RECOMMENDATIONS

COMMISSION RECOMMENDATION (EU) 2018/334

of 1 March 2018

on measures to effectively tackle illegal content online

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292 thereof,

Whereas:

(1) Internet and service providers active on the internet contribute significantly to innovation, economic growth and job creation in the Union. Many of those service providers play an essential role in the digital economy by connecting business and citizens and by facilitating public debate and the distribution and reception of factual information, opinions and ideas. However, their services are in certain cases abused by third parties to carry out illegal activities online, for instance disseminating certain information relating to terrorism, child sexual abuse, illegal hate speech or infringements of consumer protection laws, which can undermine the trust of their users and damage their business models. In certain cases the service providers concerned might even gain some advantages from such activities, for instance as a consequence of the availability of copyright protected content without authorisation of the right holders.

(2) The presence of illegal content online has serious negative consequences for users, for other affected citizens and companies and for society at large. In the light of their central role and the technological means and capabilities associated with the services that they provide, online service providers have particular societal responsibilities to help tackle illegal content disseminated through the use of their services.

(3) Given that fast removal of or disabling of access to illegal content is often essential in order to limit wider dissemination and harm, those responsibilities imply inter alia that the service providers concerned should be able to take swift decisions as regards possible actions with respect to illegal content online. Those responsibilities also imply that they should put in place effective and appropriate safeguards, in particular with a view to ensuring that they act in a diligent and proportionate manner and to preventing the unintended removal of content which is not illegal.

(4) Many online service providers have acknowledged and acted upon those responsibilities. At the collective level, important progress has been made through voluntary arrangements of various kinds, including the EU Internet Forum on terrorist content online, the Code of Conduct on Countering Illegal Hate Speech Online and the Memorandum of Understanding on the Sale of Counterfeit Goods. However, notwithstanding this commitment and progress, illegal content online remains a serious problem within the Union.

(5) Concerned by a series of terrorist attacks in the EU and the proliferation of terrorist propaganda online, the European Council of 22-23 June 2017 stated that it 'expects industry to … develop new technology and tools to improve the automatic detection and removal of content that incites to terrorist acts. …' The European Parliament, in its resolution of 15 June 2017, urged those online platforms 'to strengthen measures to tackle illegal and harmful content'. The call for the companies to take a more proactive approach in protecting their users from terrorist content has been reiterated by Ministers of the Member States within the EU Internet Forum. As for intellectual property rights, in its Conclusions of 4 December 2014 on the enforcement of such rights, the Council called on the Commission to consider the use of tools available to identify intellectual property rights infringers and the role of intermediaries in assisting the fight against intellectual property rights infringements.

(6) On 28 September 2017, the Commission adopted a Communication with guidance on the responsibilities of online service providers in respect of illegal content online ([1]). In that Communication the Commission explained that it would assess whether additional measures were needed, inter alia by monitoring progress on the basis of voluntary arrangements. This Recommendation follows-up on that Communication, reflecting the level of ambition set out therein and giving effect thereto, while taking due account of and building on the important progress made through those voluntary arrangements.

(7) This Recommendation acknowledges that due account should be taken of the particularities of tackling different types of illegal content online and the specific responses that might be required, including through dedicated legislative measures. For instance, acknowledging the need for such specific legislative measures, on 25 May 2016 the Commission adopted a proposal for the amendment of Directive 2010/13/EU of the European Parliament and of the Council ([2]) in view of changing market realities. On 14 September 2016, it also adopted a proposal for a Directive on copyright in the Digital Single Market ([3]), which provides for an obligation for certain service providers to take, in cooperation with right holders, measures to ensure the functioning of agreements with right holders for the use of their works or other subject matter or to prevent the availability on their services of works or other subject matter identified by the rights holders through the cooperation with the service providers. This Recommendation leaves such legislative measures and proposals unaffected.

(8) Directive 2000/31/EC of the European Parliament and of the Council ([4]) contains liability exemptions which are, subject to certain conditions, available to certain online service providers, including providers of 'hosting' services within the meaning of its Article 14. In order to benefit from that liability exemption, hosting service providers are to act expeditiously to remove or disable access to illegal information that they store upon obtaining actual knowledge thereof and, as regards claims for damages, awareness of facts or circumstances from which the illegal activity or information is apparent. They can obtain such knowledge and awareness, inter alia, through notices submitted to them. As such, Directive 2000/31/EC constitutes the basis for the development of procedures for removing and disabling access to illegal information. That Directive also allows for the possibility for Member States of requiring the service providers concerned to apply a duty of care in respect of illegal content which they might store.

(9) When taking measures in respect of illegal content online, Member States are to respect the country of origin principle laid down in Directive 2000/31/EC. Accordingly, they may not, for reasons falling within the coordinated field as specified in that Directive, restrict the freedom to provide information society services by providers established in another Member State, subject however to the possibility of derogations under certain conditions set out in that Directive.

(10) In addition, several other acts of Union law provide for a legal framework in respect of certain particular types of illegal content that are available and disseminated online. In particular, Directive 2011/93/EU of the European Parliament and of the Council ([5]) requires Member States to take measures to remove web pages containing or disseminating child pornography and allows them to block access to such web pages, subject to certain safeguards. Directive (EU) 2017/541 of the European Parliament and of the Council ([6]), which is to be transposed into national law by 8 September 2018, contains similar provisions in respect of online content constituting public provocation to commit a terrorist offence. Directive (EU) 2017/541 also establishes minimum rules on the definition of criminal offences in the area of terrorist offences, offences related to a terrorist group and offences

([1]) COM(2017) 555 final of 28 September 2017.
([2]) Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (OJ L 95, 15.4.2010, p. 1). COM(2016) 287 final.
([3]) COM(2016) 593 final of 14 September 2016.
([4]) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).
([5]) 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, p. 1).
([6]) 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, p. 6).

related to terrorist activities. Pursuant to Directive 2004/48/EC of the European Parliament and of the Council ([1]), it is possible for competent judicial authorities to issue injunctions against intermediaries whose services are being used by a third party to infringe an intellectual property right.

(11) In particular against this background, in addition to the voluntary measures taken by certain online services providers, some Member States have adopted rules on 'notice-and-action' mechanisms since the adoption of Directive 2000/31/EC. Other Member States are considering adopting such rules. Those mechanisms generally seek to facilitate the notification of content which the notifying party considers to be illegal to the hosting service provider concerned ('notice'), pursuant to which that provider can decide whether or not it agrees with that assessment and wishes to remove or disable access to that content ('action'). There are increasing differences between such national rules. As a consequence, the service providers concerned can be subject to a range of legal requirements which are diverging as to their content and scope.

(12) In the interest of the internal market and the effectiveness of tackling illegal content online, and in order to safeguard the balanced approach that Directive 2000/31/EC seeks to ensure, it is necessary to set out certain main principles that should guide the activities of the Member States and of the service providers concerned in this regard.

(13) Those principles should be set out and applied in full respect for the fundamental rights protected in the Union's legal order and notably those guaranteed in the Charter of Fundamental Rights of the European Union ('the Charter'). Illegal content online should be tackled with proper and robust safeguards to ensure protection of the different fundamental rights at stake of all parties concerned. Those rights include, as the case may be, the freedom of expression, including the freedom to receive and impart information, the rights to respect for a person's private life and to the protection of personal data as well as the right to effective judicial protection of the users of the services concerned. They may also include the freedom to conduct a business, including the freedom of contract, of hosting service providers, as well as the rights of the child and the rights to protection of property, including intellectual property, to human dignity and to non-discrimination of certain other affected parties. In particular, decisions taken by hosting service providers to remove or disable access to content which they store should take due account of the fundamental rights and the legitimate interests of their users as well as of the central role which those providers tend to play in facilitating public debate and the distribution and reception of facts, opinions and ideas in accordance with the law.

(14) In accordance with the horizontal approach underlying the liability exemption laid down in Article 14 of Directive 2000/31/EC, this Recommendation should be applied to any type of content which is not in compliance with Union law or with the law of Member States, irrespective of the precise subject matter or nature of those laws. It is sufficient to take account of laws of Member States which are concerned by the service provision at issue, notably those of Member States the territory of which is that in which the hosting service provider is established or that in which the services are provided. In addition, when giving effect to this Recommendation, due account should be taken of the seriousness of, and any type of potential harm caused by, the illegal content, which can be closely related to the swiftness of any action taken, and of what can be reasonably expected from hosting services providers, considering where relevant the state of development and possible use of technologies. Due account should also be taken of the relevant differences that might exist between various types of illegal content and the actions to be taken to tackle them.

(15) Providers of hosting services play a particularly important role in tackling illegal content online, as they store information provided by and at the request of their users and give other users access thereto, often on a large scale. This Recommendation therefore primarily relates to the activities and responsibilities of those providers. However, where appropriate, the recommendations made can also be applied, *mutatis mutandis*, in relation to other affected online services providers. As the purpose of this Recommendation is to address risks related to illegal content online affecting consumers in the Union, it relates to the activities of all hosting service providers, irrespective of whether they are established in the Union or in a third country, provided that they direct their activities to consumers residing in the Union.

(16) Mechanisms for submitting notices to hosting service providers regarding content which is considered to be illegal content are an important means to tackle illegal content online. Such mechanisms should facilitate the

([1]) Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30.4.2004, p. 45).

notification by all individuals or entities which wish to do so. Therefore, those mechanisms should be easy to access and use for all users. However, hosting service providers should remain flexible, for instance as regards the reporting format or technology to be used, so as to allow for efficient solutions and to avoid disproportionate burdens on those providers.

(17) In accordance with the case law of the Court of Justice relating to Article 14 of Directive 2000/31/EC, notices should be sufficiently precise and adequately substantiated so as to allow the hosting service provider receiving them to take an informed and diligent decision as regards the effect to be given to the notice. It should therefore be ensured, as much as possible, that that standard is met. However, whether or not a given notice leads to knowledge or awareness within the meaning of Article 14 of that Directive is to be to be assessed in light of the specificities of the individual case at hand, bearing in mind that such knowledge or awareness can also be obtained in other manners than through notices.

(18) Possessing the contact details of the notice provider is generally not necessary for the hosting service provider to be able to take an informed and diligent decision on the follow-up to be given to the notice received. Making the provision of contact details a prerequisite for the submission of a notice would entail an obstacle to notification. However, the inclusion of the contact details is necessary for the hosting service provider to be able to provide feedback. Including his or her contact details should therefore be a possibility for the notice provider, without this being required.

(19) In order to enhance transparency and the accuracy of notice-and-action mechanisms and to allow for redress where needed, hosting service providers should, where they possess the contact details of notice providers and/or content providers, timely and adequately inform those persons of the steps taken in the context of the said mechanisms, in particular as regards their decisions on the requested removal or disabling of access to the content concerned. The information to be provided should be proportionate, in that it should correspond to the submissions made by the persons concerned in their notices or counter-notices, while allowing for appropriate and differentiated solutions and without leading to an excessive burden on the providers.

(20) In order to ensure transparency and fairness and to avoid the unintended removal of content which is not illegal content, content providers should, as a matter of principle, be informed of the decision to remove or disable access to the content stored at their request and be given the possibility to contest the decision through a counter-notice, with a view to having that decision reversed where appropriate, regardless of whether that decision was taken on the basis of a notice or a referral or pursuant to proactive measures by the hosting service provider.

(21) However, given the nature of the content at issue, the aim of such a counter-notice procedure and the additional burden it entails for hosting service providers, there is no justification for recommending to provide such information about that decision and that possibility to contest the decision where it is manifest that the content in question is illegal content and relates to serious criminal offences involving a threat to the life or safety of persons, such as offences specified in Directive (EU) 2017/541 and Directive 2011/93/EU. In addition, in certain cases, reasons of public policy and public security, and in particular reasons related to the prevention, investigation, detection and prosecution of criminal offences, may justify not directly providing that information to the content provider concerned. Therefore, hosting service providers should not do so where a competent authority has made a request to that effect, based on reasons of public policy and public security, for as long as that authority requested in light of those reasons. Insofar as this entails a restriction of the right to be informed in respect of the processing of personal data, the relevant conditions set out in Regulation (EU) 2016/679 of the European Parliament and of the Council ([1]) should be complied with.

(22) Notice-and-action mechanisms should in no way affect the rights of the parties involved to initiate legal proceedings, in accordance with the applicable law, in respect of any content which is considered to be illegal content or of any measures taken in this regard by hosting service providers. Mechanisms for the out-of-court settlement of disputes arising in this connection can be an important complement to judicial proceedings, especially where they allow for the effective, affordable and swift resolution of such disputes. Out-of-court settlements should therefore be encouraged, provided that the relevant mechanisms meet certain standards, notably in terms of procedural fairness, that the parties' access to court remains unaffected and that abuse is avoided.

([1]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

(23) In order to better assess the effectiveness of notice-and-action mechanisms and other activities of hosting service providers in respect of content considered to be illegal content and to ensure accountability, there should be transparency vis-à-vis the general public. Hosting service providers should therefore regularly publish reports about those mechanisms and other activities, which should be sufficiently complete and detailed to allow for an adequate insight. They should also provide for clarity *ex ante*, in their terms of service, on their policies on the removal or disabling of access to any content that they store, including illegal content.

(24) In addition to notice-and-action mechanisms, proportionate and specific proactive measures taken voluntarily by hosting service providers, including by using automated means in certain cases, can also be an important element in tackling illegal content online, without prejudice to Article 15(1) of Directive 2000/31/EC. In connection to such proactive measures, account should be taken of the situation of hosting service providers which, because of their size or the scale on which they operate, have only limited resources and expertise and of the need for effective and appropriate safeguards accompanying such measures.

(25) It can, in particular, be appropriate to take such proactive measures where the illegal character of the content has already been established or where the type of content is such that contextualisation is not essential. It can also depend on the nature, scale and purpose of the envisaged measures, the type of content at issue, on whether the content has been notified by law enforcement authorities or Europol and on whether action had already been taken in respect of the content because it is considered to be illegal content. With regard to child sexual abuse material in particular, hosting service providers should take proactive measures to detect and prevent the dissemination of such material, in line with the commitments undertaken in the context of the Global Alliance against Child Sexual Abuse Online.

(26) In this context, in its Communication of 28 September 2017 on tackling illegal content online, the Commission has set out its view that taking such voluntary proactive measures does not automatically lead to the hosting service provider concerned losing the benefit of the liability exemption provided for in Article 14 of Directive 2000/31/EC.

(27) It is essential that any measures to tackle illegal content online are subject to effective and appropriate safeguards aimed at ensuring that hosting service providers act in a diligent and proportionate manner when setting and enforcing their policies in respect of any content that they store, including illegal content, so as to ensure, in particular, that users can freely receive and impart information online in compliance with the applicable law. In addition to any safeguards laid down in the applicable law, for instance regarding the protection of personal data, particular safeguards, notably human oversight and verifications, should be provided for and applied where appropriate in relation to the use of automated means, so as to avoid any unintended and erroneous decisions.

(28) Smooth, effective and appropriate cooperation between competent authorities and hosting service providers when tackling illegal content online should be ensured. Such cooperation could benefit from the assistance of Europol where appropriate, for instance when combating terrorism and sexual abuse and sexual exploitation of children, child pornography and solicitation of children. In order to facilitate such cooperation, Member States and hosting service providers should designate points of contacts, and procedures should be established for the processing of notices submitted by those authorities as a matter of priority and with an appropriate degree of confidence as regards their accuracy, taking account of the particular expertise and responsibilities of those authorities. In order to effectively tackle certain particularly serious criminal offences, such as offences specified in Directive (EU) 2017/541 and Directive 2011/93/EU, which might come to the attention of hosting service providers when carrying out their activities, Member States should be encouraged to make use of the possibility set out in Article 15(2) of Directive 2000/31/EC to establish in law reporting obligations, in compliance with the applicable law, in particular Regulation (EU) 2016/679.

(29) In addition to competent authorities, certain individuals or entities, including non-governmental organisations and trade associations, might also have particular expertise and wish to take on, on a voluntary basis, certain responsibilities related to tackling illegal content online. In light of their added-value and the sometimes high numbers of notices involved, cooperation between such trusted flaggers and hosting service providers should be encouraged, in particular by treating the notices that they submit also as a matter of priority and with an appropriate degree of confidence as regards their accuracy. However, in accordance with their particular status,

that cooperation should only be open to individuals and entities which respect the values on which the Union is founded as set out in Article 2 of the Treaty on European Union and meet certain appropriate conditions, which should moreover be clear and objective and be made publicly available.

(30) Combating illegal content online requires a holistic approach, as such content often migrates easily from one hosting service provider to another and tends to exploit the weakest links in the chain. Cooperation, consisting in particular of the sharing on a voluntary basis of experiences, technological solutions and best practices, is therefore essential. Such cooperation is particularly important in respect of hosting service providers which, because of their size or the scale on which they operate, have only limited resources and expertise.

(31) Terrorism involves the unlawful and indiscriminate use of violence and intimidation against citizens. Terrorists have become increasingly reliant on the internet to disseminate terrorist propaganda, often deploying sophisticated methods to ensure swift and broad dissemination. Whilst progress has been made, especially in the context of the EU Internet Forum, there remains an urgent need for a swifter and more effective response to terrorist content online, in addition to the need for hosting service providers participating in the EU Internet Forum to fully live up to their commitments concerning effective and comprehensive reporting.

(32) In light of the particularities related to tackling terrorist content online, the recommendations relating to tackling illegal content generally should be complemented by certain recommendations which specifically relate to tackling terrorist content online, building on and consolidating efforts undertaken in the framework of the EU Internet Forum.

(33) Considering the particularly grave risks associated with terrorist content and hosting service providers' central role in the dissemination of such content, hosting service providers should take all reasonable measures so that to they do not allow terrorist content and if possible prevent hosting it, subject to their possibility to set and enforce their terms of service and the need for effective and appropriate safeguards and without prejudice to Article 14 of Directive 2000/31/EC.

(34) Those measures should, in particular, consist of cooperating with competent authorities and Europol in relation to referrals, which are a specific means for notifying hosting services providers which is adapted to the particularities of tackling terrorist content. Competent authorities and Europol, when submitting referrals, should be able to request the removal or disabling of access to content which they consider to be terrorist content either with reference to the relevant applicable laws or to the terms of service of the hosting service provider concerned. Those referral mechanisms should exist in addition to the mechanisms for submitting notices, including by trusted flaggers, which may also be used for notifying content considered to be terrorist content.

(35) Given that terrorist content is typically most harmful in the first hour of its appearance online and given the specific expertise and responsibilities of competent authorities and Europol, referrals should be assessed and, where appropriate, acted upon within one hour, as a general rule.

(36) Those measures to tackle terrorist content should also consist of proportionate and specific proactive measures, including by using automated means, in order to detect, identify and expeditiously remove or disable access to terrorist content and to ensure that terrorist content does not reappear, without prejudice to Article 15(1) of Directive 2000/31/EC. In this regard account should be taken of the need for adequate and effective safeguards accompanying such measures, in particular those recommended in Chapter II of this Recommendation.

(37) Cooperation, both among hosting service providers and between them and competent authorities, is of the utmost importance when seeking to tackle terrorist content online. In particular, technological tools that allow for automated content detection, such as the Database of Hashes, can help achieve the objective of preventing the dissemination of terrorist content across different hosting services. Such cooperation and the development, operation and sharing of such technological tools should be encouraged, making use of Europol's expertise where appropriate. Those cooperative efforts are particularly important to help enabling hosting service providers which, because of their size or the scale on which they operate, have limited resources and expertise to respond effectively and urgently to referrals and to take proactive measures, as recommended.

(38) As many relevant hosting service providers as possible should join those cooperative efforts and all participating hosting service providers should help optimise and maximise the use of those tools. The conclusion of working arrangements between all relevant parties, including where appropriate Europol, should also be encouraged, given that such arrangements can help ensuring a consistent and effective approach and allow for the exchange of relevant experiences and expertise.

(39) In order to ensure respect for the fundamental right to the protection of natural persons in relation to the processing of personal data, as well as the free movement of personal data, the processing of personal data in the context of any measures taken to give effect to this Recommendation should be in full compliance with the rules on data protection, in particular with Regulation (EU) 2016/679 and Directive (EU) 2016/680 of the European Parliament and of the Council ([1]), and should be monitored by the competent supervisory authorities.

(40) This Recommendation respects the fundamental rights and observes the principles recognised in particular by the Charter. In particular, this Recommendation seeks to ensure full respect for Articles 1, 7, 8, 10, 11, 16, 17, 21, 24 and 47 of the Charter.

(41) The Commission intends to closely monitor any actions taken in response to this Recommendation. Member States and hosting service providers should therefore be prepared to submit to the Commission, upon its request, all relevant information which they can reasonably be expected to provide in order to allow such monitoring. On the basis of the information thus obtained and all other available information, including reporting on the basis of the various voluntary arrangements, the Commission will assess the effects given to this Recommendation and determine whether additional steps, including proposing binding acts of Union law, are required. Given the particularities and urgency of tackling terrorist content online, that monitoring and assessment should be carried out based on detailed information and particularly quickly, within three months from the date of publication of this Recommendation, whereas for other illegal content it is appropriate to do so six months after the publication,

HAS ADOPTED THIS RECOMMENDATION:

CHAPTER I

Purpose and terminology

1. Member States and hosting service providers, in respect of content provided by content providers which they store at the request of those content providers, are encouraged to take effective, appropriate and proportionate measures to tackle illegal content online, in accordance with the principles set out in this Recommendation and in full compliance with the Charter, in particular the right to freedom of expression and information, and other applicable provisions of Union law, in particular as regards the protection of personal data, competition and electronic commerce.

2. This Recommendation builds on and consolidates the progress made in the framework of voluntary arrangements agreed between hosting service providers and other affected service providers regarding different types of illegal content. In the area of terrorism, it builds on and consolidates the progress made in the framework of the EU Internet Forum.

3. This Recommendation is without prejudice to the rights and obligations of Member States to take measures in respect of illegal content online in accordance with Union law, including the possibility for courts or administrative authorities of Member States, in accordance with their legal systems, of requiring hosting service providers to remove or disable access to illegal content. This Recommendation is also without prejudice to the position of hosting service providers under Directive 2000/31/EC and their possibility to set and enforce their terms of service in accordance with Union law and the laws of the Member States.

([1]) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

4. For the purpose of this Recommendation, the following terms are used:

(a) 'hosting service provider' means a provider of information society services consisting of the storage of information provided by the recipient of the service at his or her request, within the meaning of Article 14 of Directive 2000/31/EC, irrespective of its place of establishment, which directs its activities to consumers residing in the Union;

(b) 'illegal content' means any information which is not in compliance with Union law or the law of a Member State concerned;

(c) 'user' means any natural or legal person who is the recipient of the services provided by a hosting service provider;

(d) 'content provider' means a user who has submitted information that is, or that has been, stored at his or her request by a hosting service provider;

(e) 'notice' means any communication addressed to a hosting service provider submitted by a notice provider in respect of content stored by that hosting service provider which the notice provider considers to be illegal content, requesting the removal of or the disabling of access to that content by that hosting service provider on a voluntary basis;

(f) 'notice provider' means an individual or entity which has submitted a notice to a hosting service provider;

(g) 'trusted flagger' means an individual or entity which is considered by a hosting service provider to have particular expertise and responsibilities for the purposes of tackling illegal content online;

(h) 'terrorist content' means any information the dissemination of which amounts to offences specified in Directive (EU) 2017/541 or terrorist offences specified in the law of a Member State concerned, including the dissemination of relevant information produced by or attributable to terrorist groups or entities included in the relevant lists established by the Union or by the United Nations;

(i) 'law enforcement authorities' means the competent authorities designated by the Member States in accordance with their national law to carry out law enforcement tasks for the purposes of the prevention, investigation, detection or prosecution of criminal offences in connection to illegal content online;

(j) 'competent authorities' means the competent authorities designated by the Member States in accordance with their national law to carry out tasks which include tackling illegal content online, including law enforcement authorities and administrative authorities charged with enforcing law, irrespective of the nature or specific subject matter of that law, applicable in certain particular fields;

(k) 'referral' means any communication addressed to a hosting service provider submitted by a competent authority or by Europol in respect of content stored by that hosting service provider which that authority or Europol considers to be terrorist content, requesting the removal of or the disabling of access to that content by that hosting service provider on a voluntary basis.

CHAPTER II

General recommendations relating to all types of illegal content

Submitting and processing notices

5. Provision should be made for mechanisms to submit notices. Those mechanisms should be easy to access, user-friendly and allow for the submission of notices by electronic means.

6. Those mechanisms should allow for and encourage the submission of notices which are sufficiently precise and adequately substantiated to enable the hosting provider concerned to take an informed and diligent decision in respect of the content to which the notice relates, in particular whether or not that content is to be considered illegal content and is be removed or access thereto is be disabled. Those mechanisms should be such as to facilitate the provision of notices that contain an explanation of the reasons why the notice provider considers that content to be illegal content and a clear indication of the location of that content.

7. Notice providers should have the possibility, but not be required, to include their contact details in a notice. Where they decide to do so, their anonymity should be ensured towards the content provider.

8. Where the contact details of the notice provider are known to the hosting service provider, the hosting service provider should send a confirmation of receipt to the notice provider and should, without undue delay, inform the latter in a proportionate manner of its decision in respect of the content to which the notice relates.

Informing content providers and counter-notices

9. Where a hosting service provider decides to remove or disable access to any content that it stores because it considers the content to be illegal content, irrespective of the means used for detecting, identifying or removing or disabling of access to that content, and where the contact details of the content provider are known to the hosting service provider, the content provider should, without undue delay, be informed in a proportionate manner of that decision and of reasons for taking it, as well as of the possibility to contest that decision referred to in point 11.

10. However, point 9 should not apply where it is manifest that the content concerned is illegal content and relates to serious criminal offences involving a threat to the life, or safety of persons. In addition, hosting service providers should not provide the information referred to in that point where, and for as long as, a competent authority so requests for reasons of public policy and public security and in particular the prevention, investigation, detection and prosecution of criminal offences.

11. Content providers should be given the possibility to contest the decision by the hosting service provider referred to in point 9 within a reasonable time period, through the submission of a counter-notice to that hosting service provider. The mechanism to submit such counter-notices should be user-friendly and allow for submission by electronic means.

12. It should be ensured that hosting service providers take due account of any counter-notice that they receive. Where the counter-notice contains grounds for the hosting service provider to consider that the content to which the counter-notice relates is not to be considered illegal content, it should reverse its decision to remove or disable access to that content without undue delay, without prejudice to its possibility to set and enforce its terms of service in accordance with Union law and the laws of the Member States.

13. The content provider who submitted a counter-notice, as well as the notice provider concerned, should, where their contact details are known to the hosting service provider concerned, be informed, without undue delay, of the decision that the hosting service provider has taken in respect of the content concerned.

Out-of-court dispute settlement

14. Member States are encouraged to facilitate, where appropriate, out-of-court settlements to resolve disputes related to the removal of or disabling of access to illegal content. Any mechanisms for such out-of-court dispute settlement should be easily accessible, effective, transparent and impartial and should ensure that the settlements are fair and in compliance with the applicable law. Attempts to settle such disputes out-of-court should not affect the access to court of the parties concerned.

15. Where available in the Member State concerned, hosting service providers are encouraged to allow the use of out-of-court dispute settlement mechanisms.

Transparency

16. Hosting service providers should be encouraged to publish clear, easily understandable and sufficiently detailed explanations of their policy in respect of the removal or disabling of access to the content that they store, including content considered to be illegal content.

17. Hosting service providers should be encouraged to publish at regular intervals, preferably at least annually, reports on their activities relating to the removal and the disabling of content considered to be illegal content. Those reports should include, in particular, information on the amount and type of content removed, on the number of notices and counter-notices received and the time needed for taking action.

Proactive measures

18. Hosting service providers should be encouraged to take, where appropriate, proportionate and specific proactive measures in respect of illegal content. Such proactive measures could involve the use of automated means for the detection of illegal content only where appropriate and proportionate and subject to effective and appropriate safeguards, in particular the safeguards referred to in points 19 and 20.

Safeguards

19. In order to avoid removal of content which is not illegal content, without prejudice to the possibility for hosting service providers to set and enforce their terms of service in accordance with Union law and the laws of the Member States, there should be effective and appropriate safeguards to ensure that hosting service providers act in a diligent and proportionate manner in respect of content that they store, in particular when processing notices and counter-notices and when deciding on the possible removal of or disabling of access to content considered to be illegal content.

20. Where hosting service providers use automated means in respect of content that they store, effective and appropriate safeguards should be provided to ensure that decisions taken concerning that content, in particular decisions to remove or disable access to content considered to be illegal content, are accurate and well-founded. Such safeguards should consist, in particular, of human oversight and verifications, where appropriate and, in any event, where a detailed assessment of the relevant context is required in order to determine whether or not the content is to be considered illegal content.

Protection against abusive behaviour

21. Effective and appropriate measures should be taken to prevent the submission of, or the taking of action upon, notices or counter-notices that are submitted in bad faith and other forms of abusive behaviour related to the recommended measures to tackle illegal content online set out in this Recommendation.

Cooperation between hosting services providers and Member States

22. Member States and hosting service providers should designate points of contact for matters relating to illegal content online.

23. Fast-track procedures should be provided to process notices submitted by competent authorities.

24. Member States are encouraged to establish legal obligations for hosting service providers to promptly inform law enforcement authorities, for the purposes of the prevention, investigation, detection or prosecution of criminal offences, of any evidence of alleged serious criminal offences involving a threat to the life or safety of persons obtained in the context of their activities for the removal or disabling of access to illegal content, in compliance with the applicable legal requirements, in particular regarding the protection of personal data protection, including Regulation (EU) 2016/679.

Cooperation between hosting services providers and trusted flaggers

25. Cooperation between hosting service providers and trusted flaggers should be encouraged. In particular, fast-track procedures should be provided to process notices submitted by trusted flaggers.

26. Hosting service providers should be encouraged to publish clear and objective conditions for determining which individuals or entities they consider as trusted flaggers.

27. Those conditions should aim to ensure that the individuals or entities concerned have the necessary expertise and carry out their activities as trusted flaggers in a diligent and objective manner, based on respect for the values on which the Union is founded.

Cooperation between hosting service providers

28. Hosting service providers should, where appropriate, share experiences, technological solutions and best practices to tackle illegal content online among each other and in particular with hosting service providers which, because of their size or the scale on which they operate, have limited resources and expertise, including in the context of ongoing cooperation between hosting service providers through codes of conduct, memoranda of understanding and other voluntary arrangements.

CHAPTER III

Specific recommendations relating to terrorist content

General

29. The specific recommendations relating to terrorist content set out in this Chapter apply in addition to the general recommendations set out in Chapter II.

30. Hosting service providers should expressly set out in their terms of service that they will not store terrorist content.

31. Hosting service providers should take measures so that they do not store terrorist content, in particular as regards referrals, proactive measures and cooperation in accordance with points 32 to 40.

Submitting and processing referrals

32. Member States should ensure that their competent authorities have the capability and sufficient resources to effectively detect and identify terrorist content and to submit referrals to the hosting service providers concerned, in particular through national internet referral units and in cooperation with the EU Internet Referral Unit at Europol.

33. Provision should be made for mechanisms allowing for the submission of referrals. Fast-track procedures should be provided to process referrals, in particular referrals submitted by national internet referral units and by the EU Internet Referral Unit at Europol.

34. Hosting service providers should, without undue delay, send confirmations of receipt of referrals and inform the competent authority or Europol of their decisions in respect of the content to which the referrals relate, indicating, as the case may be, when the content was removed or access thereto was disabled or why they decided not to remove or to disable access to the content.

35. Hosting service providers should assess and, where appropriate, remove or disable access to content identified in referrals, as a general rule, within one hour from the moment at which they received the referral.

Proactive measures

36. Hosting service providers should take proportionate and specific proactive measures, including by using automated means, in order to detect, identify and expeditiously remove or disable access to terrorist content.

37. Hosting service providers should take proportionate and specific proactive measures, including by using automated means, in order to immediately prevent content providers from re-submitting content which has already been removed or to which access has already been disabled because it is considered to be terrorist content.

Cooperation

38. In order to prevent the dissemination of terrorist content across different hosting services, hosting service providers should be encouraged to cooperate through the sharing and optimisation of effective, appropriate and proportionate technological tools, including such tools that allow for automated content detection. Where technologically possible, all relevant formats through which terrorist content is disseminated should be captured. Such cooperation should include, in particular, hosting service providers which, because of their size or the scale on which they operate, have limited resources and expertise.

39. Hosting service providers should be encouraged to take the necessary measures for the proper functioning and improvement of the tools referred to in point 38, in particular by providing identifiers relating to all content considered to be terrorist content and by fully exploiting the possibilities of those tools.

40. Competent authorities and hosting service providers should conclude working arrangements, where appropriate also with Europol, on matters relating to terrorist content online, including for enhancing the understanding of terrorist activities online, improving referral mechanisms, preventing unnecessary duplication of efforts and facilitating requests by law enforcement authorities for the purposes of criminal investigations in relation to terrorism.

CHAPTER IV

Provision of information

41. Member States should, at regular intervals and preferably every three months, report to the Commission on the referrals submitted by their competent authorities and the decisions taken by hosting service providers upon those referrals, as well as on their cooperation with hosting service providers relating to tackling terrorist content.

42. In order to allow for the monitoring of the effects given to this Recommendation as regards terrorist content at the latest three months from the date of its publication, hosting service providers should submit to the Commission, upon its request, all relevant information to allow for such monitoring. That information may include in particular, information on the amount of content which has been removed or to which access has been disabled, either pursuant to referrals or notices or pursuant to the taking of proactive measures and the use of automated means. It may also include the number of referrals received and the time needed for taking action, as well as the amount of content prevented from being submitted or re-submitted through the use of automated content detection and other technological tools.

43. In order to allow for the monitoring of the effects given to this Recommendation as regards illegal content, other than terrorist content, at the latest six months from the date of its publication Member States and hosting service providers should submit to the Commission, upon its request, all relevant information to allow for such monitoring.

Done at Brussels, 1 March 2018.

For the Commission
Andrus ANSIP
Vice-President