



Проектни партнери;



digiQ



anthro p o l i s



Co-funded by
the European Union



Материјал за организации за младинска работа

Како да добиете статус на доверлив известувач за пријавување говор на омраза

Вовед: Што е статус на доверлив известувач и зошто е важен

Според Законот за дигитални услуги (DSA), организациите од граѓанското општество можат да аплицираат за да станат **Доверливи означувачи** - официјално признати субјекти чии пријави за нелегална содржина (вклучувајќи говор на омраза) мора да добијат **приоритетен третман** од страна на онлајн платформите. Доверливите означувачи имаат подобрени канали за пријавување, побрзо време на преглед и структуриран однос со двете платформи и националниот **координатор за дигитални услуги (DSC)**.

За организациите за младинска работа, особено оние кои се занимаваат со говор на омраза, сајбер малтретирање, дискриминација, онлајн вознемирување или заштита на ранливи групи, статусот на доверлив известувач може значително да го зголеми нивното влијание. Многу невладини организации кои работат со млади веќе поднесуваат извештаи до социјалните мрежи, но без посебно признание, нивните извештаи минуваат низ бавни или неконзистентни процеси на преглед. Како доверлив известувач, извештаите на вашата организација се третираат со зголемен кредибилитет и итност, што овозможува штетната содржина што влијае на младите луѓе да се отстрани побрзо и посигурно.

Младинските организации исто така играат уникатно важна улога: тие имаат пристап до реални искуства на млади корисници, го разбираат еволутивниот онлајн јазик (сленг, кодирани термини, мемеа) и често се меѓу првите што забележуваат нови форми на говор на омраза или вознемирување. Статусот на доверлив известувач помага да се формализира оваа експертиза и да се интегрира во поширокиот екосистем за безбедност на интернет.

Овој прирачник објаснува кои се критериумите, како да ја подготвите вашата организација, како да аплицирате и какви одговорности треба да бидете подготвени да преземете откако ќе бидете признати.

Разбирање на критериумите за доверлив означувач



Законот за дигитални услуги утврдува јасни критериуми за станување доверлив означувач. Младинските организации треба да проценат дали ги исполнуваат - или можат да изградат - потребниот капацитет пред да аплицираат.

1. Докажана експертиза во релевантна област

Вашата организација мора да покаже континуирано искуство во областите поврзани со нелегален говор на омраза, штетна содржина, заштита на младите, онлајн безбедност или дигитално граѓанство. Ова вклучува искуство како што се водење портал за пријавување, водење програми против говор на омраза, спроведување мониторинг или истражување, справување со случаи на онлајн вознемирување или обезбедување поддршка на маргинализирани групи погодени од говор на омраза.

2. Независност и политичка неутралност

Доверливите означувачи мора да бидат независни од политичко влијание и треба да покажат дека нивното донесување одлуки е водено од експертиза, а не од политички агенди. Младинските организации треба да имаат транспарентно сопствеништво, структури на управување и да не се поврзани со партии.

3. Силни процедури за известување и верификација

Вашата организација мора да има внатрешни системи за да потврди дека пријавената содржина е нелегална или штетна според законите на ЕУ или националните закони за говор на омраза. Ова бара обучен персонал, јасен механизам за ескалација и можност за документирање на докази (URL-адреси, снимки од екранот, објаснувања на контекстот, временски печати).

4. Способност за систематска обработка на извештаи

Доверливите означувачи мора професионално и доследно да ракуваат со значителен број пријави. Ќе ви треба одржлив работен тек за примање, оценување и препраќање на случаи. Ова може да вклучува алатки за управување со случаи, внатрешни упатства, процеси за обезбедување квалитет и персонал обучен за класификација на говор на омраза.

5. Усогласеност со правилата за заштита на податоци и приватност

Бидејќи вашата организација ќе обработува чувствителна содржина што вклучува млади луѓе, мора да покажете усогласеност со GDPR. Ова вклучува минимизирање на податоци, анонимизација, безбедно складирање и јасни политики за задржување.

6. Интегритет и точност на известувањето

Платформите и DSC очекуваат висока точност. Мора да бидете способни да разликувате нелегален говор на омраза (како што е дефинирано со закон) од штетни, но законски изрази. Јасни внатрешни критериуми, правни консултации и обука на персоналот ќе бидат од суштинско значење.



Доколку вашата организација може да ги исполни овие критериуми - или е подготвена да ги развие - можете да продолжите со аплицирањето.

Подготовка на вашата организација за апликацијата

Процесот на аплицирање бара демонстрирање на капацитет, експертиза и внатрешни структури. Пред да аплицираат, младинските организации треба да ги подготват следниве елементи:

1. Документирајте го вашето искуство и експертиза

Подгответе досие во кое ќе ја сумирате вашата работа поврзана со говорот на омраза и заштитата на младите. Ова може да вклучува:

- описи на релевантни програми (против малтретирање, спречување на говор на омраза, дигитално граѓанско образование)
- годишни извештаи
- статистика за обработени случаи
- претходна соработка со платформи или власти
- истражувања или публикации за штети на интернет

Јасната документација го зајакнува вашиот кредибилитет и му покажува на DSC дека го разбирате дигиталниот ризик.

2. Создавање или ажурирање на протоколи за известување

Доверливиот известувач мора да користи структурирани механизми за известување. Подгответе или усовршете внатрешни протоколи што вклучуваат:

- процес на верификација за секој извештај
- категории на нелегална содржина
- стандарди за документација (слики од екранот, метаподатоци, контекст)
- процедури за контрола на квалитетот
- работен тек за реагирање на итни случаи што вклучуваат млади

Ова обезбедува конзистентност и покажува дека вашата организација е подготвена одговорно да управува со каналите за приоритетно известување.



3. Обука на персоналот за законските рамки

Вработените кои ќе поднесуваат извештаи мора да разберат:

- национални закони за говор на омраза
- релевантно законодавство на ЕУ
- разлики помеѓу нелегален говор на омраза и штетна, но легална содржина
- контекстуални фактори (заштитени карактеристики, поттикнување, закани)

Обуката може да се спроведува интерно, со надворешни експерти или во партнерство со организации за дигитални права.

4. Воспоставете заштитни мерки за заштита на податоци

Креирај или ажурирај:

- политики за приватност
- процедури за задржување на податоци
- безбедни решенија за складирање
- внатрешни упатства за усогласеност со GDPR
- договори за доверливост на персоналот

Ова е особено важно за организациите што работат со малолетници.

5. Изградете инфраструктура за управување со случаи

Едноставна табела може да биде доволна за мали организации, но оние кои се стремат кон статус на доверлив известувач треба да размислат за следново:

- системи за управување со случаи
- алатки за билети
- споделени папки со контролиран пристап
- безбедни платформи за следење на инциденти

Ова ќе ви помогне да управувате со обемот на известување и да одржувате ревизорски траги.



Процес на аплицирање: Соработка со координаторот за дигитални услуги

Кога вашата организација е подготвена, поднесувате апликација до вашиот национален **координатор за дигитални услуги**. Процесот може малку да се разликува во зависност од земјата, но основните елементи се исти низ цела ЕУ.

Чекор 1: Поднесете формална апликација

Вашата апликација обично ќе вклучува:

- организациски информации
- структура на управување
- документирана експертиза во говорот на омраза и заштитата на младите
- опис на работните процеси за известување
- документација за заштита на податоци
- квалификации и обука на персоналот
- примери за претходно известување или следење

Некои DSC може да побараат и препораки или докази за соработка со платформи или други регулатори.

Чекор 2: Учествувајте во евалуација и консултации

Одборот за млади може да побара дополнителни информации, појаснувања или да спроведе интервју. Тие исто така можат да се консултираат со други органи или актери од граѓанското општество за да го потврдат успехот на организацијата. Младинските организации треба да бидат подготвени да покажат:

- нивното правно разбирање на дефинициите за говор на омраза
- нивната способност да анализираат контекст
- нивната способност да избегнат лажно пријавување
- нивната независност и неутралност

Чекор 3: Добивање на назначување и започнување на соработка



Доколку биде одобрена, вашата организација ќе биде официјално наведена како **доверлив означувач**. DSC ќе ги извести социјалните мрежи и ќе ви обезбеди:

- приоритетни канали за известување
- упатства специфични за платформата
- точки на контакт за комуникација
- очекувања за точност на известувањето и обем на случаи

Доверливите даватели на пријавувања потоа мора да почнат да поднесуваат извештаи преку назначените канали, следејќи ги договорените правила.

Чекор 4: Континуиран мониторинг и одговорност

Статусот на доверлив известувач не е траен или безусловен. DSC може периодично да ги проверуваат перформансите, точноста и независноста на вашата организација. Ова осигурува дека екосистемот на доверлив известувач останува кредибилен, ефикасен и отпорен на злоупотреба.

Младинските организации кои одржуваат конзистентно, точно и етичко известување ќе го задржат статусот долгорочно и може да добијат дополнителни можности за соработка, како што е учество во системски проценки на ризик или консултации за политики.

Работење како доверлив известувач: Одговорности и најдобри практики

Откако ќе добијат статус на Доверлив Означувач, младинските организации добиваат значително влијание - но тие исто така преземаат нови одговорности. Доверливите Означувачи мора да работат според висок професионален стандард и конструктивно да соработуваат со платформите и регулаторите.

1. Одржувајте висококвалитетни извештаи засновани на докази

Секој извештај мора да биде контекстуализиран, прецизен и поткрепен со јасни докази. Извештаите со слаб квалитет го поткопуваат системот. Доверливите означувачи секогаш треба да документираат:

- точниот нелегален израз
- заштитената карактеристика насочена кон



- контекстот во кој се појавува содржината
- какви било шеми или повторувачки однесувања
- потенцијални ризици за младата личност

Ова осигурува дека платформата може да дејствува брзо и самоуверено.

2. Дајте приоритет на безбедноста и благосостојбата на младите

При пријавување на говор на омраза во кој се вклучени малолетници, младинските организации мора внимателно да ги решаваат случаите. Тие треба да го минимизираат емоционалниот товар врз младото лице, да го објаснат процесот на пријавување и да се координираат со поддршка за ментално здравје или училиште кога е потребно. Одговорностите на доверливиот известувач никогаш не ги заменуваат принципите за заштита на децата.

3. Конструктивно ангажирајте се со платформите

Доверливите означувачи честопати редовно комуницираат со онлајн платформите. Ова може да вклучува давање објаснувања за локалниот контекст, истакнување на новите трендови или разјаснување на двосмислени случаи. Конструктивниот дијалог им помага на платформите да ги подобрат системите за модерирање на содржини.

4. Споделување на сознанија со DSC и придонес кон поширока работа на политиките

Доверливите означувачи играат улога не само во пријавувањето на поединечни содржини, туку и во идентификувањето на системски неуспеси. Младинските организации треба да размислат за поднесување:

- квартални резимеа на трендовите на говор на омраза
- сознанија насочени кон младите за кодиран јазик или нови модели на вознемирување
- забелешки за одзивноста на платформата

Овие сознанија им помагаат на DSC да ги проценат ризиците и да го подберат спроведувањето низ целиот дигитален пејзаж.

5. Одржување на транспарентност, независност и етички стандарди

Статусот на доверлив известувач бара интегритет. Младинските организации мора да избегнуваат политичка пристрасност, конфликт на интереси или практики што би



можеле да ја нарушат довербата. Тие треба да се придржуваат до јасни етички упатства и да останат непристрасни при оценувањето на содржината.

Заклучок

Да станете доверлив известувач е и одговорност и можност. За организациите за младинска работа, тоа обезбедува моќен механизам за заштита на младите луѓе од говор на омраза, насилство и вознемирување преку интернет. Признанието го зајакнува влијанието на вашата организација, ја подобрува соработката со платформите и властите и придонесува за побезбедна дигитална средина за сите млади корисници.

Со силна подготовка, транспарентно управување, сигурна експертиза и робусни процедури, младинските организации можат успешно да добијат статус на доверлив означувач и да станат централни актери во новата рамка за безбедност на интернет утврдена со Законот за дигитални услуги.



Project Partners;



digiQ



anthro p o l i s



Co-funded by
the European Union



Handout for Youth-Work Organizations

How to Obtain Trusted Flagger Status for Reporting Hate Speech

Introduction: What Is Trusted Flagger Status and Why It Matters

Under the Digital Services Act (DSA), civil-society organizations can apply to become **Trusted Flaggers** — officially recognized entities whose reports of illegal content (including hate speech) must be given **priority treatment** by online platforms. Trusted Flaggers have enhanced reporting channels, faster review times, and a structured relationship with both platforms and the national **Digital Services Coordinator (DSC)**.

For youth-work organizations, especially those dealing with hate speech, cyberbullying, discrimination, online harassment, or the protection of vulnerable groups, Trusted Flagger status can significantly increase their impact. Many youth-serving NGOs already submit reports to social networks, but without special recognition, their reports move through slow or inconsistent review processes. As a Trusted Flagger, your organization's reports are treated with elevated credibility and urgency, which allows harmful content affecting young people to be removed more quickly and reliably.

Youth organizations also play a uniquely important role: they have access to real experiences of young users, understand evolving online language (slang, coded terms, memes), and are often among the first to observe new forms of hate speech or harassment. Trusted Flagger status helps formalize this expertise and integrate it into the broader online safety ecosystem.

This handout explains what the criteria are, how to prepare your organization, how to apply, and what responsibilities you should be ready to assume once recognized.

Understanding the Trusted Flagger Criteria

The Digital Services Act sets out clear criteria for becoming a Trusted Flagger. Youth organizations should assess whether they meet — or can build — the necessary capacity before applying.

1. Demonstrated Expertise in a Relevant Field

Your organization must show a sustained track record in areas related to illegal hate speech, harmful content, youth protection, online safety, or digital citizenship. This includes experience such as operating a reporting portal, running anti-hate-speech programs,



conducting monitoring or research, handling cases of online harassment, or providing support to marginalized groups affected by hate speech.

2. Independence and Political Neutrality

Trusted Flaggings must be independent from political influence and should demonstrate that their decision-making is guided by expertise, not political agendas. Youth organizations should have transparent ownership, governance structures, and no partisan alignment.

3. Strong Reporting and Verification Procedures

Your organization must have internal systems to verify that the reported content is illegal or harmful under EU or national hate-speech laws. This requires trained staff, a clear escalation mechanism, and the ability to document evidence (URLs, screenshots, context explanations, timestamps).

4. Capability to Process Reports Systematically

Trusted Flaggings must handle a significant number of reports professionally and consistently. You will need a sustainable workflow for receiving, assessing, and forwarding cases. This may include case management tools, internal guidelines, quality assurance processes, and staff trained in hate-speech classification.

5. Compliance with Data Protection and Privacy Rules

Because your organization will be processing sensitive content involving young people, you must demonstrate GDPR compliance. This includes data minimization, anonymization, secure storage, and clear retention policies.

6. Integrity and Accuracy of Reporting

Platforms and DSCs expect high accuracy. You must be able to distinguish illegal hate speech (as defined by law) from harmful but legal expressions. Clear internal criteria, legal consultation, and staff training will be essential.

If your organization can meet these criteria — or is prepared to develop them — you can proceed toward application.

Preparing Your Organization for the Application

The application process requires demonstrating capacity, expertise, and internal structures. Before applying, youth organizations should prepare the following elements:

1. Document Your Experience and Expertise



Prepare a dossier summarizing your work related to hate speech and youth protection. This may include:

- descriptions of relevant programs (anti-bullying, hate-speech prevention, digital citizenship education)
- annual reports
- statistics on cases handled
- previous cooperation with platforms or authorities
- research or publications on online harms

Clear documentation strengthens your credibility and shows the DSC that you understand the digital risk landscape.

2. Build or Update Reporting Protocols

A Trusted Flagger must use structured reporting mechanisms. Prepare or refine internal protocols that include:

- a verification process for each report
- categories of illegal content
- documentation standards (screenshots, metadata, context)
- quality control procedures
- a workflow for responding to urgent cases involving youth

This ensures consistency and demonstrates that your organization is ready to handle priority reporting channels responsibly.

3. Train Staff on Legal Frameworks

Staff members who will submit reports must understand:

- national hate speech laws
- relevant EU legislation
- distinctions between illegal hate speech and harmful, but legal, content
- contextual factors (protected characteristics, incitement, threats)



Training can be done internally, with external experts, or in partnership with digital-rights organizations.

4. Establish Data Protection Safeguards

Create or update:

- privacy policies
- data retention procedures
- secure storage solutions
- internal GDPR compliance guidelines
- staff confidentiality agreements

This is particularly important for organizations working with minors.

5. Build a Case Management Infrastructure

A simple spreadsheet may be enough for small organizations, but those aiming for Trusted Flagger status should consider:

- case management systems
- ticketing tools
- shared folders with controlled access
- secure incident-tracking platforms

This will help you manage reporting volume and maintain audit trails.

The Application Process: Working with the Digital Services Coordinator

When your organization is ready, you submit an application to your national **Digital Services Coordinator**. The process may differ slightly by country, but the core elements are the same across the EU.

Step 1: Submit a Formal Application

Your application will typically include:



- organizational information
- governance structure
- documented expertise in hate speech and youth protection
- description of reporting workflows
- data protection documentation
- staff qualifications and training
- examples of past reporting or monitoring

Some DSCs may also ask for references or evidence of cooperation with platforms or other regulators.

Step 2: Participate in Evaluation and Consultation

The DSC may request additional information, ask for clarifications, or conduct an interview. They may also consult other authorities or civil-society actors to confirm the organization's track record. Youth organizations should be ready to demonstrate:

- their legal understanding of hate-speech definitions
- their ability to analyze context
- their ability to avoid false reporting
- their independence and neutrality

Step 3: Receive Designation and Begin Cooperation

If approved, your organization will be officially listed as a **Trusted Flagger**. The DSC will notify social networks and provide you with:

- priority reporting channels
- platform-specific instructions
- communication points of contact
- expectations for reporting accuracy and case volume



Trusted Flaggers must then begin submitting reports through the designated channels, following the agreed rules.

Step 4: Ongoing Monitoring and Accountability

Trusted Flagger status is not permanent or unconditional. DSCs may periodically review your organization's performance, accuracy, and independence. This ensures the Trusted Flagger ecosystem remains credible, effective, and resistant to misuse.

Youth organizations that maintain consistent, accurate, and ethical reporting will retain status long-term and may receive additional opportunities for collaboration, such as participation in systemic risk assessments or policy consultations.

Operating as a Trusted Flagger: Responsibilities and Best Practices

Once granted Trusted Flagger status, youth organizations gain significant influence — but they also assume new responsibilities. Trusted Flaggers must operate at a high professional standard and engage constructively with platforms and regulators.

1. Maintain High-Quality, Evidence-Based Reports

Each report must be contextualized, precise, and backed by clear evidence. Poor-quality reports undermine the system. Trusted Flaggers should always document:

- the exact illegal expression
- the protected characteristic targeted
- the context in which the content appears
- any patterns or repeated behaviours
- potential risks to the young person

This ensures the platform can act quickly and confidently.

2. Prioritize Youth Safety and Wellbeing

When reporting hate speech involving minors, youth organizations must handle cases with care. They should minimize emotional burden on the young person, explain the reporting process, and coordinate with mental-health or school support when relevant. Trusted Flagger responsibilities never override child protection principles.

3. Engage with Platforms Constructively



Trusted Flaggers often communicate regularly with online platforms. This can include providing explanations of local context, highlighting emerging trends, or clarifying ambiguous cases. Constructive dialogue helps platforms improve content moderation systems.

4. Share Insights with the DSC and Contribute to Broader Policy Work

Trusted Flaggers play a role not only in reporting individual pieces of content but also in identifying systemic failures. Youth organizations should consider submitting:

- quarterly summaries of hate-speech trends
- youth-centered insights on coded language or new harassment patterns
- observations about platform responsiveness

These insights help DSCs assess risks and improve enforcement across the digital landscape.

5. Maintain Transparency, Independence, and Ethical Standards

Trusted Flagger status requires integrity. Youth organizations must avoid political bias, conflicts of interest, or practices that could damage trust. They should uphold clear ethical guidelines and remain impartial when evaluating content.

Conclusion

Becoming a Trusted Flagger is both a responsibility and an opportunity. For youth-work organizations, it provides a powerful mechanism to protect young people from online hate speech, violence, and harassment. The recognition strengthens your organization's influence, improves collaboration with platforms and authorities, and contributes to a safer digital environment for all young users.

With strong preparation, transparent governance, reliable expertise, and robust procedures, youth organizations can successfully obtain Trusted Flagger status and become central actors in the new online safety framework established by the Digital Services Act.