



ZAKON O DIGITALNIM USLUGAMA

Izvješće o transparentnosti

za izvještajno razdoblje koje završava u prosincu 2025.

Izvješće objavljeno: 17. veljače 2026.

1. Uvod

Ovo izvješće o transparentnosti pripremljeno je u skladu s člankom 15. Uredbe (EU) 2022/2065, Zakonom o digitalnim uslugama (DSA). U njemu su opisane naše prakse moderiranja sadržaja i odluke o provedbi koje se odnose na određena područja proizvoda, a cilj mu je pružiti jasne, pristupačne i sveobuhvatne informacije o tome kako upravljamo i moderiramo sadržaj na našoj platformi.

Ovo izvješće posebno obuhvaća moderatorske radnje i postupke primijenjene na sljedeće proizvode: online platforme i digitalne usluge Awaze Grupe koje olakšavaju popisivanje, otkrivanje i rezervaciju kratkoročnog smještaja za odmor, uključujući sadržaj koji generiraju korisnici, kao što su oglasi za nekretnine, opisi, slike, recenzije i srodna komunikacija.

Ovo izvješće dio je naše trajne predanosti transparentnosti, odgovornosti i poštivanju obveza utvrđenih u Zakonu o digitalnim uslugama (DSA).

Naziv pružatelja usluga	Ovo izvješće obuhvaća sljedeće pravne subjekte Awaze Grupe: Novasol, Fincallorca, Ardennes Étape i SandyBlue - Zajedno nazvani „Awaze grupa“
Datum objave izvješća	17. veljače 2026.
Datum objave posljednjeg prethodnog izvješća	17. veljače 2025.
Datum početka izvještajnog razdoblja	1. siječnja 2025.
Datum završetka izvještajnog razdoblja	31. prosinca 2025.

2. Nalozi primljeni od tijela država članica EU-a

U skladu s člancima 9. i 10. Zakona o digitalnim uslugama (DSA), ovaj odjeljak pruža informacije o nalogima primljenim od nadležnih tijela država članica EU tijekom izvještajnog razdoblja. Ti se nalozi odnose na nezakoniti sadržaj i zahtjeve za informacijama.

2.1. Nalozi za djelovanje u vezi s nezakonitim sadržajem od strane tijela država članica

Vrsta ilegalnog sadržaja	Broj primljenih narudžbi	Država članica koja izdaje nalog	Srednje vrijeme za potvrdu primitka	Srednje vrijeme potrebno za provedbu naloga
Dobrobit životinja	0	N/A	N/A	N/A
Kršenje informacija o potrošačima	0	N/A	N/A	N/A
Kibernetičko nasilje	0	N/A	N/A	N/A
Kršenja zaštite podataka i privatnosti	0	N/A	N/A	N/A
Nezakonit ili štetan govor	0	N/A	N/A	N/A
Kršenja intelektualnog vlasništva	0	N/A	N/A	N/A
Negativni učinci na građanski diskurs ili izbore	0	N/A	N/A	N/A
Zaštita maloljetnika	0	N/A	N/A	N/A
Rizik za javnu sigurnost	0	N/A	N/A	N/A
Prijevare/obmana	0	N/A	N/A	N/A
Samoozljeđivanje	0	N/A	N/A	N/A
Nesigurni, neusklađeni ili zabranjeni proizvodi	0	N/A	N/A	N/A
Nasilje	0	N/A	N/A	N/A
Vrsta ilegalnog sadržaja koju nadležno tijelo nije navelo	0	N/A	N/A	N/A
Sve ostale vrste	0	N/A	N/A	N/A
Ukupno:	0	N/A	N/A	N/A

2.2 Nalog za pružanje informacija o primateljima usluge od strane tijela država članica

Razlog prijave/Vrsta ilegalnog sadržaja	Broj primljenih obavijesti	Broj obavijesti koje su primili pouzdani prijavitelji	Broj poduzetih radnji na temelju obavijesti	Br. obrađeno isključivo automatizirano sredstva	Srednje vrijeme za poduzimanje akcije
Dobrobit životinja	0	N/A	N/A	N/A	N/A
Kršenje prava na informacije za potrošače	0	N/A	N/A	N/A	N/A
Kršenja zaštite podataka i privatnosti	0	N/A	N/A	N/A	N/A
Nezakonit ili štetan govor 0		N/A	N/A	N/A	N/A
Kršenja intelektualnog vlasništva	0	N/A	N/A	N/A	N/A
Negativni učinci na građanski diskurs ili izbore	0	N/A	N/A	N/A	N/A
Zaštita maloljetnika	0	N/A	N/A	N/A	N/A
Rizik za javnu sigurnost 0		N/A	N/A	N/A	N/A
Prijevare/obmana	0	N/A	N/A	N/A	N/A
Samoozljeđivanje	0	N/A	N/A	N/A	N/A
Nesigurni, neusklađeni ili zabranjeni proizvodi	0	N/A	N/A	N/A	N/A
Nasilje	0	N/A	N/A	N/A	N/A
Vrsta ilegalnog sadržaja koju nadležno tijelo nije navelo	0	N/A	N/A	N/A	N/A
Sve ostale vrste	0	N/A	N/A	N/A	N/A
Ukupno:	0	N/A	N/A	N/A	N/A

3. Izvješća/obavijesti korisnika

Ovaj odjeljak opisuje broj i prirodu prijave koje su podnijeli korisnici, druge osobe i subjekti u vezi sa sadržajem za koji smatraju da je nezakonit ili da krši uvjete i odredbe naše platforme. Osim toga, opisuje kako postupamo s moderiranjem sadržaja kao odgovor na korisničke prijave.

Izvješća primljena od korisnika

Razlog prijave/Vrsta ilegalnog sadržaja	Broj primljenih obavijesti	Broj obavijesti koje su primili pouzdani prijavitelji	Broj poduzetih radnji na temelju obavijesti	Br. obrađeno isključivo automatizirano sredstva	Srednje vrijeme za poduzimanje radnje
Dobrobit životinja	0	N/A	N/A	N/A	N/A
Kršenje prava na informacije za potrošače	0	N/A	N/A	N/A	N/A
Kršenja zaštite podataka i privatnosti	0	N/A	N/A	N/A	N/A
Nezakonit ili štetan govor 0		N/A	N/A	N/A	N/A
Kršenja intelektualnog vlasništva	0	N/A	N/A	N/A	N/A
Negativni učinci na građanski diskurs ili izbore	0	N/A	N/A	N/A	N/A
Zaštita maloljetnika	0	N/A	N/A	N/A	N/A
Rizik za javnu sigurnost 0		N/A	N/A	N/A	N/A
Prijevare/obmana	0	N/A	N/A	N/A	N/A
Samoozljeđivanje	0	N/A	N/A	N/A	N/A
Nesigurni, neusklađeni ili zabranjeni proizvodi	0	N/A	N/A	N/A	N/A
Nasilje	0	N/A	N/A	N/A	N/A
Vrsta ilegalnog sadržaja koju nadležno tijelo nije navelo	0	N/A	N/A	N/A	N/A
Sve ostale vrste	0	N/A	N/A	N/A	N/A
Ukupno:	0	N/A	N/A	N/A	N/A

4. Moderiranje sadržaja provedeno na Awazeovu vlastitu inicijativu

Awaze je posvećen održavanju sigurnog, zaštićenog i okruženja bez zlouporabe za naše kupce i njihove krajnje korisnike. Kao pružatelj platforme za korisničku podršku, naša platforma omogućuje tvrtkama da komuniciraju s korisnicima putem poruka, e-pošte i integracija - a sve to nosi potencijal za zlouporabu ako nije pravilno zaštićeno.

Koristimo slojevit pristup moderiranju sadržaja, kombinirajući automatizirane sustave za detekciju, interne administratorske alate i ručne procese pregleda. Ovaj odjeljak pruža pregled radnji moderiranja sadržaja poduzetih na vlastitu inicijativu, bez ikakve zakonske obveze ili obavijesti treće strane.

Moderiranje koje se provodi na našu vlastitu inicijativu uključuje proaktivna otkrivanja pomoću automatiziranih sustava i ručni pregled od strane moderatora sadržaja. Posvećeni smo osiguravanju da svi zaposlenici uključeni u moderiranje sadržaja imaju potrebne vještine, znanje i resurse za pravedno, točno i u skladu s važećim zakonima i internim politikama obavljanje svojih dužnosti.

Moderiranje sadržaja na vlastitu inicijativu

Vrsta ilegalnog sadržaja ili drugo kršenje Pravila o korištenju robe	Broj moderiranih stavki	Broj tih predmeta otkrivenih isključivo automatiziranim korištenjem sredstva	Vrsta primijenjenog ograničenja
Prijevare/obmana	Filtriranih dolaznih e-poruka: 2.691.775 (godišnje; uključuje 52.046 detekcija lažnog predstavljanja) Pronađene zlonamjerne poveznice: otkriveno 1135 nesigurnih klikova na URL-ove (e-pošta) + 98.262 blokirana događaja DNS zaštite (web, uklj. 7165 phishinga) Pronađeni zlonamjerni prijenosi: 1010 detekcija dolaznog zlonamjernog softvera (e-pošta)	Filtriranih dolaznih e-poruka: 2.691.775 Pronađene zlonamjerne poveznice: 1.135 (e-pošta) + 98.262 (web) Pronađeni zlonamjerni prijenosi: 1.010	Ograničenje vidljivosti: E-poruke su u karanteni/ blokirano; web zahtjevi su blokirani DNS filtriranjem / pravilima vatrozida. Uklanjanje sadržaja: Dolazne e-poruke mogu se odbiti (neće se isporučiti) kada se podudaraju s neželjenom poštom/ Kontrole zlonamjernog softvera/ lažnog predstavljanja. Suspendizacija računa: Ne koriste se ovim kontrolama (obrađuje se putem zasebnih HR/IT procesa gdje je to potrebno).
Druge vrste kršenja uvjeta korištenja platforme	Ukupno pritužbi na neželjenu poštu: 96.665 (Odbijanje neželjene pošte – sigurni pristupnik za e-poštu; godišnja procjena stabilnog stanja)	Automatizirane pritužbe na neželjenu poštu: 96.665 (automatsko otkrivanje neželjene pošte na sigurnom pristupniku e-pošte)	Obustavljanje dozvola platforme: Nije primjenjivo. Ovo su odbijanja pristupnika e-pošte, a ne mjere provedbe na platformi.
Ukupno:	191.072	197.072	N/A

4. Kvalitativni opis automatiziranih sredstava

Awaze koristi automatizirane sigurnosne kontrole kako bi smanjio prijevare, phishing, lažno predstavljanje i zlonamjerni softver putem e-pošte i web pristupa.

Zaštita e-pošte: Koristimo sigurni pristupnik e-pošte (Mimecast) za pregled dolazne e-pošte prije nego što bude isporučena. Pristupnik koristi automatizirane provjere (ugled, autentifikacija, analiza sadržaja, skeniranje zlonamjernog softvera i otkrivanje lažnog predstavljanja) kako bismo odbacili ili stavili u karantenu poruke povezane s prijevarama/prevarama, lažnim predstavljanjem ili zlonamjernim softverom. Također koristimo kontrole za autentifikaciju e-pošte na svim našim domenama (SPF, DKIM i DMARC). Ove kontrole pomažu prijemnim sustavima da provjere jesu li poruke za koje se tvrdi da dolaze s Awaze domena autorizirane i da nisu izmijenjene te smanjuju pokušaje lažiranja domene i lažnog predstavljanja.

Web zaštita: Koristimo upravljano SD-WAN sigurnosnu uslugu (Cato) koja primjenjuje DNS filtriranje, pravila vatrozida i sprječavanje upada. To blokira pristup poznatim zlonamjernim domenama, phishing infrastrukturi i odredištima za upravljanje i kontrolu te blokira obrasce prometa visokog rizika na rubu mreže.

Napomena o izvješćivanju: Godišnje brojke procjenjuju se korištenjem izvještajnih okvira dobavljača (Mimecast kolovoz – prosinac 2025.; Cato 12. listopada – 31. prosinca 2025.) i pretpostavljaju stabilno stanje bez promjene politike ili obujma.

Precizne svrhe

Automatizirani alati imaju za cilj zaštititi dolazne i odlazne poruke, spriječiti zlouporabu, održati ugled pošiljatelja i osigurati usklađenost sa smjernicama i zakonodavstvom (npr. smjernice za slanje e-pošte, usklađenost s CAN-SPAM-om). Specifične svrhe uključuju:

- Otkrivanje sumnjivih aktivnosti i obrazaca tijekom registracije;
- Procjena sadržaja prilikom stvaranja i pristupa putem poveznica, prijenosa i ostalog sadržaja koji generiraju korisnici;
- Praćenje ograničenja brzine i pragova korištenja za ključne značajke;
- Rizik bodovanja na temelju povijesnih podataka;
- Spriječite slanje phishinga, lažnog predstavljanja i zlonamjernog softvera putem e-pošte odbijanjem ili stavljanjem u karantenu dolazne poruke koje odgovaraju automatiziranim kontrolama prijetnji;
- Spriječite pristup zlonamjernim web odredištima blokiranjem DNS razrješenja i/ili web prometa za domene i kategorije povezane sa zlonamjernim softverom, phishingom, DGA-ovima i sustavom zapovijedanja i kontrole; i
- Otkrivanje i blokiranje napada temeljenih na mreži (na primjer, pokušaji grube sile, blokiranja temeljena na reputaciji, skeniranje ranjivosti i obrasci iskorištavanja) korištenjem IPS potpisa i pravila vatrozida.

Korištenje SPF/DKIM/DMARC autentifikacije e-pošte za smanjenje lažiranja Awaze domena i poboljšanje otkrivanja i odbacivanja lažnog predstavljanja i phishing e-poruka.

Pokazatelji točnosti i moguće stope pogreške

Povjerenje u naše alate je veliko, s niskom stopom lažno pozitivnih rezultata. Međutim, korisnici se mogu žaliti našem timu za podršku ako smatraju da je došlo do lažno pozitivnog rezultata u našim procesima moderiranja sadržaja ili alatima za sprječavanje zlouporabe.

E-pošta: Detekcija se provodi automatiziranim obavještajnim podacima o prijetnjama, provjerama autentifikacije, analizom sadržaja i skeniranjem zlonamjernog softvera. Lažno pozitivni rezultati mogu se pojaviti (na primjer, legitimni pošiljatelji masovne pošte ili novoregistrirane domene) i ublažavaju se stavljanjem na popis dopuštenih, podešavanjem pravila i pregledom poruka u karanteni/odbijenih poruka.

Web/DNS: DNS i firewall blokovi oslanjaju se na informacije o prijetnjama, kategorizaciju, pokazatelje ponašanja (na primjer, otkrivanje DGA) i IPS potpise. Mogu se pojaviti lažno pozitivni rezultati (na primjer, pogrešno kategorizirane domene ili dijeljena infrastruktura) i njima se upravlja putem iznimki/dopuštenih popisa i periodičnog podešavanja pravila.

Awaze pregledava trendove i prilagođava pravila kada je potrebno kako bi se smanjio broj lažno pozitivnih rezultata uz održavanje zaštite.

- Radni prostori moraju proći procjenu protiv zlouporabe prije nego što mogu koristiti mnoge značajke, posebno one koje omogućuju odlaznu komunikaciju.
- Ograničavanje brzine, skeniranje sadržaja i otkrivanje obrazaca neželjene pošte na snazi su na mnogim kanalima naš proizvod
- Ako sadržaj nije protivan našim uvjetima, ali korisnik želi upravljati svojim radnim prostorom prema vlastitim uvjetima, može ukloniti sadržaj ili blokirati korisnike kako smatra prikladnim.
- Za automatizirane blokove dostupna su ručna poništavanja od strane korisničke podrške (CS).
- Zaposlenici Awazea (npr. korisnička podrška) imaju alate za odobravanje ili odbijanje ponovnog pristupanja blokiranim korisnicima pokušaji slanja e-pošte.
- Primjenjujemo slojevite kontrole (e-mail pristupnik + DNS filtriranje + vatrozid + IPS) tako da nijedna kontrola nije isključivo se oslanjao.
- Koristimo popis dopuštenih/iznimke (gdje je to opravdano) i prilagođavamo pravila na temelju operativnih utjecaj i sigurnosni rizik.
- Vodimo zapisnike revizije i izvješća o sigurnosnim događajima kako bismo podržali istragu i odgovor na incidente.
- Sigurnosne politike i mogućnosti detekcije održavaju se putem ažuriranja dobavljača i internih pregled

Kao dodatnu zaštitu primjenjujemo autentifikaciju e-pošte na razini domene (SPF, DKIM i DMARC) kako bismo smanjili lažiranje i poboljšali pouzdanost automatiziranih odluka o filtriranju e-pošte.

6. Primljene pritužbe

Broj pritužbi koje smo primili putem naših internih sustava za rješavanje pritužbi

Interni mehanizam za pritužbe

Broj podnesenih pritužbi	0
Osnova pritužbe	N/A
Odluke donesene nakon pritužbe	N/A
Srednje vrijeme za rješavanje pritužbe	N/A