

When Harm Remains Invisible

Anti-LGBTIQ+ hostility, access to support and safe reporting in Ukraine

535 respondents	75.0% aged 16–24	19.6%* sought help	76.7% willing to use an online form
---------------------------	----------------------------	------------------------------	---

* Among n=316 respondents to the relevant question; the base also includes respondents who reported that no relevant incident occurred. This is not a national reporting rate.

Key message

Ukraine needs more than another channel for submitting complaints. It needs a coherent and safe pathway through which an LGBTIQ+ person can report hostility they have experienced, obtain information or support, and decide for themselves whether to proceed to a formal response.

The findings of this study show that a significant part of harm may become invisible before any formal complaint is ever considered. People may conceal their sexual orientation or gender identity, avoid environments they perceive as unsafe, seek out LGBTIQ+-friendly service providers in advance, or modify their behaviour. Even when a direct incident occurs, the person concerned may not perceive it as “serious enough” to report.

This creates a gap between experienced harm and its institutional visibility.

What the study shows

Harm is not limited to incidents directed personally at an individual. Among the 440 respondents who answered questions about exposure to hostile expressions during the previous 12 months, 50.9% reported hostility directed only at LGBTIQ+ people in general, without being personally targeted, while 43.0% reported personally directed hostility. Negative psychological and behavioural indicators were recorded in both groups.

People adapt their behaviour to risk before any formal complaint is made. Among respondents to the relevant section, 68.3% reported having to conceal themselves within their family, 53.1% in educational settings, 50.4% when accessing health or social services, and 48.6% when interacting with state or local institutions. Only 6.4% said they almost never had to conceal themselves.

Direct incidents are associated with more pronounced negative outcomes. Among respondents who reported at least one direct incident, 42.5% reported a strong or very strong impact on their sense of safety, compared with 13.4% among those who answered “no” to all four questions on direct incidents. A need for psychological support was reported by 44.9% and 9.0% respectively. These are associations within the sample and do not establish causality.

There is a substantial gap between experienced harm and help-seeking. Among the 316 respondents to the relevant section, 19.6% reported seeking help, advice or a response, while 52.8% did not. The most frequently reported reasons for not seeking help were: the situation not seeming “serious enough” — 43.7%; an expectation that reporting would change nothing — 35.3%; lack of energy or resources — 32.3%; lack of trust in institutions — 31.1%; not knowing where to turn — 26.3%; and fear of unwanted disclosure — 25.7%.

Low levels of actual reporting coexist with substantial stated willingness to use a safe mechanism. Among 318 respondents, 76.7% said they would be willing or somewhat willing to use an online form to report incidents. This measures stated willingness in a hypothetical scenario; it is not a forecast of actual use.

One of the central findings

“I wasn’t beaten... nothing serious happened. There were threats, but the threats didn’t lead to anything.”
From an in-depth interview.

This is one of the points at which information about harm can disappear from view — before it reaches the police, a complaints mechanism, a court or official statistics.

Primary support should therefore be available earlier, without requiring a person first to demonstrate the seriousness of what happened or to make their own legal assessment of the incident.

About the study

This Policy Brief draws on an online self-administered survey of 535 LGBTIQ+ respondents and 11 in-depth semi-structured interviews with separately recruited participants. The survey sample was non-probability and self-selected; question bases vary because of routing and non-response. Findings are not prevalence estimates for the whole LGBTIQ+ population of Ukraine.

An important characteristic of the sample is its strong youth profile: 75.0% of participants were aged 16–24, including 30.3% aged 16–17. The study therefore provides particularly detailed insight into the experiences of younger LGBTIQ+ people, while older age groups are less strongly represented.

The problem is not limited to incidents. The system does not see all harm

Policy responses to hate speech, discrimination and violence tend to rely heavily on what has already become institutionally visible: requests for assistance, complaints, registered proceedings and other official records.

The study points to the limits of this approach.

Before making a formal report, a person has to navigate a series of decisions: whether it is safe to be open; whether to avoid a particular setting; whether a particular institution can be trusted; whether what happened was serious enough; whether it is safe to disclose personal data; and whether reporting is likely to produce any result.

At each of these points, information about experienced harm may remain outside institutional systems.

For this reason, **the number of formally recorded cases cannot serve as the sole measure of either the safety of an environment or the need for support.**

From a hostile environment to invisible experience

The study identifies at least four mechanisms through which this gap can emerge.

1. Hostility can matter even when it is not personally directed

Hostile expressions concerning LGBTIQ+ people in general may be interpreted as information about the wider social environment and a person's own potential exposure to risk.

This does not mean that every negative or offensive expression has the same severity or legal status. However, assessments of impact should not be confined to situations in which a specific individual has already become the direct target.

This approach is consistent with the Council of Europe framework, which calls for differentiated responses according to the severity of hate speech and for attention to the experiences of those affected, barriers to reporting and broader forms of harm.

2. The absence of open conflict may be associated with self-restriction

Concealment, situational openness, avoidance of certain spaces and advance screening of service providers may all function as ways of managing anticipated risk.

The quantitative data do not allow the direction of causality to be established in each individual case. The qualitative interviews illustrate at least two possible sequences: increased caution following a negative experience, and preventive concealment intended to minimise anticipated risk.

This has an important policy implication: **an environment with few complaints is not necessarily an environment with low levels of risk.**

3. People set their own threshold for what is “serious enough”

Among respondents who had not sought help, 43.7% said that the situation had not seemed serious enough.

The qualitative data illustrate one possible mechanism behind this assessment: a threat that does not result in physical violence may be reinterpreted by the person concerned as an event that does not justify seeking help.

If access to primary support is effectively available only after harm reaches a high threshold, some people may remain outside the system until the situation escalates.

4. Reporting is not the same as consenting to formal proceedings

Among respondents to the relevant section, 49.1% wanted the option simply to report an incident without further action; 45.4% wanted legal advice; 39.2% wanted psychological support; and 29.3% wanted the option to consent to the preparation of a formal submission to an institution.

These responses point to the need to distinguish between three separate functions:

documentation → support → formal response.

Movement between them should not be automatic.

Ukraine has individual mechanisms, but they do not form a single clear pathway for the person concerned

Ukrainian legislation does not contain a single statutory definition of hate speech or a comprehensive legal regime governing responses to it. Different manifestations are addressed through different legal concepts, including incitement to hatred or hostility, incitement to discrimination or harassment, discrimination, specific criminal offences and sector-specific prohibitions.

Their scope, protected characteristics, competent authorities and possible legal consequences differ.

For example, the Law of Ukraine “On Media” covers certain forms of expression involving the incitement of hatred, hostility or cruelty and incitement to discrimination or harassment, explicitly including sexual orientation and gender identity among the protected characteristics. Other legal regimes have a different scope.

The practical consequence is that the available route for response may depend on the content of the expression, the setting in which it occurs, the form and severity of the harm, and its possible legal qualification.

A clearer legal norm alone does not create a safe reporting and support pathway. A person still needs to understand where they can turn, who will receive their data, what will happen after they report, whether support is available without initiating a formal procedure, and which subsequent actions require a separate decision or consent.

Among respondents who had not sought help, 50.9% identified guaranteed confidentiality as a condition that would make reporting safer; 49.1% identified the possibility of anonymous reporting; and 47.9% identified a clear explanation of what would happen next.

From a complaints channel to a safe response system

The central policy question is therefore not only **whether an institution exists to which a complaint can be submitted**.

It is also whether a person can make experienced harm visible **without creating a new risk for themselves and without losing control over what happens next**.

This Policy Brief considers a national system through four interconnected functions:

RECOGNITION → SAFE REPORTING → SUPPORT → FORMAL RESPONSE

A cross-cutting principle applies throughout:

CONTROL — the person understands and, where permitted by law, retains control over the use of their data, consent to subsequent actions and transition to a formal response.

Safety cannot be measured by incident counts alone

Official recording systems are best able to capture events that have already become explicit: threats, harassment, discriminatory denial of services, violence, complaints or proceedings.

The findings of this study reveal another dimension — **behavioural adaptation to anticipated risk**.

LGBTIQ+ people may alter their behaviour before any open conflict occurs: conceal information about themselves, regulate their gender expression, avoid particular spaces, screen service providers in advance or limit their public visibility.

Such strategies may be intended to reduce exposure to risk. The absence of an overt incident therefore does not necessarily mean the absence of a problem.

Hostility towards the group can become information about personal safety

Personally directed hostility is associated with more pronounced negative indicators. Its impact, however, is not limited to people who were themselves directly targeted.

Among respondents who reported personally directed hostility, 70.0% said that they often or sometimes changed their behaviour. Among those who reported only hostility towards LGBTIQ+ people in general, the corresponding figure was 58.3%.

A strong or very strong emotional impact was reported by 40.1% and 22.0% respectively. Depressed mood, anxiety and loss of trust in other people were also common in both groups.

These data do not establish that a particular expression caused a particular behavioural response. They indicate something different: **the distinction between being a “direct target” and being exposed only to hostility towards the wider community is insufficient for understanding how people experience their social environment.**

The qualitative interviews illustrate one possible mechanism: hostility towards the group as a whole may be perceived as an indication of what could happen if a person’s own identity became known.

“People are afraid to post content online; they do not show their face or use their voice because they are afraid they will be found, beaten, or no longer hired. And then you develop this feeling that you are alone and that there is nobody else like you.”

From an in-depth interview.

Concealment is not a neutral individual characteristic

In this study, concealment is not treated as a fixed personal trait or simply as a matter of privacy. It may be connected to a person’s assessment of whether a particular environment is safe.

Among 486 respondents to the relevant section, 68.3% reported having to conceal themselves within their family, 53.1% in educational settings, 50.4% when accessing health or social services, 48.6% when interacting with state or local institutions, 43.8% at work and 40.3% in public spaces.

Only 6.4% said that they almost never had to conceal themselves.

Separately, 73.6% of respondents who answered the question on openness reported fear of unwanted disclosure at least rarely; 18.3% experienced such fear often.

Openness should not itself be treated as a policy objective. People have the right to decide for themselves to whom and when they disclose information about their sexual orientation or gender identity.

The policy concern arises when concealment becomes, in practice, a condition for access to safety, education, health care, employment or public services.

Avoidance can make the problem less visible to the system

The qualitative interviews contain examples of participants avoiding places they perceived as homophobic, searching in advance for LGBTIQ+-friendly doctors, withdrawing from discussions after aggressive reactions, or restricting their public visibility.

These strategies may be rational forms of risk reduction. At the same time, they create a methodological and governance problem: a system may record fewer overt conflicts in settings that people have learned to avoid because they regard them as unsafe.

Low numbers of incidents in a particular institution, sector or environment should therefore not automatically be interpreted as evidence of safety.

Policy implication

Assessing safety requires more than counting:

- **complaints → incidents → proceedings.**

It also requires attention to:

- **concealment → avoidance → anticipated risk → fear of unwanted disclosure → trust in reporting mechanisms.**

This is particularly important in systems that people cannot simply opt out of, including education, health and social services, policing, and state or local authorities.

Implications for monitoring

A fuller assessment requires at least three types of information:

1. **Administrative data** — complaints, reports, proceedings, decisions and contacts with services.
2. **Experience data** — surveys on exposure to hostility, discrimination, threats and violence.
3. **Behavioural and access indicators** — concealment, avoidance, trust, fear of unwanted disclosure, knowledge of support pathways and barriers to reporting.

Together, these layers provide a fuller picture and help distinguish genuinely low levels of harm from situations in which harm simply does not reach official records.

One mechanism cannot respond equally well to all risk profiles

Average indicators across the LGBTIQ+ sample may obscure important differences between groups.

Two dimensions are particularly visible in this study: **age within educational settings** and **gender-related experience**.

These findings do not establish a hierarchy of “more” and “less” vulnerable groups. They show that a reporting and support system cannot be designed on the assumption that all LGBTIQ+ people face the same risks, have the same degree of autonomy or have the same ability to leave an unsafe environment.

Young people: when the environment of risk is also an environment of dependency

Three quarters of participants in the quantitative study (75.0%) were aged 16–24. Almost one third of the entire sample — 30.3% — were aged 16–17.

This limits the extent to which the findings can be applied to older age groups, but it also gives the study a particularly strong youth perspective.

For respondents aged 16–17, educational settings were especially likely to be associated with the need for concealment and the expectation of negative treatment.

Among respondents aged 16–17,

76.6% reported having to conceal themselves in an educational institution. The corresponding proportion was **56.0%** among respondents aged 18–24 and **20.8%** among respondents aged 25+.

Fear of bullying or pressure in educational settings was reported by **71.8%**, **46.4%** and **14.5%** respectively.

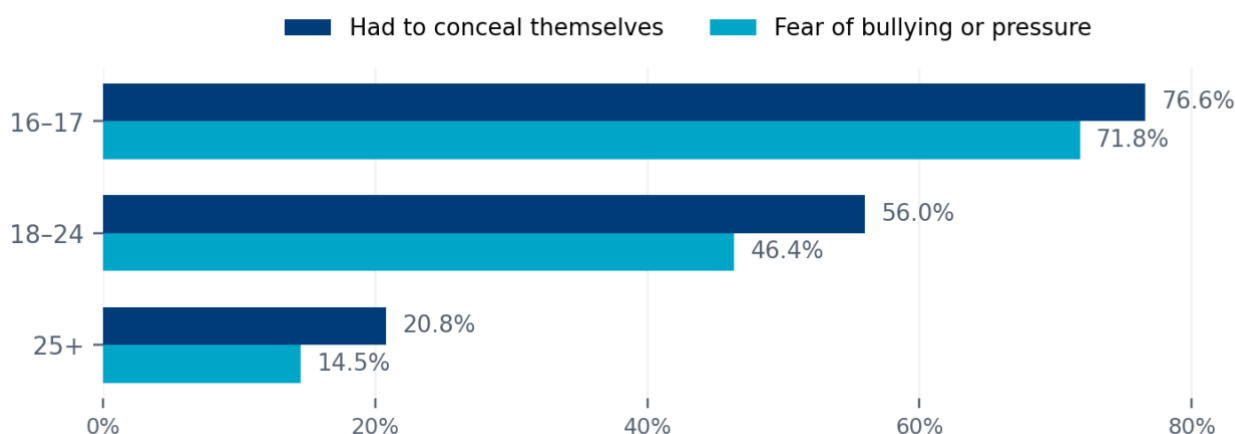


Figure 1. Educational-setting indicators by age group. *Exploratory subgroup associations within the study sample; not population estimates.*

These associations are exploratory and should not be interpreted as estimates of the proportion of “unsafe schools” in Ukraine.

They do, however, raise a concrete question for system design:

Where can a 16-year-old LGBTIQ+ person turn safely when the environment in which they study or live also controls a significant part of their access to help?

An internal reporting route is not sufficient on its own

Adults may sometimes have greater scope to change a provider or environment, although this is by no means always possible. For minors, autonomy is often even more constrained.

They may depend on family members for housing and material support, on school administration and staff, on adults for access to certain services, and on a local social environment that cannot quickly be changed.

“Report it to the administration of your institution” therefore cannot be the only available route.

At the same time, the qualitative data do not support the opposite simplification that every member of staff in an educational institution constitutes a risk. Interviews include examples in which a particular teacher, manager or other adult became a source of support.

The system should therefore provide **a choice between a trusted internal contact and a confidential external pathway**.

For minors, an external route should be understandable, confidential, mobile-accessible and designed with the risk of unwanted disclosure in mind.

Transgender and non-binary experiences should not be collapsed into a single category

A second clear signal concerns gender-related experience.

The subgroup analysis deliberately does not equate transgender and non-binary experiences, and it does not label respondents who did not select either characteristic as “cisgender”. Derived categories are used for analytical purposes and do not replace self-identification.

Misgendering was reported by:

- **82.3%** of respondents in the “transgender experience only” category;
- **47.4%** in the “non-binary experience only” category;
- **82.8%** among those reporting both transgender and non-binary experience;
- **28.0%** among respondents who selected neither of these two characteristics.

Threats as a direct incident were reported by **56.8%, 27.3%, 57.5% and 17.3%** respectively.

Unauthorised disclosure of private information was also reported more frequently among groups with transgender experience.

These results are not population estimates. Subgroup analyses are exploratory. They nevertheless have clear relevance for the design of reporting and support mechanisms.

War time context

The war context also affects the conditions under which people assess safety and access support. In this sample, 31.2% of respondents to the relevant section reported that the war had worsened or significantly worsened their sense of safety as an LGBTIQ+ person. The data also record displacement, weakened social ties and increased dependency on others. At the same time, the study does not support interpreting the war as the sole cause of anti-LGBTIQ+ hostility; qualitative data include both hostile narratives using military themes and experiences of acceptance within military environments.

An inclusive mechanism must understand the form of risk

A person reporting systematic misgendering, a threat to disclose information about their transgender status, unauthorised sharing of private information or a related experience may require a different assessment of confidentiality and risk from someone reporting a public homophobic comment.

A national reporting system should therefore:

- avoid collecting unnecessary identity data;
- allow self-description, where possible, rather than imposing rigid categories;
- recognise risks related to unwanted disclosure and the dissemination of private information;
- avoid automatically collapsing different gender-related experiences into a single category;
- provide referral to services competent to respond to the relevant form of risk.

Policy implication

Universality of access does not require identical pathways.

A common entry point, shared confidentiality standards and principles of user control over data may be universal. Initial risk assessment, support and onward routing should nevertheless be responsive to different life contexts.

For a young person, this may mean a confidential external channel outside the school.

For a transgender person, it may require greater attention to personal data, unwanted disclosure, misgendering and threats.

For another person, the primary need may simply be to document an incident without taking any further action.

Direct incidents are associated with higher levels of harm — but should not be the threshold for access to support

Hate speech, threats, harassment, discriminatory treatment and physical violence are related but distinct phenomena.

This distinction matters legally and operationally. The survey records respondents' reported experiences; it does not provide a legal qualification of each incident. A reported threat does not automatically constitute a hate crime, just as an offensive expression does not automatically amount to legally sanctionable hate speech.

Direct incidents nevertheless provide an important signal of elevated risk.

The study separately asked about four forms of direct negative experience: threats; repeated bullying, harassment, persistent messages or coordinated attacks; discriminatory treatment or denial of access to services; and physical or sexual violence.

Threats were reported by 97 of 383 respondents to the relevant question — **25.3%**. Repeated bullying, harassment, persistent messages or coordinated attacks were reported by 83 of 379 — **21.9%**. Discriminatory treatment or denial of access to services was reported by 63 of 379 — **16.6%**. Physical or sexual violence was reported by 31 of 380 — **8.2%**.

These proportions describe the respective respondent bases in this study. They are not estimates of the prevalence of these incidents among all LGBTIQ+ people in Ukraine.

Negative indicators are more pronounced following a direct incident

For a separate analysis, the study compared respondents who reported at least one of the four direct incidents with respondents who answered “no” to all four questions. Uncertain responses were excluded from the comparison.

A strong or very strong impact on the sense of safety was reported by **42.5%** of respondents with at least one direct incident, compared with **13.4%** in the group with no affirmative response to any of the four questions.

For strong or very strong emotional impact, the respective proportions were **46.0% versus 12.8%**; for a need for psychological support, **44.9% versus 9.0%**; and for often or sometimes avoiding offline spaces, **64.2% versus 29.8%**.

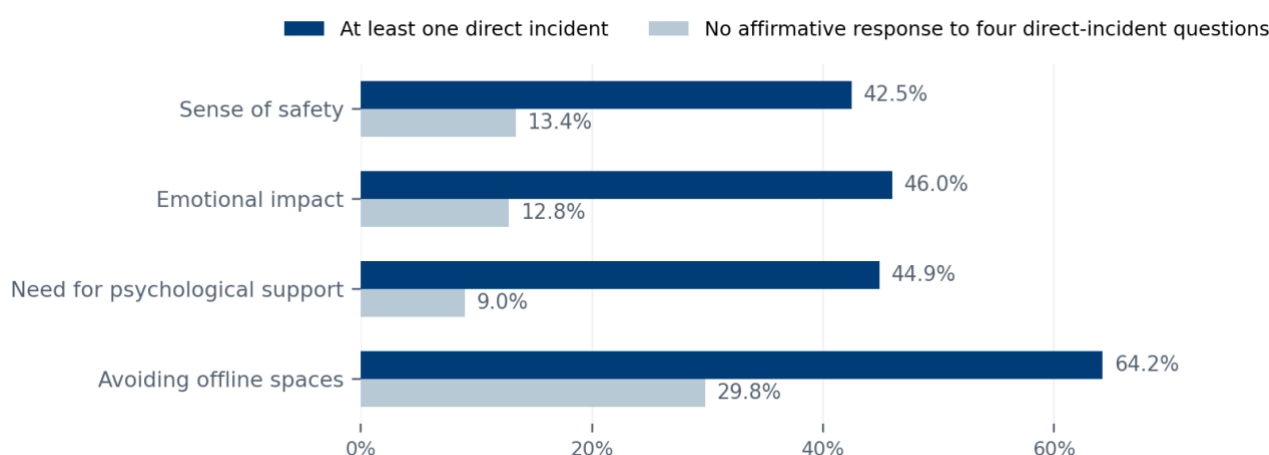


Figure 2. Selected outcomes by direct-incident status. *Exploratory associations; uncertain responses excluded from the comparison.*

Respondents in the direct-incident group also more frequently reported anxiety — 73.9% versus 48.0%; depressed mood — 69.6% versus 50.0%; and loss of trust in other people — 69.6% versus 41.0%.

These are exploratory associations within the sample and do not establish causality. The consistency of the differences across several indicators nevertheless supports treating a direct incident as an important signal when assessing safety and support needs.

Harm does not begin with a direct incident

This finding does not mean that the system should wait until hostility becomes a threat, discriminatory denial of service or violence.

Negative psychological and behavioural indicators were also present among some respondents who did not report a direct incident or who were exposed only to hostility towards LGBTIQ+ people in general.

A direct incident should therefore be treated as **a signal of increased need**, rather than **the minimum threshold for access to primary support**.

A high-threshold model

Under a high-threshold model, a person is effectively required to answer three questions first:

- “Was what happened to me serious enough?”
- “Was it an offence?”
- “Am I entitled to seek help?”

Some experiences may be filtered out before any contact with a support system takes place.

A low-barrier model

The first question becomes:

“Do you need information, documentation of the incident, a safety assessment or support?”

Legal qualification is the responsibility of a competent professional or authority. It should not be a precondition for access to primary assistance.

“I wasn’t beaten... nothing serious happened. There were threats, but the threats didn’t lead to anything.”
From an in-depth interview.

This case illustrates one possible mechanism: the threat itself is not denied, but it is reinterpreted as “not serious enough” because it did not culminate in a physical act.

Policy implication

A support system should not require harm to escalate before support becomes available.

Initial reporting, consultation, safety assessment and information on available options should be accessible before a case reaches the threshold for formal legal action or physical violence.

The visibility gap: where experienced harm becomes invisible to the system

There is no automatic transition from an incident to official statistics.

For an experience to become visible to the state or to a support system, a person must regard it as sufficiently significant, know a possible pathway, consider the process sufficiently safe, have the resources to engage with it, and regard the risks of reporting as acceptable.

If one or more of these conditions is absent, the experience may remain outside institutional records.

This Policy Brief uses the term **visibility gap** to describe the gap between experienced harm and its institutional visibility.

It is an analytical framework synthesising the study findings, not a validated quantitative index.

Formal reporting is only one possible outcome of an experience

Among the 316 respondents who answered the question about seeking help, advice or a response, **19.6%** said they had sought help, **52.8%** had not, **19.3%** said there had been no relevant incident, and **7.3%** selected “difficult to say”.

These figures cannot be used as a national estimate of reporting rates. They allow the study to examine why respondents in this sample did not move from experiencing an incident to seeking help.

There is no single reason for non-reporting

Among the 167 respondents who did not seek help, 43.7% said the situation had not seemed “serious enough”; 35.3% expected that reporting would change nothing; 32.3% lacked the energy or resources; 31.1% did not trust institutions; 26.3% did not know where to turn; and 25.7% feared unwanted disclosure.

Other reasons included fear of retaliation or deterioration of the situation — 19.8%; unwillingness to relive the experience — 17.4%; the belief that they lacked evidence — 15.0%; absence of a safe channel — 12.6%; and a previous negative experience — 9.6%.

The question allowed multiple responses. These factors therefore do not constitute a universal causal or chronological sequence.

They show that low reporting cannot be explained by one barrier or addressed through an information campaign alone.

Awareness, trust and accessibility are different problems

A person may know that an institution exists and still not trust it.

They may trust a particular organisation but still not seek help because of fear of disclosure, lack of resources or the belief that the incident was not serious enough.

They may be willing to report but not understand what will happen after they do so.

It is therefore insufficient to measure only “levels of trust”.

In this sample, high levels of distrust in the police coexisted with high levels of awareness of the police as a potential mechanism. This means that the situation cannot be explained simply by lack of information. For some specialised mechanisms, by contrast, low awareness itself constituted a significant barrier.

Different problems require different responses:

- **does not know about the mechanism → information is needed;**
- **knows about it but does not trust it → greater predictability and changes in practice are needed;**
- **trusts it but does not use it → other barriers need to be examined;**
- **fears unwanted disclosure → different data and confidentiality arrangements are needed.**

Submitting a report does not necessarily create confidence that the system is working

The visibility gap does not necessarily end once a report has been submitted.

The qualitative data include a case in which making a formal report did not create a sense that a process was under way because there was no clear feedback or visible follow-up.

This example is not an assessment of police performance as a whole. It illustrates another potential point of failure: **information has reached an institution, but the person does not understand what happened to it next.**

A reporting system should therefore assess not only whether a report was received, but whether the person received confirmation, understands the next step, receives feedback, and knows what action has or has not been taken.

Five points in the visibility gap

The identified barriers can be analytically grouped into five points. This is a synthesis of the study findings, not a validated scale.



Experienced harm can disappear from institutional visibility at any of these points.

Figure 3. Five points in the visibility gap. *Analytical synthesis of study findings; not a validated scale.*

- 1. Recognition.** The person does not consider the situation serious enough.
- 2. Navigation.** The person does not know where or how to seek help.
- 3. Trust and safety.** The person does not expect a safe or effective response.
- 4. Capacity.** Reporting requires emotional, time-related or other resources that the person does not have.
- 5. Feedback.** A report has been made, but the subsequent process remains unclear.

The policy objective is not simply to increase the number of complaints.

It is to **reduce the number of points at which people are effectively forced to abandon safe documentation of their experience or access to the support they need.**

Safe reporting is an architecture of choice, not a single form

The study findings do not support a model in which every report automatically becomes a formal complaint.

Potential users see several distinct functions in a reporting mechanism: documenting an incident, obtaining information, accessing psychological or legal support, permitting certain uses of data, or — if they choose — proceeding to a formal submission.

These functions may be connected, but they are not interchangeable.

There is substantial stated willingness to use a mechanism — under certain conditions

Among 318 respondents to the relevant section, **76.7%** said they would be willing or somewhat willing to use an online form to report incidents.

This is stated willingness in a hypothetical situation, not a prediction of actual behaviour.

Among 324 respondents, **69.8%** identified anonymity as a feature that would make the mechanism more acceptable, **68.2%** identified a clear understanding of what would happen after reporting, **45.4%** wanted to know who would see the report, **41.7%** identified simple and understandable language, and **40.7%** identified ease of use on a mobile phone.

The acceptability of a mechanism therefore depends on more than the technical existence of a form.

Process predictability is critical.

The most frequently cited barriers concern control over information

Asked about potential barriers, 55.6% of respondents identified uncertainty about who would receive the information ; 51.2% the requirement to provide personal data; 46.3% lack of confidence in data security; 44.8% fear of unwanted disclosure; 43.5% absence of a response after reporting; and 40.1% fear that information would be transferred to another institution without consent.

By comparison, 22.2% identified excessive form length as a potential barrier.

This does not mean that usability is unimportant. It means that **a user-friendly interface without clear data-governance rules does not address the central concern.**

A well-designed form that does not explain the pathway of information may still be unacceptable to potential users.

Reporting does not mean consenting to every subsequent action

Among 324 respondents, 49.1% wanted the option simply to report an incident with no further action; 45.7% wanted to allow the case to be used in aggregate statistics; 45.4% wanted legal advice; 39.2% wanted psychological support; and 38.9% wanted to allow the case to be used in legal analysis without personal data.

In addition, 36.4% wanted information on available support resources; 29.3% wanted the option to consent to preparation of a formal submission to an institution; and 22.8% wanted the ability to delete their report or withdraw consent.

These responses do not establish the motivation behind each choice. They do, however, support a systemic conclusion:

documentation, use of data, support and formal response should be clearly separated and, where applicable, should involve distinct decisions by the person concerned.

A person-controlled reporting model

This is a policy design, not an empirically tested national system; it translates the study findings and Council of Europe standards into five user-controlled decisions.

What to disclose. Personal information that is not necessary for the selected function should not be collected.

Whether to identify oneself. Anonymous or minimally identified reporting should be available where compatible with the function of the mechanism and applicable law.

How information may be used. Storage of the report, use in anonymised statistics or analysis, contact with the person, referral to another service and preparation of a formal complaint should be clearly distinguished.

What type of support is needed. Legal advice and psychological support should not be triggered automatically together or required in a fixed sequence.

Whether to proceed to formal action. A formal complaint, transfer of personal data to another institution or another subsequent action should require separate informed consent where this is applicable and where the law does not provide otherwise.

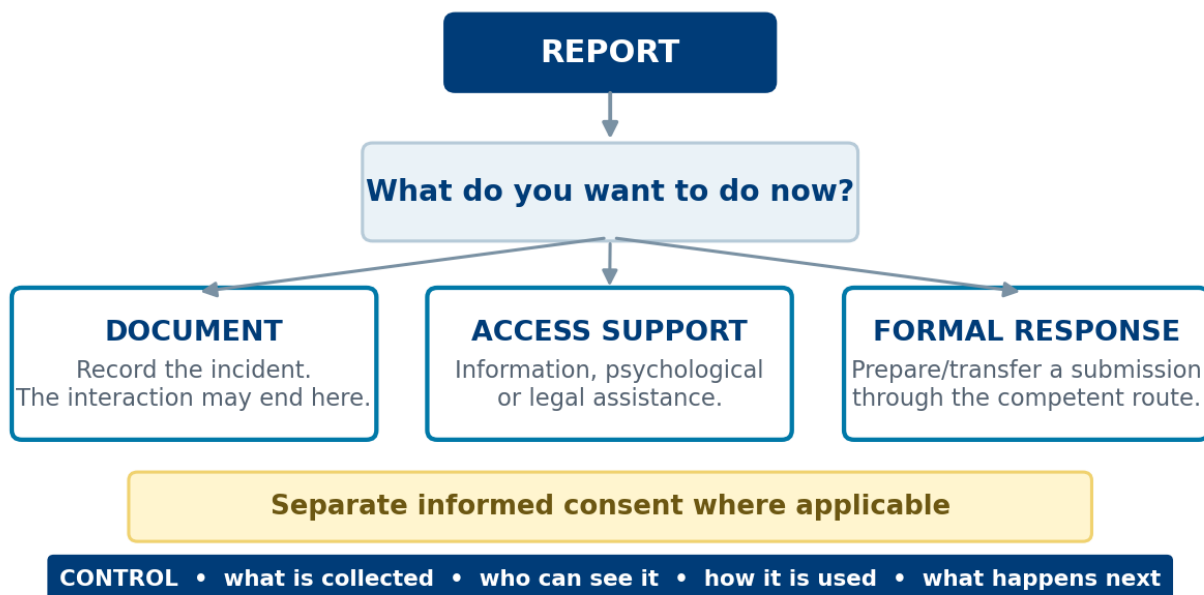


Figure 4. Person-controlled reporting architecture. Documentation, support and formal response are distinct functions; transitions should not be automatic.

Basic architecture

REPORT

↓

What do you want to do now?

→ **DOCUMENT** Record the incident. The interaction may end at this point.

→ **ACCESS SUPPORT** Obtain information, psychological support or legal assistance. The interaction may also end at this point.

→ **PROCEED TO FORMAL RESPONSE** Prepare a submission or transfer information to the competent institution in accordance with the law and the pathway chosen by the person.

Between these functions there should be **separate informed consent where applicable**.

The cross-cutting principle is **control**.

Before beginning the form, a person should understand who will receive the information, why it is being collected, which data are necessary, what will happen after they click “submit”, and which subsequent actions will not take place without a separate decision or consent.

Success should not be measured only by the number of formal cases

The effectiveness of such a system should not be assessed solely by the number of cases transferred to the police or other institutions.

It is also important to know how many people were able to document an experience safely; how many received the information they needed; how many accessed psychological or legal support; whether users understood the rules governing their data; whether they received feedback; and how many chose to proceed to a formal response.

Central conclusion

People should not have to choose between complete invisibility and complete loss of control over their own story.

There should be a safe space between these two extremes for documentation, consultation, support and an informed decision about what happens next.

From fragmented law to a coherent pathway for the person concerned

Ukraine is not starting from zero in its response to anti-LGBTIQ+ hostility. The problem lies elsewhere: different manifestations of one lived experience fall under different legal regimes, trigger different intervention thresholds and lead to different institutions.

Ukrainian legislation does not contain a single statutory definition of “**hate speech**”.

The Ukrainian Parliament Commissioner for Human Rights has repeatedly identified the absence of a comprehensive approach to defining and countering hate speech; the 2025 Annual Report states that this remained an unresolved issue.

Legal protection exists, but is distributed across different regimes

Media law is one example.

Article 36 of the Law of Ukraine “On Media” covers certain forms of expression involving the incitement of hatred, hostility or cruelty and incitement to discrimination or harassment. Sexual orientation and gender identity are explicitly included among the protected characteristics.

The criminal-law framework is different. Part 1 of Article 161 of the Criminal Code uses the categories of national, regional, racial or religious hostility and hatred. A broader list of characteristics in the same article is used for a different legal construction — direct or indirect restriction of rights or the establishment of privileges.

For the person concerned, an experience may be perceived as one event, while the law divides it into different legal categories depending on its content, setting, form of conduct, severity, consequences and the competence of the relevant authority.

Legal qualification should not be the first task placed on the affected person

A person who receives a threat following a homophobic comment, experiences systematic harassment or encounters public calls targeting LGBTIQ+ people may not know whether the situation constitutes hate speech in a legal sense, discrimination, an administrative or criminal offence, a matter of media regulation or another legal category.

Among respondents who had not sought help, 26.3% explicitly identified not knowing where to turn as one of the barriers.

Legal fragmentation is therefore not only a matter of legal technique. It can become **a navigation problem for the person concerned**.

A national system should compensate for this complexity through a different principle:

a person should not be required to identify the correct legal qualification of an incident in order to obtain initial information, documentation or support.

Initial assessment and identification of a possible legal pathway should take place after entry into the system.

Draft Law No. 13597 is part of the legal context, not the entire system

Legislative changes in this area are under consideration in the Verkhovna Rada. Draft Law No. 13597 was registered on 4 August 2025, included in the parliamentary agenda on 1 September 2026 and, as of 19 September 2026, remained under consideration in committee. Alternative draft laws No. 13597-1 and No. 13597-2 are also registered.

For the purposes of this Policy Brief, two levels should be distinguished.

Substantive legal framework: which acts are covered by law, which characteristics are protected, what forms of liability apply and which authorities have competence.

Access architecture: how a person finds an available pathway, reports safely, receives assistance and moves towards a formal response.

Change at the first level does not automatically create the second.

Council of Europe standards support a broader response logic

Council of Europe Recommendation CM/Rec(2022)16 takes a comprehensive human-rights approach to combating hate speech rather than focusing exclusively on the criminalisation of its most serious manifestations.

Relevant Council of Europe instruments also address the accessibility of support, the role of independent public institutions and civil society, data collection and the protection of privacy.

This is consistent with one of the central conclusions of the study:

the need for support does not coincide with the threshold of criminal liability.

From legal regimes to system functions

Rather than seeking one universal mechanism, a national architecture can be considered through five interconnected functions.

1. RECOGNITION

The system can distinguish between hostile expressions, threats, harassment, discrimination, violence and risks of unwanted disclosure without assigning the same legal qualification to all of them.

2. SAFE INITIAL CONTACT

A person can report an experience without having to know in advance which authority is competent or which legal category applies.

3. SUPPORT

Access to information, psychological support and legal assistance does not automatically depend on willingness to file a formal complaint.

4. ROUTING AND FORMAL RESPONSE

Where a case requires formal action, or where the person chooses that pathway, the system helps identify the competent mechanism. Transfer of personal data and initiation of a separate procedure take place in accordance with the law and applicable consent requirements.

5. MONITORING AND SYSTEM LEARNING

De-identified data can show not only cases that reached formal proceedings, but also types of reported harm, risk environments, barriers to reporting, support needs, referral pathways and points at which people discontinue engagement.

Reporting thereby becomes not only a service function, but also a source of evidence for policy.

Cross-cutting principle: CONTROL

At every stage, the person should understand:

what is collected → who can see it → why it is used → to whom it may be transferred → what happens next.

One national system does not require a single operator

The most straightforward response to fragmentation would be to create one central form and designate one institution to receive all reports.

The data from this study do not provide a sufficient basis for identifying one institution as the optimal operator of a future mechanism.

There is also a practical reason. Different institutions have different functions, powers, identification requirements and procedures.

For example, the Ukrainian Parliament Commissioner for Human Rights has a specific mandate in the field of preventing and combating discrimination and receives complaints concerning human-rights violations. At the same time, a formal submission to the Commissioner requires the applicant to be identified; anonymous submissions are not considered.

This is not inherently a problem. Formal legal procedures may legitimately require identification.

It does, however, demonstrate why **anonymous low-barrier reporting and a formal complaint are different functions**.

As noted above, 69.8% of respondents identified anonymity as a feature that would make a potential reporting mechanism more acceptable.

The solution may therefore lie not in changing every formal procedure, but in creating a clear connection between low-barrier reporting and existing competent mechanisms.

A networked model: multiple entry points, shared rules

As a policy-design option, a national system can be structured as a network of interoperable entry points rather than a single institution.

Level 1. Safe initial contact

Initial contact may take place through a human-rights or LGBTIQ+ organisation, a specialised online mechanism, an appropriate public human-rights mechanism, a trusted internal contact in a particular setting, or another channel operating according to common minimum standards.

The purpose of this level is to:

receive information → explain available options → assess needs → identify a possible next pathway.

In the relevant section of the study, 83.4% of respondents reported trust in LGBTIQ+ organisations. At the same time, high stated trust does not automatically translate into actual use of this route.

Civil society organisations may therefore form an important part of the trusted layer of the system, but trust alone does not resolve the problem of access.

Level 2. Initial assessment and routing

Following an initial report, the primary task is not to determine “guilt” or “innocence”, but to identify the nature of the person’s needs.

These may include information, psychological support, legal advice, safety assessment, documentation, a possible discrimination case, a possible media-related violation, indicators of an administrative or criminal offence, or an immediate risk requiring urgent intervention.

Where there are indications of a criminal or administrative offence or an immediate threat, the relevant formal channels of the National Police apply.

Sector-specific legal regimes apply to other types of cases. For example, content falling within the scope of the Law of Ukraine “On Media” is subject to a distinct regulatory framework.

Level 3. Routing based on the person’s decision and applicable consent requirements

Following initial assessment, the person is presented with available options:

- **leave the case documented only;**
- **access support;**
- **permit use of de-identified data;**
- **request assistance in preparing a formal submission;**
- **consent to the transfer of personal data to a specific institution — where such consent is required and legally applicable.**

The central principle is:

reporting does not automatically mean escalation to formal action.

Level 4. Formal response by competent institutions

At this level, the powers and procedures of specific institutions apply.

Ukrainian Parliament Commissioner for Human Rights — complaints concerning human-rights violations and discrimination, parliamentary oversight in the field of non-discrimination, and systemic monitoring.

National Police — cases indicating possible criminal or administrative offences and situations requiring an urgent response.

Sector-specific mechanisms — cases for which legislation establishes a specialised competence, including in the media field.

Education system — a trusted internal contact where safe, alongside an external confidential route so that a minor is not dependent exclusively on the administration of the same institution.

Civil society organisations — low-barrier documentation, primary support, legal navigation, referral and, with the person’s agreement where applicable, assistance in accessing a formal mechanism.

These actors do not need to have identical powers.

What is required is **interoperability between pathways**.

Shared minimum standards

Institutions may remain different. The logic of their interaction with the person should be consistent.

Before a report is submitted, it should be clear:

- **who the operator is;**
- **which data are collected;**
- **whether identification is required;**
- **what will happen after the report is submitted;**
- **which actions require a separate decision or consent.**

Each channel should collect only the personal data required for the selected function.

Storage of an incident report, contact with the person, use for statistics, transfer to another institution and preparation of a formal complaint should not be automatically bundled into one general consent.

Referral to another authority should not amount simply to “here is the contact — approach them yourself”. The person should understand why the route is relevant and what is likely to happen next.

Even where no further action is possible, the person should receive clear feedback.

Measuring results

If a system is assessed only by the number of formal cases, a substantial part of its function becomes invisible again.

A monitoring framework may separately track:

ACCESS — number of reports and completed initial contacts;

SAFETY — anonymous and identified reports, withdrawals of consent, incidents related to data handling;

SUPPORT — legal consultations, psychological assistance and referrals in situations involving safety risks;

ROUTING — cases transferred through the appropriate legal mechanism and, where required, on the basis of separate consent;

FEEDBACK — whether the person received confirmation and information on status and outcome;

VISIBILITY — types of experience that recur in de-identified data but do not progress to formal proceedings;

EQUALITY OF ACCESS — whether the mechanism is accessible to young people, transgender and non-binary people and other groups with different risk profiles.

This makes it possible to distinguish between **how many people received the support they needed** and **how many cases proceeded to formal action**.

One indicator cannot substitute for the other.

Practical conclusion

Ukraine does not necessarily need one new institution to take responsibility for all cases of anti-LGBTIQ+ hostility.

The findings point instead to the need for a different property of the system:

a person can enter through a safe and understandable channel without knowing the correct legal qualification in advance, receive the support they need, and move into the competent formal mechanism only when and to the extent consistent with the law and their informed decision.

Such a model does not eliminate the legal distinctions between hate speech, discrimination, threats and violence.

It makes legal and institutional complexity **the responsibility of the system rather than of the person seeking help**.

KEY REFERENCES

Council of Europe: [European Convention on Human Rights](#); [Recommendation CM/Rec\(2022\)16 on combating hate speech](#); [Recommendation CM/Rec\(2024\)4 on combating hate crime](#).

ECRI: [General Policy Recommendation No. 15 on combating hate speech](#); [General Policy Recommendation No. 17 on preventing and combating intolerance and discrimination against LGBTI persons](#).

Ukraine: [Law of Ukraine “On Media”, Article 36](#); [Criminal Code of Ukraine, Article 161](#); [Ukrainian Parliament Commissioner for Human Rights — applicant requirements](#); [2025 Annual Report](#).

Verkhovna Rada of Ukraine: [Draft Law No. 13597 — official parliamentary record \(including alternatives No. 13597-1 and No. 13597-2\)](#).

PUBLICATION INFORMATION

Volodymyr KOSENKO, Author / Director, HUMAN RIGHTS BUREAU “WE ARE!”, NGO • Kyiv, Ukraine • 2026

This assessment was produced with the financial support of the Council of Europe. The opinions expressed in this work are the responsibility of the author and do not necessarily reflect the official policy of the Council of Europe.