobilienangebote, Beschreibungen, Bilder, Bewertungen und zugehörige Mitteilungen.

Dieser Bericht ist Teil unseres kontinuierlichen Engagements für Transparenz, Rechenschaftspflicht und die Einhaltung der im DSA festgelegten Verpflichtungen.

Name des Dienstanbieters	Dieser Bericht umfasst die folgenden juristischen Personen der Awaze-Gruppe: Novasol, Fincallorca, Ardennes Étape und SandyBlue – gemeinsam die „Awaze-Gruppe“
Datum der Veröffentlichung des Berichts	**17. Februar 2026**
Datum der Veröffentlichung des letzten vorherigen Berichts	**17. Februar 2025**
Beginn des Berichtszeitraums	**1. Januar 2025**
Enddatum des Berichtszeitraums	**31. Dezember 2025**

2. Von Behörden der EU-Mitgliedstaaten erteilte Aufträge

Gemäß Artikel 9 und 10 des DSA enthält dieser Abschnitt Informationen über Anordnungen, die im Berichtszeitraum von zuständigen Behörden der EU-Mitgliedstaaten ergangen sind. Diese Anordnungen beziehen sich auf illegale Inhalte und Informationsanfragen.

2.1. Anordnungen von Behörden der Mitgliedstaaten zur Bekämpfung illegaler Inhalte

Art der illegalen Inhalte	Anzahl der eingegangenen Bestellungen	Mitgliedstaat, der die Anordnung erlässt	Mittlere Zeit bis zur Empfangsbestätigung	Mittlere Zeit bis zur Umsetzung der Bestellung
Tierschutz	0	N / A	N / A	N / A
Verstöße gegen Verbraucherschutz	0	N / A	N / A	N / A
Cybergewalt	0	N / A	N / A	N / A
Datenschutz- und Privatsphäreverletzungen	0	N / A	N / A	N / A
Illegale oder schädliche Äußerungen	0	N / A	N / A	N / A
Verletzungen des geistigen Eigentums	0	N / A	N / A	N / A
Negative Auswirkungen auf den öffentlichen Diskurs oder Wahlen	0	N / A	N / A	N / A
Schutz von Minderjährigen	0	N / A	N / A	N / A
Risiko für die öffentliche Sicherheit	0	N / A	N / A	N / A
Betrug/Abzocke	0	N / A	N / A	N / A
Selbstverletzung	0	N / A	N / A	N / A
Unsichere, nicht konforme oder verbotene Produkte	0	N / A	N / A	N / A
Gewalt	0	N / A	N / A	N / A
Art der illegalen Inhalte nicht von der Behörde spezifiziert	0	N / A	N / A	N / A
Alle anderen Arten	0	N / A	N / A	N / A
Gesamt:	0	N / A	N / A	N / A

2.2 Anordnung der Behörden eines Mitgliedstaats zur Übermittlung von Informationen über die Leistungsempfänger

Grund für die Meldung/Art des illegalen Inhalts	Anzahl der eingegangenen Benachrichtigungen	Anzahl der von vertrauenswürdigen Meldern erhaltenen Benachrichtigungen	Anzahl der aufgrund der Bekanntmachungen ergriffenen Maßnahmen	Nein. ausschließlich automatisiert bedeutet	Mittlere Zeit bis zum Handeln
Tierschutz	0	N / A	N / A	N / A	N / A
Verstöße gegen Verbraucherschutz	0	N / A	N / A	N / A	N / A
Datenschutz- und Privatsphäreverletzungen	0	N / A	N / A	N / A	N / A
Illegale oder schädliche Äußerungen	0	N / A	N / A	N / A	N / A
Verletzungen des geistigen Eigentums	0	N / A	N / A	N / A	N / A
Negative Auswirkungen auf den öffentlichen Diskurs oder Wahlen	0	N / A	N / A	N / A	N / A
Schutz von Minderjährigen	0	N / A	N / A	N / A	N / A
Risiko für die öffentliche Sicherheit	0	N / A	N / A	N / A	N / A
Betrug/Abzocke	0	N / A	N / A	N / A	N / A
Selbstverletzung	0	N / A	N / A	N / A	N / A
Unsichere, nicht konforme oder verbotene Produkte	0	N / A	N / A	N / A	N / A
Gewalt	0	N / A	N / A	N / A	N / A
Art der illegalen Inhalte nicht von der Behörde spezifiziert	0	N / A	N / A	N / A	N / A
Alle anderen Arten	0	N / A	N / A	N / A	N / A
Gesamt:	0	N / A	N / A	N / A	N / A

3. Benutzerberichte/-mitteilungen

Dieser Abschnitt beschreibt Anzahl und Art der Meldungen, die von Nutzern, anderen Personen und Organisationen bezüglich Inhalten eingereicht werden, die ihrer Ansicht nach illegal sind oder gegen unsere Nutzungsbedingungen verstoßen. Außerdem wird erläutert, wie wir bei der Inhaltsmoderation auf Nutzermeldungen reagieren.

Von Nutzern erhaltene Berichte

Grund für die Meldung/Art des illegalen Inhalts	Anzahl der eingegangenen Benachrichtigungen	Anzahl der von vertrauenswürdigen Meldern erhaltenen Benachrichtigungen	Anzahl der aufgrund der Bekanntmachungen ergriffenen Maßnahmen	Nein. ausschließlich automatisiert bedeutet	Mittlere Zeit bis zum Handeln bedeutet
Tierschutz	0	N / A	N / A	N / A	N / A
Verstöße gegen Verbraucherschutz	0	N / A	N / A	N / A	N / A
Datenschutz- und Privatsphäreverletzungen	0	N / A	N / A	N / A	N / A
Illegale oder schädliche Äußerungen	0	N / A	N / A	N / A	N / A
Verletzungen des geistigen Eigentums	0	N / A	N / A	N / A	N / A
Negative Auswirkungen auf den öffentlichen Diskurs oder Wahlen	0	N / A	N / A	N / A	N / A
Schutz von Minderjährigen	0	N / A	N / A	N / A	N / A
Risiko für die öffentliche Sicherheit	0	N / A	N / A	N / A	N / A
Betrug/Abzocke	0	N / A	N / A	N / A	N / A
Selbstverletzung	0	N / A	N / A	N / A	N / A
Unsichere, nicht konforme oder verbotene Produkte	0	N / A	N / A	N / A	N / A
Gewalt	0	N / A	N / A	N / A	N / A
Art der illegalen Inhalte nicht von der Behörde spezifiziert	0	N / A	N / A	N / A	N / A
Alle anderen Arten	0	N / A	N / A	N / A	N / A
Gesamt:	0	N / A	N / A	N / A	N / A

4. Inhaltsmoderation auf eigene Initiative von Awaze.

Awaze setzt sich für eine sichere und missbrauchsfreie Umgebung für unsere Kunden und deren Endnutzer ein. Als Anbieter einer Kundenservice-Plattform ermöglicht unsere Plattform Unternehmen die Kommunikation mit Nutzern über Messaging, E-Mail und Integrationen – Kanäle, die alle ein Missbrauchspotenzial bergen, wenn sie nicht ausreichend geschützt sind.

Wir nutzen einen mehrstufigen Ansatz zur Inhaltsmoderation, der automatisierte Erkennungssysteme, interne Verwaltungstools und manuelle Prüfprozesse kombiniert. Dieser Abschnitt bietet einen Überblick über die von uns aus eigener Initiative ergriffenen Maßnahmen zur Inhaltsmoderation, ohne dass eine rechtliche Verpflichtung oder eine Benachrichtigung Dritter erforderlich war.

Die von uns aus eigener Initiative durchgeführte Moderation umfasst sowohl proaktive Erkennungen mithilfe automatisierter Systeme als auch die manuelle Überprüfung durch unsere Inhaltsmoderatoren. Wir stellen sicher, dass alle an der Inhaltsmoderation beteiligten Mitarbeiter über die notwendigen Fähigkeiten, Kenntnisse und Ressourcen verfügen, um ihre Aufgaben fair, präzise und im Einklang mit geltenden Gesetzen und internen Richtlinien zu erfüllen.

Eigeninitiative Inhaltsmoderation

Art des illegalen Inhalts oder sonstiger Verstoß gegen die Nutzungsrichtlinien	Anzahl der moderierten Elemente	Anzahl der ausschließlich mit automatisierten Verfahren erkannten Elemente	Art der angewandten Beschränkung
Betrug/Abzocke	Eingehende E-Mails gefiltert: 2.691.775 (jährlich hochgerechnet; beinhaltet 52.046 Fälle von Identitätsdiebstahl) Schädliche Links gefunden: 1.135 unsichere URL-Klicks erkannt (E-Mail) + 98.262 blockierte DNS-Schutzereignisse (Web, inkl. 7.165 Phishing) Schadsoftware-Uploads gefunden: 1.010 eingehende Malware-Erkennungen (E-Mail)	Eingehende E-Mails gefiltert: 2.691.775 Schadlinks gefunden: 1.135 (E-Mail) + 98.262 (Web) Schadhafte Uploads gefunden: 1.010	Sichtbarkeitseinschränkung: E-Mails werden unter Quarantäne gestellt/ blockiert; Webanfragen werden durch DNS-Filterung/Firewall-Richtlinien blockiert. Inhaltsentfernung: Eingehende E-Mails können abgelehnt (nicht zugestellt) werden, wenn sie als Spam eingestuft werden. Malware-/Identitätsdiebstahl-Kontrollen. Kontosperrung: Wird von diesen Kontrollen nicht genutzt (wird bei Bedarf über separate HR-/IT-Prozesse abgewickelt).
Andere Arten von Verstößen gegen die Nutzungsbedingungen der Plattform	Gesamtzahl der Spam-Beschwerden: 96.665 (Spamabweisung – sicheres E-Mail-Gateway; annualisierte Steady-State-Schätzung)	Automatisierte Spam-Beschwerden: 96.665 (Automatisierte Spam-Erkennung am sicheren E-Mail-Gateway)	Plattformberechtigungen aussetzen: Nicht zutreffend. Es handelt sich hierbei um Ablehnungen durch das E-Mail-Gateway, nicht um Maßnahmen zur Durchsetzung der Plattform
Gesamt:	191.072	197.072	N / A

4. Qualitative Beschreibung der automatisierten Mittel

Awaze nutzt automatisierte Sicherheitskontrollen, um Betrug, Phishing, Identitätsdiebstahl und Malware beim E-Mail- und Webzugriff zu reduzieren.

E-Mail-Schutz: Wir nutzen ein sicheres E-Mail-Gateway (Mimecast), um eingehende E-Mails vor der Zustellung zu prüfen. Das Gateway verwendet automatisierte Prüfungen (Reputation, Authentifizierung, …). Wir analysieren Inhalte, scannen Schadsoftware und erkennen Identitätsdiebstahl, um Nachrichten im Zusammenhang mit Betrug, Identitätsdiebstahl oder Schadsoftware abzulehnen oder unter Quarantäne zu stellen. Zudem verwenden wir für unsere Domains E-Mail-Authentifizierungsmechanismen (SPF, DKIM und DMARC). Diese Mechanismen helfen empfangenden Systemen zu überprüfen, ob Nachrichten, die angeblich von Awaze-Domains stammen, autorisiert und nicht verändert wurden. Dadurch werden Domain-Spoofing und Identitätsdiebstahl reduziert.

Webschutz: Wir nutzen einen verwalteten SD-WAN-Sicherheitsdienst (Cato), der DNS-Filterung, Firewall-Richtlinien und Intrusion Prevention einsetzt. Dadurch wird der Zugriff auf bekannte schädliche Domains, Phishing-Infrastrukturen und Command-and-Control-Server blockiert und risikoreiche Datenverkehrsmuster am Netzwerkrand unterbunden.

Anmerkung zur Berichterstattung: Die Jahreszahlen wurden unter Verwendung der Berichtszeiträume der Anbieter geschätzt (Mimecast Aug–Dez 2025; Cato 12. Okt–31. Dez 2025) und basieren auf der Annahme eines stabilen Zustands ohne Änderung der Richtlinien oder des Volumens.

Genaue Zwecke

Die automatisierten Tools dienen dem Schutz des ein- und ausgehenden Nachrichtenverkehrs, der Missbrauchsprävention, der Aufrechterhaltung der Absenderreputation und der Sicherstellung der Einhaltung von Richtlinien und Gesetzen (z. B. Richtlinien für den E-Mail-Versand, CAN-SPAM-Konformität). Zu den konkreten Zwecken gehören:

- **Erkennung verdächtiger Aktivitäten und Muster während der Registrierung;**
- **Bewertung von Inhalten bei der Erstellung und beim Zugriff über Links, Uploads und andere nutzergenerierte Inhalte;**
- **Überwachung von Ratenbegrenzungen und Nutzungsschwellenwerten für wichtige Funktionen;**
- **Risikobewertung auf Basis historischer Daten;**
- **Verhindern Sie die Zustellung von Phishing-, Identitätsdiebstahl- und Malware-E-Mails durch Ablehnen oder Quarantäne. eingehende Nachrichten, die mit automatisierten Bedrohungsabwehrsystemen übereinstimmen;**
- **Verhindern Sie den Zugriff auf schädliche Webseiten, indem Sie die DNS-Auflösung und/oder den Webverkehr blockieren. Domänen und Kategorien im Zusammenhang mit Malware, Phishing, DGAs und Command-and-Control-Systemen; und**
- **Netzwerkbasierte Angriffe (z. B. Brute-Force-Angriffe, reputationsbasierte Blockierungen, Schwachstellenscans und Exploit-Muster) mithilfe von IPS-Signaturen und Firewall-Richtlinien erkennen und blockieren.**

Die Verwendung von SPF/DKIM/DMARC-E-Mail-Authentifizierung soll das Spoofing von Awaze-Domains reduzieren und die Erkennung und Ablehnung von Identitätsdiebstahl- und Phishing-E-Mails verbessern.

Indikatoren für Genauigkeit und mögliche Fehlerrate

Wir haben großes Vertrauen in unsere Tools, da sie eine niedrige Rate an Fehlalarmen aufweisen. Sollten Kunden jedoch der Ansicht sein, dass es in unseren Inhaltsmoderationsprozessen oder unseren Tools zur Missbrauchsbekämpfung zu einem Fehlalarm gekommen ist, können sie sich an unser Support-Team wenden.

E-Mail: Die Erkennung basiert auf automatisierter Bedrohungsanalyse, Authentifizierungsprüfungen, Inhaltsanalyse und Malware-Scans. Fehlalarme können auftreten (z. B. bei legitimen Massenabsendern oder neu registrierten Domains) und werden durch Whitelisting, Richtlinienanpassung und Überprüfung von unter Quarantäne gestellten/abgelehnten Nachrichten minimiert.

Web/DNS: DNS- und Firewall-Blockierungen basieren auf Bedrohungsdaten, Kategorisierung, Verhaltensindikatoren (z. B. DGA-Erkennung) und IPS-Signaturen. Fehlalarme können auftreten (z. B. bei falsch kategorisierten Domains oder gemeinsam genutzter Infrastruktur) und werden über Ausnahme-/Zulassungslisten und regelmäßige Regelanpassungen verwaltet.

Awaze analysiert Trends und passt die Richtlinien bei Bedarf an, um Fehlalarme zu reduzieren und gleichzeitig den Schutz aufrechtzuerhalten.

- **Arbeitsbereiche müssen eine Missbrauchsprüfung bestehen, bevor sie viele Funktionen nutzen können.**
  insbesondere solche, die ausgehende Kommunikation ermöglichen.
- **Ratenbegrenzung, Inhaltsprüfung und Spammustererkennung sind auf vielen Kanälen implementiert.**
  unser Produkt
- **Wenn Inhalte nicht gegen unsere Nutzungsbedingungen verstoßen, ein Kunde aber seinen Arbeitsbereich nach eigenen Vorgaben verwalten**
  möchte, kann er Inhalte entfernen oder Benutzer nach eigenem Ermessen sperren.
- **Manuelle Überschreibungen durch den Kundendienst sind für automatisierte Sperren möglich.**
- **Awaze-Mitarbeiter (z. B. der Kundensupport) verfügen über die nötigen Werkzeuge, um die Wiederherstellung gesperrter Konten zu genehmigen oder abzul**
  E-Mail-Versuche.
- **Wir setzen mehrschichtige Kontrollen ein (E-Mail-Gateway + DNS-Filterung + Firewall + IPS), sodass keine einzelne Kontrollmaßnahme ausreicht.**
  ausschließlich darauf verlassen.
- **Wir verwenden Zulassungslisten/Ausnahmen (wo gerechtfertigt) und passen die Richtlinien basierend auf dem operativen Bedarf an.**
  Auswirkungen und Sicherheitsrisiko.
- **Wir führen Audit-Protokolle und erstellen Berichte über Sicherheitsereignisse, um die Untersuchung und die Reaktion auf Vorfälle zu unterstützen.**
- **Sicherheitsrichtlinien und Erkennungsfunktionen werden durch Herstelleraktualisierungen und interne Updates aufrechterhalten.**
  Rezension

Wir setzen die Domain-basierte E-Mail-Authentifizierung (SPF, DKIM und DMARC) als zusätzliche Sicherheitsmaßnahme ein, um Spoofing zu reduzieren und die Zuverlässigkeit der automatisierten E-Mail-Filterentscheidungen zu verbessern.

6. Eingegangene Beschwerden

Anzahl der Beschwerden, die wir über unsere internen Beschwerdebearbeitungssysteme erhalten haben

Interner Beschwerdemechanismus

Anzahl der eingereichten Beschwerden	**0**
Grundlage der Beschwerde	**N / A**
Entscheidungen, die aufgrund einer Beschwerde getroffen wurden	**N / A**
Durchschnittliche Bearbeitungszeit einer Beschwerde	**N / A**