Το Ευρωπαϊκό Συμβούλιο Ψηφιακών Υπηρεσιών στις 24.9.26 ενέκρινε και εξέδωσε έγγραφο που καταγράφει καλές πρακτικές στο θέμα της ειδοποίησης για ύπαρξη υπόνοιας τέλεσης ποινικού αδικήματος σύμφωνα με το άρθρο 18 του Κανονισμού (ΕΕ) 2022/2065 για τις ψηφιακές υπηρεσίες.

Το άρθρο 18 του Κανονισμού (ΕΕ) 2022/2065 προνοεί ότι, όταν ένας πάροχος υπηρεσιών φιλοξενίας αντιληφθεί τυχόν πληροφορίες που εγείρουν υπόνοια ότι έχει διαπραχθεί, διαπράττεται ή είναι πιθανό να διαπραχθεί ποινικό αδίκημα το οποίο συνεπάγεται απειλή για τη ζωή ή την ασφάλεια ενός ή περισσότερων προσώπων, ενημερώνει αμέσως τις αρχές επιβολής του νόμου ή τις δικαστικές αρχές του οικείου κράτους μέλους ή των οικείων κρατών μελών σχετικά με την υπόνοιά του και παρέχει όλες τις διαθέσιμες σχετικές πληροφορίες. Η υποχρέωση αναφοράς βαρύνει όλους τους παρόχους υπηρεσιών φιλοξενίας οι οποίοι εμπίπτουν στο πεδίο εφαρμογής του Κανονισμού, ανεξαρτήτως μεγέθους.

Η σχετική ανακοίνωση, το έγγραφο και κατάλογος με τα σημεία επαφής κάθε κράτους μέλους, στους ακόλουθους συνδέσμους:

https://digital-strategy.ec.europa.eu/el/library/european-board-digital-services-adopts-good-practices-notify-suspected-criminal-offences-under

https://digital-strategy.ec.europa.eu/en/library/points-contact-notifying-suspected-criminal-offences

EUROPEAN BOARD FOR DIGITAL SERVICES

Notification of suspicions of criminal offences under Article 18 DSA

Good practices

September 2026

DISCLAIMER

This document is the result of work carried out in Working Group 7 - Orders and criminal issues of the European Board for Digital Services ("the Board"). It is intended solely as a practical resource for reference, is not legally binding, does not prejudge any future position of the Commission, the Board, the Digital Services Coordinators, and other authorities of the Member States, and is without prejudice to the interpretation of the Regulation (EU) 2022/2065 (Digital Services Act - DSA) by the Court of Justice of the European Union.

1. BACKGROUND . . . 5
2. SCOPE . . . 6
3. NOTION OF AWARENESS . . . 7
3.1 Sources of information . . . 7
3.2 Diligent assessment . . . 9
4. CRIMINAL OFFENCES TYPICALLY INVOLVING A THREAT TO LIFE OR SAFETY . . . 10
4.1 National annexes . . . 11
4.2 Notifications concerning suicide and/or self-harm . . . 11
5. PRACTICAL EXAMPLES OF INDICATORS . . . 12
6. IDENTIFICATION OF THE MEMBER STATE CONCERNED . . . 16
6.1 Internal assessment workflow . . . 16
6.2 Notifications where multiple Member States are concerned . . . 17
6.3 Notifications where the Member State concerned cannot be identified with reasonable certainty . . . 17
7. TRANSMISSION OF RELEVANT INFORMATION . . . 18
8. NOTIFICATION AND COMMUNICATION CHANNELS . . . 20
8.1 Single Points of Contacts (SPOCs) . . . 20
8.2 Technical solutions for transmission . . . 21
8.3 Interplay with other reporting obligations . . . 21
9. SUPERVISION OF COMPLIANCE . . . 22
10. REVIEW OF THE DOCUMENT . . . 23

1. BACKGROUND

Article 18 (1) of the Digital Services Act (DSA)[1] requires providers of hosting services (hereinafter referred to as "HSPs") to promptly inform the law enforcement or judicial authorities (hereinafter collectively referred to as "LEAs") of the Member State or Member States concerned when they become aware of any information giving rise to a suspicion that a criminal offence involving a threat to the life or safety of a person or persons has taken place, is taking place or is likely to take place. When notifying the LEAs, HSPs must provide all relevant information available.

Article 18 (2) DSA states that the Member State concerned refers to the Member State where the offence is suspected to have taken place, is taking place or is likely to take place, where the suspected offender resides or is located, or where the suspected victim resides or is located. When HSPs cannot identify with reasonable certainty the Member State concerned, they shall inform the Member State of establishment or legal representation, or inform Europol, or both.

The European Board of Digital Services (hereinafter referred to as "the Board") recalls that HSPs may find themselves in a position to become aware of information that is critical for enabling the LEAs to investigate criminal offences and to prevent a threat to a person's life or safety from materialising. Such a threat need not be directed at one or more identifiable individuals but may equally concern the public at large. The Board therefore reiterates the relevance of Article 18 DSA in circumstances entailing a threat to the life or safety of the general public, including where a criminal offence risks giving rise to a public crisis, and with regard to dangerous or life-threatening online challenges encouraging or instructing users to commit criminal offences.

The Board, following consultations among Digital Services Coordinators (hereinafter referred to as "DSCs") and with representatives of LEAs, observes that since the full entry into application of the DSA on 17 February 2024, several Member States have not received any or very few notifications under Article 18 DSA. There is a tendency among some HSPs to send notifications first and foremost only to Europol and, in some instances, to the incorrect Member State, although the Member State concerned could be identified with reasonable certainty. This may result in delays in notifying the LEAs which, in turn can have unwanted adverse effects in particular in cases of imminent or ongoing threats to life or safety. Furthermore, the Board notes, in the context of notifications received from HSPs, noticeable disparities in terms of numbers of notifications, range of offences notified and relevance of the information submitted, elements which are crucial in regard to actions by LEAs. Additionally, the Board notes that while DSCs are tasked to supervise compliance with Article 18 DSA under their jurisdiction, they frequently lack information about the notifications submitted by HSPs to LEAs, thereby creating significant challenges in the enforcement of the Article.

Considering the above, the Board notes inconsistencies in the application of Article 18 DSA by HSPs and takes the view that providing a repository of good practices and practical examples will contribute to improving the common understanding of the practical issues relating to the obligation set out in the Article.

The Board recalls that according to Recital 9 of the DSA, a key objective of the DSA is to ensure a safe, predictable and trusted online environment within which fundamental rights enshrined in the Charter of Fundamental Rights of the European Union are effectively protected. In particular, as set out in Recital 56, HSPs should respect applicable rules of Union or national law for the protection of the rights and freedoms of individuals, including the rights of the victim. The application of Article 18 should therefore be guided by full respect of these rights and freedoms.

(1) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC.

2. SCOPE

This document aims to serve as a practical resource to inform and promote the consistent application of the DSA across Member States, in accordance with Article 61 (2) (a) DSA, by providing a compendium of good practices and practical examples. It will assist the DSCs, as well as the Commission, in supervising compliance with Article 18 DSA. In doing so, it seeks to help ensure that HSPs comply with their obligation to promptly notify the LEAs in Member State(s) concerned and to provide all relevant information available to them.

This document is the result of a collaborative effort within the Working Group 7 of the Board. It takes due account of the results of a targeted consultation, conducted by the Commission services from 18 November 2025 to 9 January 2026 that gathered feedback from relevant stakeholders, including LEAs, HSPs, business associations and civil society organisations, on areas that warrant further clarification, as well as good practices and practical examples regarding the application of Article 18 DSA.[2]

As a result, this document includes:

- Considerations on the notion of awareness, including an overview of sources of relevant information (Section 3);
- A non-exhaustive overview of criminal offences that typically involve a threat to life or safety (Section 4);
- Practical examples to illustrate indicators that give rise to a suspicion of criminal offences involving a threat to life or safety (Section 5);
- Good practices for the identification of the Member State(s) concerned (Section 6);
- Good practices for the transmission of relevant information by HSPs to LEAs (Section 7);
- Examples of the notification and communication channels for the submission of notifications to the LEAs (Section 8);
- Considerations on the supervision of compliance with Article 18 DSA (Section 9).

While the practical examples draw on real-life events and cases, any names referred to in this document are fictional.

(2) Factual Summary Report on the targeted consultation on the notification of suspicions of criminal offences under DSA, available here: https://digital-strategy.ec.europa.eu/en/library/factual-summary-report-targeted-consultation-notification-suspicions-criminal-offences-under-dsa.

3. NOTION OF AWARENESS

The obligation imposed on HSPs to inform the LEA arises once they become aware of information giving rise to a suspicion of a criminal offence involving a threat to life or safety.

At the outset, the Board recalls that, where HSPs, upon becoming aware of an item of content, decide to remove or disable access to it (e.g., as it constitutes illegal content or violates its terms and conditions), this does not affect the obligation to notify the LEA under Article 18 DSA, where applicable. This includes the obligation to transmit the relevant information available.

3.1 Sources of information

Based on the feedback gathered, in particular the results of the targeted consultation and exchanges in the Working Group 7, the Board notes that HSPs may become aware of relevant information under Article 18 DSA through a variety of sources, including user notices, notices from trusted flaggers and voluntary mechanisms, as well as own-initiative monitoring and investigations. An overview of these sources as well as examples of good practices is provided hereafter.

Awareness triggered by user notices

Pursuant to Article 16 (1) DSA, HSPs are obliged to put in place notice and action mechanisms which allow any individual or entity to notify them of the presence on their service of specific items of information that they consider to be illegal content. Depending on the type of service, size and resources available, the HSP may also have additional reporting mechanisms in place, pursuant to other obligations under Union or Member State law in compliance with Union law, as well as mechanisms to allow users to report suspected violations of their own terms and conditions.

Such user notices and reports may concern items of information which, either in themselves, or in combination with the reasoning why the individual or entity alleges the information in question to be illegal or in violation of the terms and conditions, indicate a suspicion of a criminal offence involving a threat to life or safety.

Good practice: User notices

As required pursuant to Article 16 (1) DSA, ABC Gaming Forum provides a notice and action mechanism that allows users to notify items of information which they consider to be illegal content. ABC Gaming Forum assesses the notified content, taking into account the elements set out in Article 16 (2) DSA, in particular whether the explanation of the reasons why the notifier alleges the content to be illegal includes relevant indications of a criminal offence involving a threat to life or safety. ABC Gaming Forum voluntarily adds an option in the mechanism to allow users to flag that the notice indicates a threat to life or safety, to facilitate the assessment of notices by the provider. ABC Gaming Forum designs such voluntary option in a manner that does not affect the accessibility of the notice and action mechanism nor that mechanism's user friendliness.

Awareness triggered by trusted flagger notices and voluntary mechanisms

Pursuant to Article 22 DSA, HSPs which are online platforms, are obliged to ensure that notices submitted by entities that have been awarded the status of trusted flagger by DSCs, are given priority and are processed without undue delay. The expertise of trusted flaggers pertains to detecting, identifying and notifying specific types of illegal content, such as content related to child sexual abuse, trafficking in human beings or terrorism. More than 80 entities with diverse expertise have been awarded trusted flagger status by DSCs since the full entry into application of the DSA. In addition, HSPs may enter into voluntary mechanisms with external experts, such as civil society organisations, to address specific types of content that is incompatible with their terms and conditions.

While in principle any notice may include relevant information, notices received from trusted flaggers or by partners in the framework of voluntary mechanisms that have expertise in relevant crime areas are expected to be more accurate and therefore, can be of particular relevance for becoming aware of criminal offences involving threats to life or safety.

Awareness triggered by own-initiative measures

While pursuant to Article 8 DSA, no general obligation shall be imposed on HSPs to monitor the information transmitted or stored nor to proactively seek facts or circumstances indicating illegal activity, this does not prevent HSPs from voluntarily searching proactively for content indicating a criminal offence involving a threat to life or safety. In practice, the feedback gathered indicates that some HSPs carry out voluntary own-initiative monitoring or investigations on their service, including by means of automated systems and human reviewers, to identify content that is illegal or in violation of their terms and conditions. Such content may also give rise to a suspicion of a criminal offence under Article 18 DSA.

Good practice: Own-initiative measures

The terms and conditions of ABC Network explicitly prohibit certain type of content, including in particular threats to physically harm people, promotion or glorification of violence, hate speech and hateful behaviour, sexual abuse and exploitation, and harassment and bullying. ABC Network employs content moderation systems on its service to enforce its terms and conditions. Given the scale of uploaded content on its service, ABC Network implements automated detection systems, including machine learning models, to help detect violative and illegal content at scale. The detection systems can escalate high-severity content in all EU languages to relevant trust and safety teams with human reviewers with specialised knowledge and expertise, who conduct further contextual, semantic and language assessments.

3.2 Diligent assessment

The Board recalls that the obligation set out in Article 18 (1) DSA does not, in general, require HSPs to be certain that a criminal offence involving a threat to life or safety has taken place, is taking place or will take place. A mere suspicion to that effect suffices. Nonetheless, establishing such a suspicion, requires a diligent assessment of the information that the HSP becomes aware of.

Drawing on the feedback gathered, this section sets out examples of measures to support the assessment of information that HSPs become aware of through the relevant sources. In particular, the Board considers it good practice that the assessment involves human reviewers with specialised knowledge and expertise (e.g., in the relevant crime areas) to establish a suspicion under Article 18 DSA. Human oversight, expertise and accountability reduce risks of systematic over- or underreporting of notifications to LEAs.

Such measures may include:

- Conducting a regular assessment how the specific characteristics, nature and use of the service affect the categories of criminal offences that are present on the services.

- Establishing a set of internally defined criteria, signals and thresholds for automated detection and review systems to escalate suspected threats to life or safety to human reviewers. Machine learning models are continuously tested and validated, for example, by using specified evaluation metrics and overseen by humans.

- Establishing and regularly updating standard operating procedures (SOPs) that outline procedures and tactical steps to enable the assessment of relevant information by specialised human reviewers. SOPs are based on a set of internally defined criteria, signals and thresholds, considering for example:
  - Credibility and severity of a suspected threat, including the presence of identifiable victim(s) or location(s);
  - History of the associated user account(s);
  - Linguistic elements such as regional slang, coded language, or in-group jargon in all EU languages;
  - Aesthetic elements such as symbols, signs, and memes;
  - Expertise of the individual, entity or partner that notified the content, where applicable;
  - Other contextual and technical information.

- Holding regular internal trainings to ensure that the relevant teams are aware of and well-accustomed with the SOPs.

- Maintaining simple, clearly defined internal triaging and escalation pathways to allow human reviewers to quickly flag specific situations such as imminent or ongoing threats to life or safety to the appropriate team(s) and management.

- Appointing specifically trained human reviewers with specialised expertise and knowledge responsible for handling notifications, in particular for conducting a final review of the content and extracting the relevant information to be included in the notification to LEAs.

The Board notes that these measures are non-exhaustive examples and may vary, depending on the type of service, the size and the resources available to the HSP.

4. CRIMINAL OFFENCES TYPICALLY INVOLVING A THREAT TO LIFE OR SAFETY

There are certain types of criminal offences which **typically** involve a threat to the life or safety of a person or persons. The Board underlines that such offences encompass both, offences involving a threat to the life or safety of individual persons and offences posing a threat to the life and safety of the general public.

Based on the feedback gathered, this section provides a general, non-exhaustive list of categories of such criminal offences, including those harmonised on EU level, and subject to the implementation in the criminal law of the Member State concerned:

- Crimes against a person's life and/or physical integrity such as:
  - Intentional killing;
  - Manslaughter;
  - Bodily injury;
  - Torture;
  - Offences related to illicit trafficking in human organs and tissue.

- Crimes against a person's liberty such as:
  - Trafficking in human beings[3] including offences concerning exploitation of the prostitution or other forms of sexual exploitation, forced labour or services, exploitation of criminal activities, removal of organs, and exploitation of surrogacy, of forced marriage, or of illegal adoption;
  - Kidnapping, hostage-taking and abduction;
  - Aggravated extortion.

- Crimes against a person's sexual integrity and/or self-determination such as:
  - Sexual abuse and sexual exploitation of children[4] including the dissemination child sexual abuse material, solicitation of children for sexual purposes and sexual extortion;
  - Violence against women and domestic violence[5] including female genital mutilation, forced marriage, non-consensual sharing of intimate or manipulated material, cyber stalking, cyber harassment, and cyber incitement to violence or hatred;
  - Rape and sexual assault.

(3) Further specified in Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA (OJ L 101, 15.4.2011, p. 1) and amended by Directive (EU) 2024/1712 of the European Parliament and of the Council of 13 June 2024.
(4) Further specified in Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, pp. 1–14) and its (upcoming) recast.
(5) Further specified in Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence (OJ L, 2024/1385, 24.5.2024).

- Crimes against public safety and/or security such as:
  - Terrorism[6] including terrorist offences and offences relating to a terrorist group, offences related to terrorist activities, and terrorist content online[7];
  - Public incitement to violence or hatred directed against a person or a group of persons or a member of such a group defined by reference to protected characteristics;
  - Arson causing death or injury to persons.

In addition, certain types of crimes against public safety and/or security may involve a threat to life or safety of a person or persons, depending on the individual situation:

- Offences related to drugs, new psychoactive substances or precursors;
- Offences related to weapons, firearms, their parts and components, ammunition, explosives and their precursors;
- Offences related to the facilitation of unauthorised entry, transit or residence[8];
- Offences related to nuclear materials or other hazardous radioactive substances;
- Offences related to hazardous waste;
- Offences related to dangerous interference with road traffic as well as rail, ship and air traffic.

4.1 National annexes

Based on the feedback gathered, the Board notes that Member States' national criminal laws may specify additional criminal offences within or outside the above listed categories that involve threats to life or safety and are therefore captured by the obligation under Article 18 DSA. Where national annexes are available in a Member State, setting out additional or further specified offences that should be considered in their respective jurisdiction, the Board recommends that DSCs consider to publicly communicate them, for example, by publishing such annexes on their website or other appropriate means.

4.2 Notifications concerning suicide and/or self-harm

The feedback gathered demonstrates that, while suicide and/or self-harm by themselves in principle do not constitute a criminal offence under Union or national law, cases where suicide and/or self-harm is suspected to be linked to criminal conduct such as incitement, coercion, sextortion or grooming are considered to fall under the obligation of Article 18 DSA. Given the severity of the threat, the Board considers it good practice that in case of doubt, HSPs may still send a notification to the LEA. Even where suicide and/or self-harm related content does not indicate a criminal offence, such content may have to be reported under national online safety laws and/or via other voluntary expedited reporting channels for non-criminal threats to a person's life or safety.

(6) Further specified in Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, pp. 6–21).
(7) Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Text with EEA relevance) (OJ L 172, 17.5.2021, pp. 79–109).
(8) Further specified in Council Directive 2002/90/EC of 28 November 2002.

5. PRACTICAL EXAMPLES OF INDICATORS

The Board considers that indicators of suspected criminal offences involving threats to life or safety may either result directly from the item of content itself or from the content in combination with additional information available to HSPs, such as contextual and technical information, presence of identifiable victim(s) or location(s), or the area of expertise of the individual or entity that notified the HSP of the content (e.g., a trusted flagger specialised in detecting specific types of illegal content).

Based on the feedback gathered, this section provides a **non-exhaustive** overview of practical examples containing different types of information that, when assessed together by a human reviewer with specialised expertise and knowledge, give rise to a suspicion of an offence involving a threat to life or safety. The examples concern different types of hosting services, including online platforms (e.g., social media platform, gaming platform, discussion forums) and other hosting services (e.g., hosted chat groups, file sharing services, cloud services). These practical examples, while drawing on real-life documented cases, are **fictional**.

Example 1 (Category: Crimes against public safety and/or security)

Type of content: Textual content (posts on a social media platform).

Content: Incitement to commit violent attacks, including arson attacks on homes ("f*** deporting, start killing"). Some posts share a "hit list" containing names of locations and address details.

Additional information: A human review of the associated user accounts and the user engagement with the content, including the suspected locations confirms a credible threat.

Example 2 (Category: Crimes against a person's life and/or physical integrity)

Type of content: Textual and visual content (posts in a closed group on a social media platform)

Content: Explicit threats of bodily injury, including depictions of a knife, and directed towards a named individual.

Additional information: A human review of the associated user account, the group, and the engagement with the content, including the comments, confirms a credible threat.

Example 3 (Category: Crimes against a person's life and/or physical integrity)

Type of content: Textual content (posts in a discussion forum)

Content: Descriptions of ongoing preparations to commit a school shooting.

Additional information: A human review of the associated user account indicates that the location of the account is near the location of a school. Repeated uploads from the same IP address indicate real-time developments.

Example 4 (Category: Crimes against a person's sexual integrity and/or self-determination)

Type of content: Textual content (messages in a group chat hosted in the cloud)

Content: Detailed information and instructions on how to purchase a bottle of the liquid that is "tasteless and odourless" for drugging a person, indicating "Your wife won't feel anything and won't remember anything."

Additional information: A human review of the group chat indicates that it contains several messages from different user accounts, sharing practical tips and instructions on how to drug their partners for sexual assault and rape.

Example 5 (Category: Crimes against a person's sexual integrity and/or self-determination)

Type of content: Textual content (posts in a discussion forum)

Content: Explicit tips on luring potential minors into producing sexually explicit material before using it for coercion and extortion.

Additional information: The content was notified by a trusted flagger with specialised expertise in countering online grooming.

Example 6 (Category: Crimes against a person's liberty)

Type of content: Textual content (posts on a social media platform)

Content: Violent insults against an identifiable person, doxxing of that person in the form of a picture and the address of her supposed home and announcing that the user will wait for them and "make sure she will never walk again."

Additional information: While the information is at first ambiguous, a human review of the associated user account and its account history confirms a real-life event and credible threat.

Example 7 (Category: Crimes against a person's liberty and a person's sexual integrity)

Type of content: Visual content (video in a closed group on a social media platform)

Content: Video headline "New Girls just in", including depictions of transporting and harbouring suspected victims of human trafficking for sexual exploitation.

Additional information: A civil society organisation specialised in scraping the web for content indicating trafficking in human beings notified the content to the provider. A human review of the content, including a visual analysis, its metadata and the user account history confirms a credible threat.

Example 8 (Category: Crimes against a person's life and/or physical integrity)

Type of content: Visual content (live streamed video on a gaming platform)

Content: Live stream with several users coercing and encouraging another user to engage in acts of self-harm. The live stream shows a knife and a rope.

Additional information: Several user accounts comment on the live stream and instruct the depicted person to hurt themselves and their pet and family members.

Example 9 (Category: Crimes against public safety and/or security)

Type of content: Visual content (images in a public group chat hosted by a provider of a messenger service)

Content: Several images depicting a synagogue, firearms and ammunition, symbols of extremist ideology.

Additional information: A human review of the content, the associated user account and its chat history indicates the use of known antisemitic codes and dog whistles. The review reveals the real-life existence of the synagogue, confirming a credible threat of a violent attack against that location.

Example 10 (Category: Crimes against a person's sexual integrity and/or self-determination)

Type of content: Visual content (images in a closed group on a social media platform)

Content: Intimate imagery of a person with captions indicating that the images were taken and shared without the consent of the depicted person ("watch **** while asleep" and "...while passed out") as well as indicating past and present sexual abuse ("Comment what you would like me to do to her").

Additional information: A trusted flagger with specialised expertise in image-based abuse notified the content to the provider.

Example 11 (Category: Crimes against a person's life and/or physical integrity)

Type content: Visual and textual content (folder containing documents on file-sharing website)

Content: Manuals that provide "how-to" instructions and immediately actionable guidance for arson, beatings, stabbings (including a selection of bladed weapons and bodily places to strike), shootings, improvised explosive, and bioweapons manufacture (poisons and contamination of food and water supplies), along with operational and tactical instructions.

Additional information: Another user account, who had received the link to the file sharing folder on a gaming platform, reported the content to the provider.

Example 12 (Category: Crimes against public safety and/or security)

Type of content: Visual content (images in a public group on social media platform)

Content: Videos and images appear to depict a boat with a powerful engine being promoted for departing to enter into the territory of a Member State. There is no information on immigration or visa requirements, and the cost of transfer is excessive. There appears to be no life-saving equipment such as life jackets.

Additional information: A human review of the content, including a visual analysis, its metadata and the associated user account confirms a suspicion of facilitation of unauthorised entry into Member States, posing a credible threat to the life and safety of persons using such a transfer. The assessment reveals that the group contains several posts from different user accounts promoting entry into EU territory, including prices, departure points and contact numbers.

Example 13 (Category: Crimes against public safety and/or security)

Type of content: Visual content (live stream on social media platform)

Content: Live stream that appears to show a person intentionally driving at speed in the wrong direction on a motorway.

Additional information: A human review of the manner of driving, its apparent intent, speed and contraflow direction, confirms a threat to the life or safety of road users and the public in general.

Example 14 (Category: Crimes against a person's life and/or physical integrity)

Type of content: Audio content (voice messages in an online multi-player game)

Content: Concrete gun violence threats and bragging about access to firearms and munition. Mentions of a local supermarket.

Additional information: Another user account reported the content to the provider, identifying the person making the threats and warning about a planned violent attack in a supermarket.

6. IDENTIFICATION OF THE MEMBER STATE CONCERNED

Pursuant to Article 18 (1) DSA, HSPs shall inform the LEAs of the Member State(s) concerned. Article 18 (2) DSA sets out that this includes the Member State where the suspected offender and/or victim resides or is located as well as the location where the offence is suspected to have taken place, is taking place or is likely to take place, including where an offence is committed when entering into a Member State.

At the outset, it is noted that depending on the type of HSP, different data categories may be available to the provider and therefore the following assessment workflow should be considered as applicable in a given context.

6.1 Internal assessment workflow

Based on the feedback gathered, this section provides good practices for the HSP's assessment of the available information for the purpose of identifying the Member State(s) concerned.

First, the internal assessment may include an examination of the content item itself for any indications of the location where the suspected offence has taken place, is taking place or will likely be taking place as well as the location or residence of the suspected offender, or the location or residence of the suspected victim. For example, the content may already refer to a location or provide implicit information such as language and dialects, background, local landmarks, specific events, details such as signs/posters/products/t-shirts/electrical sockets, or typical trends in particular areas.

Next, an internal assessment may include an examination of technical information, where available, such as:

- IP address used when uploading the content, with exact timestamp;
- IP address history over time;
- Geolocation data such as GPS data within associated metadata;
- Basic Subscriber Information (BSI) such as account registration details, delivery addresses, billing addresses, banking details, telephone number with a national prefix, email addresses with a Country Code Top-Level Domain.

In addition, an internal assessment may include an examination of contextual information, where available, such as:

- Language(s) used in associated content (e.g., comments, captions);
- Language(s) used in associated user account name(s);
- Language(s) used in associated folders/file names;
- Implicit information in other associated user accounts and content.

6.2 Notifications where multiple Member States are concerned

The available information may indicate multiple Member States concerned. For example, the available information may indicate different locations for the suspected victim and the suspected offender. Based on the feedback gathered, in such cases, it is considered good practice that the competent LEAs of all identified concerned Member States are notified and that the notification should contain clear information of which other respective authority was notified in parallel.

6.3 Notifications where the Member State concerned cannot be identified with reasonable certainty

Pursuant to Article 18 (2) DSA, **only** in case the available information **does not give reasonable certainty** of the concerned Member State, HSPs shall notify the Member State of their establishment and/or Europol.

Accordingly, where, on the basis of the information available and the internal assessment, the HSP is unable to reliably identify one or more Member State(s) concerned (e.g., due to the use of location-masking technologies), or where the information indicates that the offence concerns exclusively a third-country, HSPs can resort to the Member State of their establishment and/or Europol as fall-back options. As outlined above, where HSPs inform both, the notification should contain clear information of which other respective authority was notified in parallel.

7. TRANSMISSION OF RELEVANT INFORMATION

Pursuant to Article 18 (1) DSA, when informing LEAs, HSPs shall transmit **all relevant information available** to them. Given the wide variety of hosting services, content concerned and information available, the Board notes that Article 18 DSA does not provide an exhaustive list of such information.

Recital 56 DSA provides further details by setting out that this information should include, **where relevant**, the content in question, and, if available, the time when the content was published, including the designated time zone, an explanation of its suspicion and the information necessary to locate and identify the relevant recipient of the service. The Board also recalls that Recital 56 DSA provides that the DSA does not provide the legal basis for profiling of users with a view to the possible identification of criminal offences by HSPs. Furthermore, it is recalled that HSPs should respect other applicable rules of Union or national law for the protection of the rights and freedoms of individuals when informing LEAs.

When determining which relevant information to share, the Board therefore considers it good practice for the HSP to take into account in particular the type of content and criminal offence as well as the level of urgency and affected rights and freedoms of the individuals concerned such as victim's rights[9] as well as the right to data protection.

In practice, the main purpose of providing available information is to allow the LEAs receiving the notification to take the **necessary** action, which include in particular:

- Responding directly to an imminent or ongoing threat to the life or safety of a person or persons;
- Assessing the criminal relevance of the notified content;
- Taking investigative measures such as issuing or obtaining an order to provide further information or to preserve evidence, where applicable.

The Board considers that the following information is, where available, **necessary and relevant** to allow the LEAs to take action and should therefore be provided by the HSP as a good practice when notifying the LEAs under Article 18 DSA:

- The respective item(s) of content (textual, visual or audio content in their respective file formats, screenshots) and corresponding information to locate the content on the service (e.g., exact URL or other available formats if the content has been removed or made inaccessible);
- An indication whether according to the HSP's internal assessment the threat to life or safety is imminent or ongoing or otherwise requires a prompt response by the LEAs, including the presence of identifiable victim(s) or location(s);
- A summary of the HSP's internal assessment, containing relevant information such as:
  - Information to concretise the relevant part of the content (e.g., a timestamp of a video), where applicable;
  - Information on whether the content has been reported by another entity to LEAs, where applicable;
  - Information on whether the respective user account shows indications of automated or coordinated inauthentic behaviour, where applicable.

(9) The Board recalls the application of the Directive 2012/29 establishing minimum standards on the rights, support and protection of victims of crime, and revised by Directive 2026/1472, with regard to any information concerning victims of crime, including the processing of their personal data.

Depending on the information processed by the HSP, the criminal offence and level of urgency, the Board considers that the notification by the HSP should include as necessary and relevant in addition to the above listed information, the following:

- Information to identify the suspected offender(s) and/or suspected victim(s) such as basic subscriber information (e.g., name, email address, user ID, phone number), source IP address used for login and/or upload, technical information (e.g., time of last login, device information). This may also include available information on third parties directly linked to the suspected offender(s) and/or victim(s) where identification is not possible via other means (e.g., related or shared user accounts, holders of payment instruments used by the suspected offender, holders of phone numbers used by the suspected offender);

- Information to locate the threat such as source IP address used for login and/or upload, geolocation data, billing address, information in the content, language settings;

- Precise timestamps when the content was uploaded and/or published including the time zone in UTC;

- User account history such as content removal, account suspensions, repeat offending behaviour, or linked accounts.

Good practice: Preservation of relevant information

WXZ Marketplace determines that an item of content indicates a criminal offence involving a threat to a person's safety. WXZ Marketplace immediately disables access to the content and promptly notifies the LEA in the Member State concerned. A human reviewer examines the available data, extracts and prepares the relevant information, and preserves it for purposes of transmitting it in response to potential subsequent requests or orders by LEAs, where applicable.

Based on the feedback gathered, the Board considers it good practice for HSPs to transfer relevant information in a structured, standardised and consistent manner. When transmitting via web-based portals or APIs, the technical interface typically already requires a clearly structured format for the data provided. For the transmission of information through other established channels, in particular via email, the Board notes that HSPs may rely on voluntary templates, for example, developed by national LEAs.

Good practice: Transmission of relevant information

WXZ Community becomes aware of a suspected criminal offence involving a threat to life. A human reviewer within the trust and safety team of WXZ Community reviews the available information and assesses whether it implies an imminent or ongoing threat. The reviewer extracts and structures the relevant information and submits the necessary information to the LEA of the identified Member State, using an established and consistent formatting for the notification. WXZ Community implements automated systems for streamlining the transmission however ensures human oversight and review of the transmitted information.

8. NOTIFICATION AND COMMUNICATION CHANNELS

The feedback gathered shows that for the receipt of notifications, LEAs and Europol rely on email communications and, in some case, on web-based portals established at national level. Some Member States in addition provide a dedicated telephone number to alert LEAs about an incoming or submitted notification through the established channels allowing the authority to mobilise the necessary resources in a timely manner. In particular, such telephone numbers should be used to notify the LEA of imminent or ongoing incidents in cases where the authority does not monitor the receipt of notifications on a 24/7 basis.

8.1 Single Points of Contacts (SPOCs)

The Board considers it good practice for LEAs to designate, or where already established, maintain and publicly communicate, for example on a website, a SPOC that can act as the first entry point for assessing and processing notifications under Article 18 DSA. Such SPOC may have 24/7 monitoring capacities available, in particular to respond to imminent or ongoing threats.

The Board notes that the Working Group 7 of the Board maintains and regularly updates a directory of POCs. The Commission services are distributing the directory to VLOPs. The Board encourages the DSCs to distribute the directory to HSPs established in their Member State. The Commission services and the DSCs may, where appropriate and with the explicit consent of the parties, make this information publicly available on their respective websites to allow HSPs to proactively identify the points of contact of LEAs.

Furthermore, the Board considers it good practice for HSPs to designate and publicly communicate a SPOC responsible for communicating and liaising with LEAs in all Member States and Europol. Depending on the size of and the available resources to the relevant HSP, such an individual or team may function as a 24/7 point of contact.

The establishment and operational readiness of SPOCs by both the LEAs in Member States and the HSPs help with clarifying roles on each side, enabling the prompt and structured submission of information as well as facilitating feedback loops and information requests, where necessary.

Voluntary partnerships

The feedback gathered shows that voluntary partnerships, such as networks and informal fora, which include both HSPs and LEAs have been established to focus on jointly addressing specific types of illegal online content or conduct. Such partnerships can, for example, inform context- and language-specific exchange of information between HSPs and LEAs, including the notification channels set up for the receipt of notifications under Article 18 DSA.

Good practice: Voluntary partnership between HSP and LEA

ABC Chat, an online platform hosting chatrooms, is targeted at the domestic audience of the Member State in which it is established, offering the service only in the official language of that Member State. The service is especially popular among minors. ABC Chat entered into a voluntary partnership with the respective LEA in the Member State, with a particular focus on addressing grooming of minors and sextortion on the service. The partnership includes regular exchanges on the notification channels, transmission practices and on service-specific crime areas and emerging threats.

8.2 Technical solutions for transmission

Where technical solutions such as web portals or APIs are available, such solutions are considered useful to enable efficient and standardised receipt of notifications. The Board therefore encourages DSCs to facilitate the onboarding of HSPs established in their Member State to use these solutions, where available.

The Board also notes that the Commission services work with Europol to support the development, maintenance and operation of a platform that can act as an EU-wide point of entry for receiving notifications pursuant to Article 18 DSA.[(10)] Such a platform will allow for the standardised intake of notifications across Member States. The Board therefore encourages the DSCs to support the work of the Commission services and Europol with respect to facilitating the future onboarding of HSPs established in their Member State to this platform.

8.3 Interplay with other reporting obligations

The Board notes that other Union legislation sets out similar reporting obligations to Article 18 DSA, in particular Article 14(5) Regulation (EU) 2021/784 (Terrorist Content Online Regulation - TCO Regulation) concerning terrorist content involving an imminent threat to life, and Article 9 Regulation (EU) 2019/1148 concerning suspicious transactions, thefts or disappearances of explosive precursors on online marketplaces.

The Commission analysed the way in which these provisions interact with Article 18 DSA in the report adopted pursuant to Article 91 (1) second paragraph DSA.[(11)] In particular, when an HSP becomes aware of terrorist content indicating an imminent threat to life, the TCO Regulation prevails as the more specific obligation for the notification of terrorist content.

Based on the feedback gathered, the Board considers it good practice for HSPs that notifications clearly indicate the specific reporting obligation (e.g., referring to Article 18 DSA) and are not sent in parallel under separate reporting obligations, to avoid duplicative or conflicting responses by the authorities. For example, if an HSP sends a notification under Article 14(5) TCO Regulation, it would not be necessary to additionally notify the same content under Article 18 DSA.

Furthermore, the Board considers that when an HSP notifies a LEA under Article 18 DSA in relation to a suspected terrorist or violent extremist incident, this may be considered by the affected LEA as a notification of a potential crisis under the “EU Online Crisis Response Framework”, a voluntary mechanism meant to prevent or reduce the virality of illegal online content related to a suspected violent extremist or terrorist attack. However, it is recalled that a notification under Article 18 DSA does not automatically trigger the activation of this Framework.

(10) Adaption of the platform ‘PERCI’ (Plateforme Européenne de Retraits de Contenus Illégaux sur Internet)
(11) Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the application of Article 33 of Regulation (EU) 2022/2065 and the interaction of that Regulation with other legal acts, SWD(2025) 268 final.

9. SUPERVISION OF COMPLIANCE

The DSA does not foresee any transparency reporting obligations for HSPs concerning the notifications under Article 18 DSA. The Board however takes the view that transparency on the receipt of notifications is a key requirement for informed and knowledge-based supervision of HSPs' compliance with Article 18 DSA.

The Board encourages DSCs to consult LEAs that receive and process notifications under Article 18 DSA on a regular basis. For example, the LEAs may produce reports in accordance with the applicable restrictions under national criminal procedural law, that provide statistics on the total number of the notifications received, for example disaggregated by:

- Name and type of HSP (e.g., social media platform, video-sharing platform, gaming platform);
- Criminal relevance in terms of involving a threat to life or safety (e.g., relevant/ non-relevant);
- Quality (sufficient/non-sufficient information to allow the LEA to take the next steps);
- Geographical relevance in terms of the identification of the Member State concerned (relevant, non-relevant);
- Type of criminal offence (crime areas).

In addition, the Board notes that the platform for communication between Europol, LEAs and HSPs (see Section 8.2. above) will offer the possibility to extract EU-wide statistical reports on the notifications registered on this platform.

Transparency reports published under Article 15 DSA can be of particular importance for the supervision of compliance. The Board therefore encourages DSCs to consider analysing these reports, specifically concerning the notices received in accordance with Article 16 DSA which may relate to relevant criminal offences. Such reports may increase knowledge about the scale and scope of potentially relevant illegal content with regard to Article 18 DSA that HSPs are aware of.

10. REVIEW OF THE DOCUMENT

This document provides good practices and practical examples drawing on the feedback received from the application of Article 18 DSA to date. It therefore may be reviewed and updated in view of the practical experiences, new criminal phenomena and emerging trends, new technological developments, new regulatory developments,[12] and changes in operational standards.

The Board will monitor the effectiveness and relevance of this document on a continuous basis and review the document, when necessary, in cooperation with the Commission services. This monitoring will also rely on the creation of supervision frameworks that facilitate regular reporting and transparency concerning the receipt of notifications under Article 18 DSA.

(12) For example, the proposed Regulation laying down rules to prevent and combat child sexual abuse may, when adopted and applicable, introduce an obligation for HSPs, when becoming aware of any information indicating the presence of potential online dissemination of child sexual abuse material and solicitation of children for sexual purposes, to promptly submit a report thereon to a newly established EU Centre.

