awaze

LOV OM DIGITALE TJENESTER

Åpenhetsrapport

for rapporteringsperioden som slutter i desember 2025

Rapport publisert: 17. februar 2026

1. Innledning

Denne åpenhetsrapporten er utarbeidet i samsvar med artikkel 15 i forordning (EU) 2022/2065, loven om digitale tjenester (DSA). Den beskriver våre innholdsmodereringspraksiser og håndhevingsbeslutninger knyttet til spesifikke produktområder, og har som mål å gi tydelig, tilgjengelig og omfattende informasjon om hvordan vi administrerer og modererer innhold på plattformen vår.

Denne rapporten dekker spesifikt modereringstiltak og -prosedyrer som brukes på følgende produkter: Awaze Groups nettplattformer og digitale tjenester som forenkler oppføring, oppdagelse og bestilling av korttidsferieinnkvartering, inkludert brukergenerert innhold som eiendomsoppføringer, beskrivelser, bilder, anmeldelser og relatert kommunikasjon.

Denne rapporten er en del av vår løpende forpliktelse til åpenhet, ansvarlighet og overholdelse av forpliktelsene som er fastsatt i DSA.

Navn på tjenesteleverandør	Denne rapporten dekker følgende juridiske enheter i Awaze Group: Novasol, Fincallorca, Ardennes Étape og SandyBlue – Samlet sett «Awaze-gruppen»
Dato for publisering av rapporten	**17. februar 2026**
Publiseringsdato for den siste forrige rapporten	**17. februar 2025**
Startdato for rapporteringsperioden	**1. januar 2025**
Sluttdato for rapporteringsperioden	**31. desember 2025**

2. Ordrer mottatt fra myndighetene i EU-medlemsstatene

I samsvar med artikkel 9 og 10 i DSA inneholder denne delen informasjon om pålegg mottatt fra kompetente myndigheter i EU-medlemsstater i rapporteringsperioden. Disse påleggene gjelder ulovlig innhold og forespørsler om informasjon.

2.1. Pålegg om å gripe inn på ulovlig innhold fra myndighetene i medlemsstatene

Type ulovlig innhold	Antall mottatte bestillinger	Medlemsstat som utsteder ordre	Median tid for å bekrefte mottak	Median tid for å iverksette ordren
Dyrevelferd	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Brudd på forbrukerinformasjon	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Nettvold	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Brudd på databeskyttelse og personvern	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Ulovlig eller skadelig tale	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Krenkelser av immaterielle rettigheter	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Negative effekter på samfunnsdebatt eller valg	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Beskyttelse av mindreårige	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Risiko for offentlig sikkerhet	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Svindel/svindel	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Selvskading	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Usikre, ikke-samsvarende eller forbudte produkter	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Vold	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Type ulovlig innhold ikke spesifisert av myndigheten	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Alle andre typer	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Total:	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt

2.2 Pålegg om å gi informasjon om tjenestemottakere fra myndighetene i medlemsstatene

Rapporter årsak/type ulovlig innhold	Antall mottatte varsler	Antall varsler mottatt av betrodde varslere	Antall tiltak iverksatt etter varsler	Antall behandlet utelukkende av automatiserte betyr	Median tid til å iverksette tiltak
Dyrevelferd	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Brudd på forbrukerinformasjon	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Brudd på databeskyttelse og personvern	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Ulovlig eller skadelig tale 0		Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Krenkelser av immaterielle rettigheter	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Negative effekter på samfunnsdebatt eller valg	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Beskyttelse av mindreårige	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Risiko for offentlig sikkerhet 0		Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Svindel/svindel	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Selvskading	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Usikre, ikke-samsvarende eller forbudte produkter	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Vold	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Type ulovlig innhold ikke spesifisert av myndigheten	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Alle andre typer	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Total:	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt

3. Brukerrapporter/-meldinger

Denne delen beskriver antallet og typen rapporter som er sendt inn av brukere, andre enkeltpersoner og enheter angående innhold de mener er ulovlig eller i strid med plattformens vilkår og betingelser. I tillegg beskriver den hvordan vi håndterer innholdsmodereringstiltak som svar på brukerrapporter.

Rapporter mottatt fra brukere

Rapporter årsak/type ulovlig innhold	Antall mottatte varsler	Antall varsler mottatt av betrodde varslere	Antall tiltak iverksatt etter varsler	Antall behandlet utelukkende av automatiserte betyr	Median tid til å iverksette tiltak
Dyrevelferd	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Brudd på forbrukerinformasjon	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Brudd på databeskyttelse og personvern	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Ulovlig eller skadelig tale 0		Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Krenkelser av immaterielle rettigheter	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Negative effekter på samfunnsdebatt eller valg	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Beskyttelse av mindreårige	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Risiko for offentlig sikkerhet 0		Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Svindel/svindel	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Selvskading	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Usikre, ikke-samsvarende eller forbudte produkter	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Vold	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Type ulovlig innhold ikke spesifisert av myndigheten	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Alle andre typer	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
Total:	0	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt

4. Innholdsmoderering utført på Awazes eget initiativ

Awaze er forpliktet til å opprettholde et trygt, sikkert og misbruksfritt miljø for både kundene våre og sluttbrukerne deres. Som leverandør av kundeserviceplattformer lar plattformen vår bedrifter kommunisere med brukere via meldinger, e-post og integrasjoner – som alle har potensial for misbruk hvis de ikke beskyttes på riktig måte.

Vi bruker en lagdelt tilnærming til innholdsmoderering, som kombinerer automatiserte deteksjonssystemer, interne administrasjonsverktøy og manuelle gjennomgangsprosesser. Denne delen gir en oversikt over innholdsmodereringshandlinger som er utført på eget initiativ, uten noen juridisk forpliktelse eller varsel til tredjepart.

Moderering utført på eget initiativ inkluderer både proaktiv deteksjon ved hjelp av automatiserte systemer og manuell gjennomgang av innholdsmoderatorer. Vi er forpliktet til å sikre at alle ansatte som er involvert i innholdsmoderering er utstyrt med nødvendige ferdigheter, kunnskaper og ressurser for å utføre sine oppgaver rettferdig, nøyaktig og i tråd med gjeldende lover og interne retningslinjer.

Innholdsmoderering på eget initiativ

Type ulovlig innhold eller annet brudd på AUP	Antall modererte elementer	Antall av disse elementene som ble oppdaget utelukkende ved hjelp av automatiserte betyr	Type begrensning som er pålagt
Svindel/svindel	Innkommende e-poster filtrert: 2 691 775 (årlig; inkluderer 52 046 registreringer av etterligning) Ondsinnede lenker funnet: 1135 usikre URL-klikk oppdaget (e-post) + 98 262 DNS-beskyttelseshendelser blokkert (nett, inkl. 7165 phishing) Skadelige opplastinger funnet: 1010 innkommende skadevaredeteksjoner (e-post)	Innkommende e-poster filtrert: 2 691 775 Ondsinnede lenker funnet: 1135 (e-post) + 98 262 (nett) Skadelige opplastinger funnet: 1010	Synlighetsbegrensning: E-poster er satt i karantene/ blokkert; nettforespørsler blokkeres av DNS-filtrering / brannmurpolicy. Fjerning av innhold: Innkommende e-poster kan avvises (ikke leveres) når de samsvarer med spam/ Kontroller for skadelig programvare/etterligning. Kontosuspensjon: Brukes ikke av disse kontrollene (håndteres via separate HR-/IT-prosesser der det er nødvendig).
Andre typer brudd på plattformens vilkår og betingelser	Totalt antall spamklager: 96 665 (Spamavvisning – sikker e-postgateway; årlig stabil estimat)	Automatiserte spamklager: 96 665 (automatisk spamdeteksjon ved den sikre e-postgatewayen)	Suspender plattformtillatelser: Ikke aktuelt. Dette er avvisninger av e-postgatewayer, ikke håndhevingstiltak for plattformen.
Total:	191 072	197 072	Ikke aktuelt

4. Kvalitativ beskrivelse av de automatiserte metodene

Awaze bruker automatiserte sikkerhetskontroller for å redusere svindel, phishing, identitetstyveri og skadelig programvare på tvers av e-post og nettilgang.

E-postbeskyttelse: Vi bruker en sikker e-postgateway (Mimecast) for å inspisere innkommende e-post før den leveres. Gatewayen bruker automatiserte kontroller (omdømme, autentisering, innholdsanalyse, skanning etter skadelig programvare og deteksjon av etterligning) for å avvise eller sette meldinger knyttet til svindel/svindel, etterligning eller skadelig programvare i karantene. Vi bruker også e-postautentiseringskontroller på tvers av domenene våre (SPF, DKIM og DMARC). Disse kontrollene hjelper mottakssystemer med å bekrefte at meldinger som hevder å komme fra Awaze-domener er autoriserte og ikke har blitt endret, og de reduserer forfalskning av domener og forsøk på etterligning.

Nettbeskyttelse: Vi bruker en administrert SD-WAN-sikkerhetstjeneste (Cato) som bruker DNS-filtrering, brannmurpolicy og inntrengingsforebygging. Dette blokkerer tilgang til kjente ondsinnede domener, phishing-infrastruktur og kommando- og kontrolldestinasjoner, og det blokkerer høyrisikotrafikkmønstre i nettverkskanten.

Rapporteringsmerknad: Årstallene er estimert ved bruk av leverandørrapporteringsvinduer (Mimecast aug.–des. 2025; Cato 12. okt.–31. des. 2025) og forutsetter stabil tilstand uten endringer i policy eller volumendring.

Presise formål

De automatiserte verktøyene har som mål å beskytte innkommende og utgående meldingsaktivitet, forhindre misbruk, opprettholde avsenderens omdømme og sikre samsvar med retningslinjer og lovgivning (f.eks. retningslinjer for e-postsending, samsvar med CAN-SPAM). Spesifikke formål inkluderer:

- **Oppdage mistenkelig aktivitet og mønstre under registrering;**
- **Evaluering av innhold ved opprettelse og tilgang på tvers av lenker, opplastinger og annet brukergenerert innhold;**
- **Overvåking av hastighetsgrenser og brukterskler for viktige funksjoner;**
- **Scoring av risiko basert på historiske data;**
- **Forhindre levering av phishing, etterligning og skadelig programvare via e-post ved å avvise eller sette i karantene innkommende meldinger som samsvarer med automatiserte trusselkontroller;**
- **Forhindre tilgang til ondsinnede nettdestinasjoner ved å blokkere DNS-oppløsning og/eller nettrafikk for domener og kategorier knyttet til skadevare, phishing, DGA-er og kommando-og-kontroll; og**
- **Oppdag og blokker nettverksbaserte angrep (for eksempel brute force-forsøk, omdømmebaserte blokkeringer, sårbarhetsskanning og utnyttelsesmønstre) ved hjelp av IPS-signaturer og brannmurpolicy.**

Bruk av SPF/DKIM/DMARC e-postautentisering for å redusere forfalskning av Awaze-domener og forbedre deteksjon og avvisning av personifisering og phishing-e-poster.

Indikatorer for nøyaktighet og mulig feilrate

Vi har stor tillit til verktøyene våre, med en lav andel falske positive resultater. Kunder kan imidlertid klage til supportteamet vårt hvis de mener at det har vært en falsk positiv feil i innholdsmodereringsprosessene våre eller verktøyene mot misbruk.

E-post: Deteksjoner drives av automatisert trusselinformasjon, autentiseringskontroller, innholdsanalyse og skanning etter skadelig programvare. Falske positiver kan forekomme (for eksempel legitime massesendere eller nyregistrerte domener) og reduseres gjennom tillatelseslister, justering av retningslinjer og gjennomgang av meldinger i karantene/avvist.

Web/DNS: DNS- og brannmurblokkeringer er avhengige av trusselfeeder, kategorisering, atferdsindikatorer (for eksempel DGA-deteksjon) og IPS-signaturer. Falske positiver kan forekomme (for eksempel feilkategoriserte domener eller delt infrastruktur) og håndteres via unntak/tillatelseslister og periodisk regeljustering.

Awaze gjennomgår trender og justerer retningslinjer når det er nødvendig for å redusere falske positiver, samtidig som beskyttelsen opprettholdes.

- **Arbeidsområder må bestå en vurdering for å motvirke misbruk før de kan benytte seg av mange funksjoner, spesielt de som tillater utgående kommunikasjon.**
- **Hastighetsbegrensning, innholdsskanning og spammønsterdeteksjon er på plass på tvers av mange kanaler vårt produkt**
- **Hvis innholdet ikke er i strid med våre vilkår, men en kunde ønsker å administrere arbeidsområdet sitt i henhold til sine egne vilkår, kan de fjerne innhold eller blokkere brukere etter eget ønske.**
- **Manuelle overstyringer fra kundestøtte (CS) er tilgjengelige for automatiserte blokkeringer.**
- **Awaze-ansatte (f.eks. kundestøtte) har verktøy for å godkjenne eller avslå gjeninnsetting av blokkerte e-postforsøk.**
- **Vi bruker lagdelte kontroller (e-postgateway + DNS-filtrering + brannmur + IPS) slik at ingen enkelt kontroll er nødv utelukkende stolt på.**
- **Vi bruker tillatelseslister/unntak (der det er berettiget), og vi finjusterer retningslinjer basert på driftsmessige påvirkning og sikkerhetsrisiko.**
- **Vi fører revisjonslogger og rapportering av sikkerhetshendelser for å støtte etterforskning og hendelsesrespons.**
- **Sikkerhetspolicyer og deteksjonsfunksjoner vedlikeholdes gjennom leverandøroppdateringer og interne anmeldelse**

Vi bruker e-postautentisering på domenenivå (SPF, DKIM og DMARC) som en ekstra sikkerhetsforanstaltning for å redusere forfalskning og forbedre påliteligheten til automatiserte e-postfiltreringsbeslutninger.

6. Mottatte klager

Antall klager vi mottok gjennom våre interne klagebehandlingssystemer

Intern klagemekanisme

Antall innleverte klager	**0**
Klagens grunnlag	Ikke aktuelt
Avgjørelser tatt etter en klage	Ikke aktuelt
Median tid for å behandle klagen	Ikke aktuelt