LAGEN OM DIGITALA TJÄNSTER

Transparensrapport

för rapporteringsperioden som slutar i december 2025

Rapport publicerad: 17 februari 2026

1. Introduktion

Denna transparensrapport har utarbetats i enlighet med artikel 15 i förordning (EU) 2022/2065, lagen om digitala tjänster (DSA). Den beskriver våra metoder för innehållsmoderering och verkställighetsbeslut som rör specifika produktområden och syftar till att ge tydlig, tillgänglig och omfattande information om hur vi hanterar och modererar innehåll på vår plattform.

Denna rapport behandlar specifikt modereringsåtgärder och procedurer som tillämpas på följande produkter: Awaze Groups onlineplattformar och digitala tjänster som underlättar listning, upptäckt och bokning av korttidsboende, inklusive användargenererat innehåll såsom fastighetsannonser, beskrivningar, bilder, recensioner och relaterad kommunikation.

Denna rapport är en del av vårt fortsatta engagemang för transparens, ansvarsskyldighet och efterlevnad av de skyldigheter som anges i DSA.

Namn på tjänsteleverantör	Denna rapport omfattar följande juridiska enheter inom Awaze Group: Novasol, Fincallorca, Ardennes Étape och SandyBlue - Tillsammans "Awaze-gruppen"
Datum för rapportens publicering	**17 februari 2026**
Publiceringsdatum för den senaste föregående rapporten	**17 februari 2025**
Rapporteringsperiodens startdatum	**1 januari 2025**
Slutdatum för rapporteringsperioden	**31 december 2025**

2. Order mottagna från myndigheter i EU:s medlemsstater

I enlighet med artiklarna 9 och 10 i DSA innehåller detta avsnitt information om beslut som mottagits från behöriga myndigheter i EU:s medlemsstater under rapporteringsperioden. Dessa beslut avser olagligt innehåll och begäranden om information.

2.1. Beslut om att vidta åtgärder mot olagligt innehåll från medlemsstaternas myndigheter

Typ av olagligt innehåll	Antal mottagna beställningar	Medlemsstat som utfärdar order	Median tid för att bekräfta mottagandet	Median tid för att verkställa beslutet
Djurskydd	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Intrång i konsumentinformation	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Cybervåld	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Dataskydd och integritetsintrång	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Olagligt eller skadligt tal	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Intrång i immateriella rättigheter	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Negativa effekter på samhällsdebatt eller val	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Skydd av minderåriga	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Risk för allmän säkerhet	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Bedrägerier/bedrägerier	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Självskadebeteende	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Osäkra, icke-kompatibla eller förbjudna produkter	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Våld	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Typ av olagligt innehåll som inte specificerats av myndigheten	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Alla andra typer	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Total:	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt

2.2 Föreläggande om att lämna information om tjänstemottagare från medlemsstaternas myndigheter

Rapportera orsak/typ av olagligt innehåll	Antal mottagna meddelanden	Antal meddelanden mottagna av betrodda flaggare	Antal vidtagna åtgärder till följd av meddelanden	Antal bearbetas enbart automatiserat medel	Median tid för att vidta åtgärder
Djurskydd	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Intrång i konsumentinformation	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Dataskydd och integritetsintrång	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Olagligt eller skadligt tal 0		Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Intrång i immateriella rättigheter	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Negativa effekter på samhällsdebatt eller val	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Skydd av minderåriga	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Risk för allmän säkerhet 0		Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Bedrägerier/bedrägerier	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Självskadebeteende	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Osäkra, icke-kompatibla eller förbjudna produkter	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Våld	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Typ av olagligt innehåll som inte specificerats av myndigheten	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Alla andra typer	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Total:	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt

3. Användarrapporter/meddelanden

Det här avsnittet beskriver antalet och typen av rapporter som lämnats in av användare, andra individer och enheter gällande innehåll som de anser vara olagligt eller bryter mot vår plattforms villkor. Dessutom beskriver det hur vi hanterar innehållsmodereringsåtgärder som svar på användarrapporter.

Rapporter mottagna från användare

Rapportera orsak/typ av olagligt innehåll	Antal mottagna meddelanden	Antal meddelanden mottagna av betrodda flaggare	Antal vidtagna åtgärder till följd av meddelanden	Antal bearbetas enbart automatiserat medel	Median tid för att vidta åtgärder
Djurskydd	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Intrång i konsumentinformation	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Dataskydd och integritetsintrång	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Olagligt eller skadligt tal 0		Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Intrång i immateriella rättigheter	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Negativa effekter på samhällsdebatt eller val	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Skydd av minderåriga	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Risk för allmän säkerhet 0		Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Bedrägerier/bedrägerier	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Självskadebeteende	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Osäkra, icke-kompatibla eller förbjudna produkter	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Våld	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Typ av olagligt innehåll som inte specificerats av myndigheten	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Alla andra typer	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Total:	0	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt

4. Innehållsmoderering utförd på Awazes eget initiativ

Awaze strävar efter att upprätthålla en säker, trygg och missbruksfri miljö för både våra kunder och deras slutanvändare. Som leverantör av kundtjänstplattformar gör vår plattform det möjligt för företag att interagera med användare via meddelanden, e-post och integrationer – vilka alla medför potential för missbruk om de inte skyddas ordentligt.

Vi använder en flerskiktad metod för innehållsmoderering, som kombinerar automatiserade detekteringssystem, interna administrationsverktyg och manuella granskningsprocesser. Det här avsnittet ger en översikt över innehållsmodereringsåtgärder som vidtas på eget initiativ, utan någon rättslig skyldighet eller meddelande till tredje part.

Moderering som utförs på eget initiativ omfattar både proaktiva upptäckter med hjälp av automatiserade system och manuell granskning av innehållsmoderatorer. Vi strävar efter att säkerställa att all personal som är involverad i innehållsmoderering har de färdigheter, kunskaper och resurser som krävs för att utföra sina uppgifter rättvist, korrekt och i enlighet med gällande lagar och interna policyer.

Innehållsmoderering på eget initiativ

Typ av olagligt innehåll eller annan överträdelse av AUP	Antal modererade objekt	Antal av dessa objekt som upptäckts enbart med hjälp av automatiserade metoder	Typ av tillämpad begränsning
Bedrägerier/bedrägerier	Inkommande e-postmeddelanden filtrerade: 2 691 775 (årsvis; inkluderar 52 046 identifieringar av identitetsstölder) Skadliga länkar hittades: 1 135 osäkra URL-klick upptäckta (e-post) + 98 262 DNS-skyddshändelser blockerade (webb, inkl. 7 165 nätfiske) Skadliga uppladdningar hittades: 1 010 inkommande skadlig kod upptäckt (e-post)	Inkommande e-postmeddelanden filtrerade: 2 691 775 Skadliga länkar hittades: 1 135 (e-post) + 98 262 (webb) Skadliga uppladdningar hittades: 1 010	Synlighetsbegränsning: E-postmeddelanden är i karantän/ blockerad; webbförfrågningar blockeras av DNS-filtrering/ brandväggspolicy. Borttagning av innehåll: Inkommande e-postmeddelanden kan avvisas (inte levereras) när de matchar skräppost/ Kontroller för skadlig kod/ personifiering. Kontoavstängning: Används inte av dessa kontroller (hanteras via separata HR-/IT-processer där det behövs).
Andra typer av brott mot plattformens villkor	Totalt antal skräppostklagomål: 96 665 (Spamavvisning – säker e-postgateway; årlig uppskattning i stabilt tillstånd)	Automatiserade skräppostklagomål: 96 665 (automatisk skräppostdetektering vid den säkra e-postgatewayen)	Stäng av plattformsbehörigheter: Ej tillämpligt. Dessa är avslag på e-postgateways, inte plattformsåtgärder.
Total:	191 072	197 072	Ej tillämpligt

4. Kvalitativ beskrivning av de automatiserade medlen

Awaze använder automatiserade säkerhetskontroller för att minska bedrägerier, nätfiske, identitetsstöld och skadlig programvara via e-post och webbåtkomst.

E-postskydd: Vi använder en säker e-postgateway (Mimecast) för att inspektera inkommande e-post innan den levereras. Gatewayen använder automatiserade kontroller (rykte, autentisering, innehållsanalys, skanning efter skadlig kod och identifiering av identitetsstölder) för att avvisa eller karantänera meddelanden som är kopplade till bedrägerier/bedrägerier, identitetsstölder eller skadlig kod. Vi använder även e-postautentiseringskontroller över våra domäner (SPF, DKIM och DMARC). Dessa kontroller hjälper mottagande system att verifiera att meddelanden som påstås komma från Awaze-domäner är auktoriserade och inte har ändrats, och de minskar domänförfalskning och identitetsstöldförsök.

Webbskydd: Vi använder en hanterad SD-WAN-säkerhetstjänst (Cato) som tillämpar DNS-filtrering, brandväggspolicy och intrångsskydd. Detta blockerar åtkomst till kända skadliga domäner, nätfiskeinfrastruktur och kommando- och kontrolldestinationer, och det blockerar högrisktrafikmönster vid nätverkskanten.

Rapporteringsanmärkning: Årssiffrorna uppskattas med hjälp av leverantörsrapporteringsfönster (Mimecast aug–dec 2025; Cato 12 okt–31 dec 2025) och antar steady state utan policy- eller volymförändringar.

Precisa syften

De automatiserade verktygen syftar till att skydda inkommande och utgående meddelandeaktivitet, förhindra missbruk, upprätthålla avsändarens rykte och säkerställa efterlevnad av riktlinjer och lagstiftning (t.ex. riktlinjer för e-postutskick, efterlevnad av CAN-SPAM). Specifika syften inkluderar:

- **Upptäcka misstänkt aktivitet och misstänkta mönster under registrering;**
- **Utvärdera innehåll vid skapande och åtkomst via länkar, uppladdningar och annat användargenererat innehåll;**
- **Övervakning av hastighetsgränser och användningströsklar för viktiga funktioner;**
- **Riskbedömning baserad på historisk data;**
- **Förhindra leverans av nätfiske, identitetsstöld och skadlig kod via e-post genom att avvisa eller sätta i karantän inkommande meddelanden som matchar automatiserade hotkontroller;**
- **Förhindra åtkomst till skadliga webbdestinationer genom att blockera DNS-upplösning och/eller webbtrafik för domäner och kategorier associerade med skadlig kod, nätfiske, DGA:er och kommando- och kontrollsystem; och**
- **Upptäck och blockera nätverksbaserade attacker (till exempel brute force-försök, ryktesbaserade blockeringar, sårbarhetsskanning och exploitmönster) med hjälp av IPS-signaturer och brandväggspolicy.**

Användning av SPF/DKIM/DMARC e-postautentisering för att minska förfalskning av Awaze-domäner och förbättra detektering och avvisning av personifiering och nätfiskemeddelanden.

Indikatorer för noggrannhet och möjlig felfrekvens

Förtroendet för våra verktyg är starkt, med en låg andel falskt positiva resultat. Kunder kan dock överklaga till vårt supportteam om de tror att det har förekommit ett falskt positivt resultat i våra processer för innehållsmoderering eller verktyg mot missbruk.

E-post: Detekteringar drivs av automatiserad hotinformation, autentiseringskontroller, innehållsanalys och skanning efter skadlig kod. Falska positiva resultat kan förekomma (till exempel legitima massutskick eller nyregistrerade domäner) och minskas genom tillåtelselistning, policyjustering och granskning av karantänsatta/avvisade meddelanden.

Webb/DNS: DNS- och brandväggsblockeringar är beroende av hotflöden, kategorisering, beteendeindikatorer (till exempel DGA-detektering) och IPS-signaturer. Falska positiva resultat kan förekomma (till exempel felkategoriserade domäner eller delad infrastruktur) och hanteras via undantag/tillåtelselistor och regelbunden regeljustering.

Awaze granskar trender och justerar policyer vid behov för att minska falska positiva resultat samtidigt som skyddet bibehålls.

- **Arbetsytor måste genomgå en bedömning mot missbruk innan de kan använda många funktioner, särskilt de som tillåter utgående kommunikation.**
- **Hastighetsbegränsning, innehållsskanning och detektering av skräppostmönster finns på plats i många kanale vår produkt**
- **Om innehållet inte strider mot våra villkor men en kund vill administrera sin arbetsyta enligt sina egna villkor, kan de ta bort innehåll eller blockera användare som de finner lämpligt.**
- **Manuella åsidosättningar av kundsupport (CS) är tillgängliga för automatiserade block.**
- **Awaze-anställda (t.ex. kundsupport) har verktyg för att godkänna eller neka återinsättning för blockerade e-postförsök.**
- **Vi tillämpar kontroller i flera lager (e-postgateway + DNS-filtrering + brandvägg + IPS) så att ingen enskild kontr enbart förlitat sig på.**
- **Vi använder tillåtelselistor/undantag (där det är motiverat) och vi justerar policyer baserat på operativa påverkan och säkerhetsrisk.**
- **Vi för granskningsloggar och rapporterar säkerhetshändelser för att stödja utredningar och incidenter.**
- **Säkerhetspolicyer och detekteringsfunktioner upprätthålls genom leverantörsuppdateringar och interna recension**

Vi använder e-postautentisering på domännivå (SPF, DKIM och DMARC) som en extra skyddsåtgärd för att minska förfalskning och förbättra tillförlitligheten hos automatiserade e-postfiltreringsbeslut.

6. Mottagna klagomål

Antal klagomål vi mottagit via våra interna system för klagomålshantering

Intern klagomålsmekanism

Antal inlämnade klagomål	**0**
Grund för klagomål	Ej tillämpligt
Beslut som fattats efter ett klagomål	Ej tillämpligt
Median tid för att hantera klagomål	Ej tillämpligt