awaze

LOV OM DIGITALE TJENESTER

Gennemsigtighedsrapport

for rapporteringsperioden, der slutter i december 2025

Rapport udgivet: 17. februar 2026

1. Introduktion

Denne gennemsigtighedsrapport er udarbejdet i overensstemmelse med artikel 15 i forordning (EU) 2022/2065, Digital Services Act (DSA). Den beskriver vores praksis for indholdsmoderering og håndhævelsesbeslutninger vedrørende specifikke produktområder og har til formål at give klare, tilgængelige og omfattende oplysninger om, hvordan vi administrerer og modererer indhold på vores platform.

Denne rapport dækker specifikt modereringshandlinger og -procedurer, der anvendes på følgende produkter: Awaze Groups onlineplatforme og digitale tjenester, der letter annoncering, opdagelse og booking af korttidsferieboliger, herunder brugergenereret indhold såsom ejendomsfortegnelser, beskrivelser, billeder, anmeldelser og relateret kommunikation.

Denne rapport er en del af vores løbende forpligtelse til gennemsigtighed, ansvarlighed og overholdelse af de forpligtelser, der er fastsat i DSA.

Navn på tjenesteudbyder	Denne rapport dækker følgende juridiske enheder i Awaze Group: Novasol, Fincallorca, Ardennes Étape og SandyBlue - Samlet kaldet "Awaze Gruppen"
Dato for rapportens offentliggørelse	**17. februar 2026**
Dato for offentliggørelse af den seneste forrige rapport	**17. februar 2025**
Startdato for rapporteringsperioden	**1. januar 2025**
Slutdato for rapporteringsperioden	**31. december 2025**

2. Ordrer modtaget fra myndigheder i EU-medlemsstater

I overensstemmelse med artikel 9 og 10 i DSA indeholder dette afsnit oplysninger om påbud modtaget fra kompetente myndigheder i EU-medlemsstaterne i rapporteringsperioden. Disse påbud vedrører ulovligt indhold og anmodninger om oplysninger.

2.1. Påbud om at gribe ind over for ulovligt indhold fra medlemsstaternes myndigheder

Type af ulovligt indhold	Antal modtagne ordrer	Medlemsstat udstedende ordre	Median tid til bekræftelse af modtagelse	Median tid til at iværksætte ordren
Dyrevelfærd	0	Ikke tilgængelig	Ikke tilgængelig	Ikke tilgængelig
Overtrædelser af forbrugeroplysninger	0	Ikke tilgængelig	Ikke tilgængelig	Ikke tilgængelig
Cybervold	0	Ikke tilgængelig	Ikke tilgængelig	Ikke tilgængelig
Databeskyttelse og krænkelser af privatlivets fred	0	Ikke tilgængelig	Ikke tilgængelig	Ikke tilgængelig
Ulovlig eller skadelig tale	0	Ikke tilgængelig	Ikke tilgængelig	Ikke tilgængelig
Krænkelser af intellektuel ejendomsret	0	Ikke tilgængelig	Ikke tilgængelig	Ikke tilgængelig
Negative virkninger på den borgerlige diskurs eller valg	0	Ikke tilgængelig	Ikke tilgængelig	Ikke tilgængelig
Beskyttelse af mindreårige	0	Ikke tilgængelig	Ikke tilgængelig	Ikke tilgængelig
Risiko for den offentlige sikkerhed	0	Ikke tilgængelig	Ikke tilgængelig	Ikke tilgængelig
Svindel/bedrageri	0	Ikke tilgængelig	Ikke tilgængelig	Ikke tilgængelig
Selvskade	0	Ikke tilgængelig	Ikke tilgængelig	Ikke tilgængelig
Usikre, ikke-overensstemmende eller forbudte produkter	0	Ikke tilgængelig	Ikke tilgængelig	Ikke tilgængelig
Vold	0	Ikke tilgængelig	Ikke tilgængelig	Ikke tilgængelig
Type af ulovligt indhold ikke specificeret af myndigheden	0	Ikke tilgængelig	Ikke tilgængelig	Ikke tilgængelig
Alle andre typer	0	Ikke tilgængelig	Ikke tilgængelig	Ikke tilgængelig
Total:	0	Ikke tilgængelig	Ikke tilgængelig	Ikke tilgængelig

2.2 Påbud om at give oplysninger om modtagere af tjenesteydelsen fra medlemsstaternes myndigheder

Rapportér årsag/type af ulovligt indhold	Antal modtagne meddelelser	Antal meddelelser modtaget af betroede anmeldere	Antal handlinger foretaget på baggrund af meddelelser	Antal behandlet udelukkende automatiseret betyder	Median tid til at handle
Dyrevelfærd	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Overtrædelser af forbrugeroplysninger	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Databeskyttelse og krænkelser af privatlivets fred	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Ulovlig eller skadelig tale 0		ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Krænkelser af intellektuel ejendomsret	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Negative virkninger på den borgerlige diskurs eller valg	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Beskyttelse af mindreårige	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Risiko for den offentlige sikkerhed 0		ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Svindel/bedrageri	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Selvskade	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Usikre, ikke-overensstemmende eller forbudte produkter	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Vold	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Type af ulovligt indhold ikke specificeret af myndigheden	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Alle andre typer	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Total:	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig

3. Brugerrapporter/meddelelser

Dette afsnit beskriver antallet og arten af rapporter indsendt af brugere, andre enkeltpersoner og enheder vedrørende indhold, som de mener er ulovligt eller i strid med vores platforms vilkår og betingelser. Derudover beskriver det, hvordan vi håndterer indholdsmodereringshandlinger som reaktion på brugerrapporter.

Rapporter modtaget fra brugere

Rapportér årsag/type af ulovligt indhold	Antal modtagne meddelelser	Antal meddelelser modtaget af betroede anmeldere	Antal handlinger foretaget på baggrund af meddelelser	Antal behandlet udelukkende automatiseret betyder	Median tid til at handle
Dyrevelfærd	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Overtrædelser af forbrugeroplysninger	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Databeskyttelse og krænkelser af privatlivets fred	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Ulovlig eller skadelig tale 0		ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Krænkelser af intellektuel ejendomsret	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Negative virkninger på den borgerlige diskurs eller valg	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Beskyttelse af mindreårige	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Risiko for den offentlige sikkerhed 0		ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Svindel/bedrageri	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Selvskade	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Usikre, ikke-overensstemmende eller forbudte produkter	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Vold	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Type af ulovligt indhold ikke specificeret af myndigheden	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Alle andre typer	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig
Total:	0	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig	ikke tilgængelig

4. Indholdsmoderering udført på Awazes eget initiativ

Awaze er forpligtet til at opretholde et sikkert og misbrugsfrit miljø for både vores kunder og deres slutbrugere. Som udbyder af kundeserviceplatforme gør vores platform det muligt for virksomheder at interagere med brugerne via beskeder, e-mail og integrationer - som alle indebærer potentiale for misbrug, hvis de ikke beskyttes korrekt.

Vi bruger en lagdelt tilgang til indholdsmoderering, der kombinerer automatiserede detektionssystemer, interne administrationsværktøjer og manuelle gennemgangsprocesser. Dette afsnit giver et overblik over indholdsmodereringshandlinger, der udføres på vores eget initiativ, uden nogen juridisk forpligtelse eller varsel til tredjepart.

Moderering udført på vores eget initiativ omfatter både proaktiv detektion ved hjælp af automatiserede systemer og manuel gennemgang foretaget af indholdsmoderatorer. Vi er forpligtet til at sikre, at alle medarbejdere involveret i indholdsmoderering er udstyret med de nødvendige færdigheder, viden og ressourcer til at udføre deres ansvar retfærdigt, præcist og i overensstemmelse med gældende love og interne politikker.

Indholdsmoderering på eget initiativ

Type af ulovligt indhold eller anden overtrædelse af AUP	Antal modererede elementer	Antal af disse elementer, der udelukkende er detekteret ved hjælp af automatiserede betyder	Type af anvendt begrænsning
Svindel/bedrageri	Indgående e-mails filtreret: 2.691.775 (årlig; inkluderer 52.046 registreringer af personefterligning) Ondsindede links fundet: 1.135 usikre URL-klik registreret (e-mail) + 98.262 DNS-beskyttelseshændelser blokeret (web, inkl. 7.165 phishing) Ondsindede uploads fundet: 1.010 indgående malware-detektioner (e-mail)	Indgående e-mails filtreret: 2.691.775 Ondsindede links fundet: 1.135 (e-mail) + 98.262 (web) Ondsindede uploads fundet: 1.010	Synlighedsbegrænsning: E-mails er sat i karantæne/ blokeret; webanmodninger blokeres af DNS-filtrering/firewallpolitik. Fjernelse af indhold: Indgående e-mails kan afvises (ikke leveres), når de matcher spam/ Malware-/ personefterligningskontroller. Kontosuspendering: Bruges ikke af disse kontroller (håndteres via separate HR/IT-processer, hvor det er nødvendigt)
Andre typer overtrædelser af platformens vilkår og betingelser	Samlet antal spamklager: 96.665 (Spamafvisning – sikker e-mailgateway; årligt estimat for stabil tilstand)	Automatiserede spamklager: 96.665 (automatisk spamregistrering ved den sikre e-mailgateway)	Suspender platformtilladelser: Ikke relevant. Disse er afvisninger af e-mailgateways, ikke håndhævelseshandlinger for platformen.
Total:	191.072	197.072	Ikke tilgængelig

4. Kvalitativ beskrivelse af de automatiserede midler

Awaze bruger automatiserede sikkerhedskontroller til at reducere svindel, phishing, efterligning og malware på tværs af e-mail og webadgang.

E-mailbeskyttelse: Vi bruger en sikker e-mailgateway (Mimecast) til at inspicere indgående e-mail, før den leveres. Gatewayen bruger automatiserede kontroller (omdømme, godkendelse, indholdsanalyse, malware-scanning og efterligningsdetektion) for at afvise eller sætte meddelelser i karantæne, der er forbundet med svindel/bedrageri, efterligning eller malware. Vi bruger også e-mail-godkendelseskontroller på tværs af vores domæner (SPF, DKIM og DMARC). Disse kontroller hjælper modtagende systemer med at verificere, at meddelelser, der hævder at komme fra Awaze-domæner, er autoriserede og ikke er blevet ændret, og de reducerer domæneforfalskning og efterligningsforsøg.

Webbeskyttelse: Vi bruger en administreret SD-WAN-sikkerhedstjeneste (Cato), der anvender DNS-filtrering, firewallpolitik og indtrængningsforebyggelse. Dette blokerer adgang til kendte ondsindede domæner, phishing-infrastruktur og kommando-og-kontrol-destinationer, og det blokerer højrisikotrafikmønstre i netværkskanten.

Rapporteringsnote: Årlige tal er estimeret ved hjælp af leverandørrapporteringsvinduer (Mimecast aug.-dec. 2025; Cato 12. okt.-31. dec. 2025) og antager en stabil tilstand uden ændringer i politik eller volumen.

Præcise formål

De automatiserede værktøjer har til formål at beskytte indgående og udgående beskedaktivitet, forhindre misbrug, opretholde afsenderens omdømme og sikre overholdelse af retningslinjer og lovgivning (f.eks. retningslinjer for afsendelse af e-mails, CAN-SPAM-overholdelse). Specifikke formål omfatter:

- **Registrering af mistænkelig aktivitet og mønstre under tilmelding;**
- **Evaluering af indhold ved oprettelse og adgang på tværs af links, uploads og andet brugergenereret indhold;**
- **Overvågning af hastighedsgrænser og brugstærskler for nøglefunktioner;**
- **Risikovurdering baseret på historiske data;**
- **Forhindr levering af phishing, personefterligning og malware via e-mail ved at afvise eller sætte e-mails i karantæ indgående beskeder, der matcher automatiserede trusselskontroller;**
- **Forhindr adgang til ondsindede webdestinationer ved at blokere DNS-opløsning og/eller webtrafik for domæner og kategorier forbundet med malware, phishing, DGA'er og kommando-og-kontrol; og**
- **Registrer og bloker netværksbaserede angreb (f.eks. brute-force-forsøg, omdømmebaserede blokeringer, sårbarhedsscanning og udnyttelsesmønstre) ved hjælp af IPS-signaturer og firewallpolitik.**

Brug af SPF/DKIM/DMARC e-mail-godkendelse til at reducere spoofing af Awaze-domæner og forbedre detektion og afvisning af personefterligning og phishing-e-mails.

Indikatorer for nøjagtighed og mulig fejlrate

Tilliden til vores værktøjer er stærk, med en lav andel af falsk positive resultater. Kunder kan dog klage til vores supportteam, hvis de mener, at der har været en falsk positiv i vores indholdsmodereringsprocesser eller værktøjer til bekæmpelse af misbrug.

E-mail: Registreringer drives af automatiseret trusselsinformation, godkendelsestjek, indholdsanalyse og malwarescanning. Falske positiver kan forekomme (f.eks. legitime masseafsendere eller nyregistrerede domæner) og afbødes gennem tilladelseslister, politikjustering og gennemgang af meddelelser i karantæne/afvist.

Web/DNS: DNS- og firewallblokeringer er afhængige af trusselsfeeds, kategorisering, adfærdsindikatorer (f.eks. DGA-detektion) og IPS-signaturer. Falske positiver kan forekomme (f.eks. forkert kategoriserede domæner eller delt infrastruktur) og håndteres via undtagelser/tilladelseslister og periodisk regeljustering.

Awaze gennemgår tendenser og justerer politikker, når det er nødvendigt, for at reducere falske positiver, samtidig med at beskyttelsen opretholdes.

- **Arbejdsområder skal bestå en anti-misbrugsvurdering, før de kan benytte sig af mange funktioner, især dem, der tillader udgående kommunikation.**
- **Hastighedsbegrænsning, indholdsscanning og spammønsterdetektion er på plads på tværs af mange kanaler vores produkt**
- **Hvis indholdet ikke er i strid med vores vilkår, men en kunde ønsker at administrere sit arbejdsområde i henhold til sine egne vilkår, kan de fjerne indhold eller blokere brugere, som de finder passende.**
- **Manuelle tilsidesættelser fra kundesupport (CS) er tilgængelige for automatiserede blokke.**
- **Awaze-medarbejdere (f.eks. kundesupport) har værktøjer til at godkende eller afvise genindsættelse for blokerede e-mailforsøg.**
- **Vi anvender lagdelte kontroller (e-mailgateway + DNS-filtrering + firewall + IPS), så der ikke er én enkelt kontrol udelukkende stolet på.**
- **Vi bruger tilladelseslister/undtagelser (hvor det er berettiget), og vi finjusterer politikker baseret på operationelle påvirkning og sikkerhedsrisiko.**
- **Vi opbevarer revisionslogfiler og rapportering af sikkerhedshændelser for at understøtte undersøgelse og håndtering af hænd**
- **Sikkerhedspolitikker og detektionsfunktioner vedligeholdes gennem leverandøropdateringer og interne anmeldelse**

Vi anvender e-mail-godkendelse på domæneniveau (SPF, DKIM og DMARC) som en ekstra sikkerhedsforanstaltning for at reducere spoofing og forbedre pålideligheden af automatiserede e-mail-filtreringsbeslutninger.

6. Modtagne klager

Antal klager, vi har modtaget via vores interne klagehåndteringssystemer

Intern klagemekanisme

Antal indgivne klager	**0**
Klagens grundlag	ikke tilgængelig
Afgørelser truffet efter en klage	ikke tilgængelig
Median tid til behandling af klage	ikke tilgængelig