Annex

CROSSBORDER DISSEMINATION OF ONLINE CONTENT

Current and Possible Future Regulation of the Online Environment with a Focus on the EU E-Commerce Directive

This Annex reprints or lists the provisions or extracts from recommendations in particular relevant in the context of the dissemination of online content.

I. EU Primary Law und Fundamental Rights and Freedoms

In this part of the Annex we are not reprinting provisions of the EU Treaties, the EU Charter of Fundamental Rights or the European. Convention on Human. Rights, but only listing the especially relevant provisions in the context of the study. For each legal source an easily accessible online text is mentioned.

Treaty on European Union, *OJ C 326, 26.10.2012, p. 13–390* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012M%2FTXT
Art. 2, 3, 4, 5, 7, 49.

Treaty on the Functioning of the European Union, *OJ C 326, 26.10.2012, p. 47–390* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT
Art. 3, 4, 6, 28, 29, 49 – 55, 56 – 62, 114, 167.

Charter of Fundamental Rights of the European Union, *OJ C 326, 26.10.2012, p. 391–407* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT
Art. 1, 6, 7, 8, 11, 14, 15, 17, 24, 51, 52.

European Convention on Human Rights https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=
Art. 2, 3, 6, 8, 10, 11, Art. 1 of 1st amending Protocol

II. EU Secondary Law (in force and proposed)

A. e-Commerce Directive

Directive 2000/31/EC, *OJ L 178, 17.7.2000, p. 1–16* https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031
Recital 5
The development of information society services within the Community is hampered by a number of legal obstacles to the proper functioning of the internal market which make less attractive the exercise of the freedom of establishment and the freedom to provide services; these obstacles arise from divergences in legislation and from the legal uncertainty as to which national rules apply to such services; in the absence of coordination and adjustment of legislation in the relevant areas, obstacles might be justified in the light of the case-law of the Court of Justice of the European Communities; legal uncertainty exists with regard to the extent to which Member States may control services originating from another Member State.
Recital 19
The place at which a service provider is established should be determined in conformity with the case-law of the Court of Justice according to which the concept of establishment involves the actual pursuit of an economic activity through a fixed establishment for an indefinite period; this requirement is also fulfilled where a company is constituted for a given period; the place of establishment of a company providing services via an Internet website is not the place at which the technology supporting its website is located or the place at which its website is accessible but the place where it pursues its economic activity; in cases where a provider has several places of establishment it is important to determine from which place of establishment the service concerned is provided; in cases where it is difficult to determine from which of several places of establishment a given service is provided, this is the place where the provider has the centre of his activities relating to this particular service.
Recital 22
Information society services should be supervised at the source of the activity, in order to ensure an effective protection of public interest objectives; to that end, it is necessary to ensure that the competent authority provides such protection not only for the citizens of its own country but for all Community citizens; in order to improve mutual trust between Member States, it is essential to state clearly this responsibility on the part of the Member State where the services originate; moreover, in order to effectively guarantee freedom to provide services and legal certainty for suppliers and recipients of services, such information society services should in principle be subject to the law of the Member State in which the service provider is established.
Recital 24
In the context of this Directive, notwithstanding the rule on the control at source of information society services, it is legitimate under the conditions established in this Directive for Member States to take measures to restrict the free movement of information society services.
Recital 40
Both existing and emerging disparities in Member States' legislation and case-law concerning liability of service providers acting as intermediaries prevent the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition; service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities; this Directive should constitute the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information; such mechanisms could be developed on the basis of voluntary agreements between all parties concerned and should be encouraged by Member States; it is in the interest of all parties involved in the provision of information society services to adopt and implement such procedures; the provisions of this Directive relating to liability should not preclude the

development and effective operation, by the different interested parties, of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology within the limits laid down by Directives 95/46/EC and 97/66/EC.

Recital 41

This Directive strikes a balance between the different interests at stake and establishes principles upon which industry agreements and standards can be based.

Recital 46

In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level; this Directive does not affect Member States' possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information.

Recital 47

Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation.

Recital 48

This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.

Recital 49

Member States and the Commission are to encourage the drawing-up of codes of conduct; this is not to impair the voluntary nature of such codes and the possibility for interested parties of deciding freely whether to adhere to such codes.

Recital 57

The Court of Justice has consistently held that a Member State retains the right to take measures against a service provider that is established in another Member State but directs all or most of his activity to the territory of the first Member State if the choice of establishment was made with a view to evading the legislation that would have applied to the provider had he been established on the territory of the first Member State.

Recital 58

This Directive should not apply to services supplied by service providers established in a third country; in view of the global dimension of electronic commerce, it is, however, appropriate to ensure that the Community rules are consistent with international rules; this Directive is without prejudice to the results of discussions within international organisations (amongst others WTO, OECD, Uncitral) on legal issues.

Recital 59

Despite the global nature of electronic communications, coordination of national regulatory measures at European Union level is necessary in order to avoid fragmentation of the internal market, and for the establishment of an appropriate European regulatory framework; such coordination should also contribute to the establishment of a common and strong negotiating position in international forums.

Recital 63

The adoption of this Directive will not prevent the Member States from taking into account the various social, societal and cultural implications which are inherent in the advent of the information society; in particular it should not hinder measures which Member States might adopt in conformity with Community law to achieve social, cultural and democratic goals taking into account their linguistic diversity, national and regional specificities as well as their cultural heritage, and to ensure and maintain public access to the widest possible range of information society services; in any case, the development of the information society is to ensure that Community citizens can have access to the cultural European heritage provided in the digital environment.

Article 2
Definitions

For the purpose of this Directive, the following terms shall bear the following meanings:
(a) "information society services": services within the meaning of Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC;
(b) "service provider": any natural or legal person providing an information society service;
(c) "established service provider": a service provider who effectively pursues an economic activity using a fixed establishment for an indefinite period. The presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider;
(d) "recipient of the service": any natural or legal person who, for professional ends or otherwise, uses an information society service, in particular for the purposes of seeking information or making it accessible;
(e) "consumer": any natural person who is acting for purposes which are outside his or her trade, business or profession;
(f) "commercial communication": any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organisation or person pursuing a commercial, industrial or craft activity or exercising a regulated profession. The following do not in themselves constitute commercial communications:
- information allowing direct access to the activity of the company, organisation or person, in particular a domain name or an electronic-mail address,
- communications relating to the goods, services or image of the company, organisation or person compiled in an independent manner, particularly when this is without financial consideration;
(g) "regulated profession": any profession within the meaning of either Article 1(d) of Council Directive 89/48/EEC of 21 December 1988 on a general system for the recognition of higher-education diplomas awarded on completion of professional education and training of at least three-years' duration or of Article 1(f) of Council Directive 92/51/EEC of 18 June 1992 on a second general system for the recognition of professional education and training to supplement Directive 89/48/EEC;
(h) "coordinated field": requirements laid down in Member States' legal systems applicable to information society service providers or information society services, regardless of whether they are of a general nature or specifically designed for them.
(i) The coordinated field concerns requirements with which the service provider has to comply in respect of:
- the taking up of the activity of an information society service, such as requirements concerning qualifications, authorisation or notification,
- the pursuit of the activity of an information society service, such as requirements concerning the behaviour of the service provider, requirements regarding the quality or content of the service including those applicable to advertising and contracts, or requirements concerning the liability of the service provider;
(ii) The coordinated field does not cover requirements such as:
- requirements applicable to goods as such,

- requirements applicable to the delivery of goods,
- requirements applicable to services not provided by electronic means.

Article 3
Internal market

1. Each Member State shall ensure that the information society services provided by a service provider established on its territory comply with the national provisions applicable in the Member State in question which fall within the coordinated field.
2. Member States may not, for reasons falling within the coordinated field, restrict the freedom to provide information society services from another Member State.
3. Paragraphs 1 and 2 shall not apply to the fields referred to in the Annex.
4. Member States may take measures to derogate from paragraph 2 in respect of a given information society service if the following conditions are fulfilled:
(a) the measures shall be:
(i) necessary for one of the following reasons:
- public policy, in particular the prevention, investigation, detection and prosecution of criminal offences, including the protection of minors and the fight against any incitement to hatred on grounds of race, sex, religion or nationality, and violations of human dignity concerning individual persons,
- the protection of public health,
- public security, including the safeguarding of national security and defence,
- the protection of consumers, including investors;
(ii) taken against a given information society service which prejudices the objectives referred to in point (i) or which presents a serious and grave risk of prejudice to those objectives;
(iii) proportionate to those objectives;
(b) before taking the measures in question and without prejudice to court proceedings, including preliminary proceedings and acts carried out in the framework of a criminal investigation, the Member State has:
- asked the Member State referred to in paragraph 1 to take measures and the latter did not take such measures, or they were inadequate,
- notified the Commission and the Member State referred to in paragraph 1 of its intention to take such measures.
5. Member States may, in the case of urgency, derogate from the conditions stipulated in paragraph 4(b). Where this is the case, the measures shall be notified in the shortest possible time to the Commission and to the Member State referred to in paragraph 1, indicating the reasons for which the Member State considers that there is urgency.
6. Without prejudice to the Member State's possibility of proceeding with the measures in question, the Commission shall examine the compatibility of the notified measures with Community law in the shortest possible time; where it comes to the conclusion that the measure is incompatible with Community law, the Commission shall ask the Member State in question to refrain from taking any proposed measures or urgently to put an end to the measures in question.

Article 12
“Mere conduit”

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:
(a) does not initiate the transmission;
(b) does not select the receiver of the transmission; and
(c) does not select or modify the information contained in the transmission.
2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.
3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 13
“Caching”

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:

(a) the provider does not modify the information;

(b) the provider complies with conditions on access to the information;

(c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;

(d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and

(e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 14
“Hosting”

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

Article 15
No general obligation to monitor

1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

Article 16
Codes of conduct

1. Member States and the Commission shall encourage:

(a) the drawing up of codes of conduct at Community level, by trade, professional and consumer associations or organisations, designed to contribute to the proper implementation of Articles 5 to 15;

(b) the voluntary transmission of draft codes of conduct at national or Community level to the Commission;

(c) the accessibility of these codes of conduct in the Community languages by electronic means;

(d) the communication to the Member States and the Commission, by trade, professional and consumer associations or organisations, of their assessment of the application of their codes of conduct and their impact upon practices, habits or customs relating to electronic commerce;

(e) the drawing up of codes of conduct regarding the protection of minors and human dignity.

2. Member States and the Commission shall encourage the involvement of associations or organisations representing consumers in the drafting and implementation of codes of conduct affecting their interests and drawn up in accordance with paragraph 1(a). Where appropriate, to take account of their specific needs, associations representing the visually impaired and disabled should be consulted.

Article 19
Cooperation

1. Member States shall have adequate means of supervision and investigation necessary to implement this Directive effectively and shall ensure that service providers supply them with the requisite information.

2. Member States shall cooperate with other Member States; they shall, to that end, appoint one or several contact points, whose details they shall communicate to the other Member States and to the Commission.

3. Member States shall, as quickly as possible, and in conformity with national law, provide the assistance and information requested by other Member States or by the Commission, including by appropriate electronic means.

4. Member States shall establish contact points which shall be accessible at least by electronic means and from which recipients and service providers may:

(a) obtain general information on contractual rights and obligations as well as on the complaint and redress mechanisms available in the event of disputes, including practical aspects involved in the use of such mechanisms;

(b) obtain the details of authorities, associations or organisations from which they may obtain further information or practical assistance.

5. Member States shall encourage the communication to the Commission of any significant administrative or judicial decisions taken in their territory regarding disputes relating to information society services and practices, usages and customs relating to electronic commerce. The Commission shall communicate these decisions to the other Member States.

B. Audiovisual Media Services Directive

Directive (EU) 2018/1808, *OJ L 303, 28.11.2018, p. 69–92*

https://eur-lex.europa.eu/eli/dir/2018/1808/oj

synopsis and unofficial codified version of EMR: https://emr-sb.de/synopsis-avms/

Recital 1

The last substantive amendment to Council Directive 89/552/EEC, subsequently codified by Directive 2010/13/EU of the European Parliament and of the Council, was made in 2007 with the adoption of Directive 2007/65/EC of the European Parliament and of the Council. Since then, the audiovisual media services market has evolved significantly and rapidly due to the ongoing convergence of television and internet services. Technical developments have allowed for new types of services and user experiences. Viewing habits, particularly those of younger generations, have changed significantly. While the main TV screen remains an important device for sharing audiovisual experiences, many viewers have moved to other, portable devices to watch audiovisual content. Traditional TV content still accounts for a major share of the average daily viewing time.
However, new types of content, such as video clips or user-generated content, have gained an increasing importance and new players, including providers of video-on-demand services and video-sharing platforms, are now well-established. This convergence of media requires an updated legal framework in order to reflect developments in the market and to achieve a balance between access to online content services, consumer protection and competitiveness.

Recital 3

Directive 2010/13/EU should remain applicable only to those services the principal purpose of which is the provision of programmes in order to inform, entertain or educate. The principal purpose requirement should also be considered to be met if the service has audiovisual content and form which are dissociable from the main activity of the service provider, such as stand-alone parts of online newspapers featuring audiovisual programmes or user-generated videos where those parts can be considered dissociable from their main activity. A service should be considered to be merely an indissociable complement to the main activity as a result of the links between the audiovisual offer and the main activity such as providing news in written form. As such, channels or any other audiovisual services under the editorial responsibility of a provider can constitute audiovisual media services in themselves, even if they are offered on a video-sharing platform which is characterised by the absence of editorial responsibility. In such cases, it will fall to the providers with editorial responsibility to comply with Directive 2010/13/EU.

Recital 4

Video-sharing platform services provide audiovisual content which is increasingly accessed by the general public, in particular by young people. This is also true with regard to social media services, which have become an important medium to share information and to entertain and educate, including by providing access to programmes and user-generated videos. Those social media services need to be included in the scope of Directive 2010/13/EU because they compete for the same audiences and revenues as audiovisual media services. Furthermore, they also have a considerable impact in that they facilitate the possibility for users to shape and influence the opinions of other users. Therefore, in order to protect minors from harmful content and all citizens from incitement to hatred, violence and terrorism, those services should be covered by Directive 2010/13/EU to the extent that they meet the definition of a video-sharing platform service.

Recital 5

While the aim of Directive 2010/13/EU is not to regulate social media services as such, a social media service should be covered if the provision of programmes and user-generated videos constitutes an essential functionality of that service. The provision of programmes and user-generated videos could be considered to constitute an essential functionality of the social media service if the audiovisual content is not merely ancillary to, or does not constitute a minor part of, the activities of that social media service. In order to ensure clarity, effectiveness and consistency of implementation, the Commission should, where necessary, issue guidelines, after consulting the Contact

Committee, on the practical application of the essential functionality criterion of the definition of a ‘video-sharing platform service’. Those guidelines should be drafted with due regard for the general public interest objectives to be achieved by the measures to be taken by video-sharing platform providers and the right to freedom of expression

Recital 12

In its Communication to the European Parliament and to the Council on Better Regulation for Better Results – an EU Agenda, the Commission stressed that, when considering policy solutions, it would consider both regulatory and non-regulatory means, modelled on the Community of practice and the Principles for Better Self- and Co-regulation. A number of codes of conduct set up in the fields coordinated by Directive 2010/13/EU have proved to be well designed, in line with the Principles for Better Self- and Co-regulation. The existence of a legislative backstop was considered an important success factor in promoting compliance with a self- or co-regulatory code. It is equally important that such codes establish specific targets and objectives allowing for the regular, transparent and independent monitoring and evaluation of the objectives aimed at by the codes of conduct. The codes of conduct should also provide for effective enforcement. These principles should be followed by the self- and co-regulatory codes adopted in the fields coordinated by Directive 2010/13/EU.

Recital 18

Considering the evolution of the means by which content is disseminated via electronic communications networks, it is important to protect the general public from incitement to terrorism. Directive 2010/13/EU should therefore ensure that audiovisual media services do not contain public provocation to commit a terrorist offence. In order to ensure coherence and legal certainty for businesses and Member States' authorities, the notion of ‘public provocation to commit a terrorist offence’ should be understood within the meaning of Directive (EU) 2017/541 of the European Parliament and of the Council.

Recital 19

In order to empower viewers, including parents and minors, to make informed decisions about the content to be watched, it is necessary that media service providers provide sufficient information about content that may impair minors' physical, mental or moral development. That could be done, for example, through a system of content descriptors, an acoustic warning, a visual symbol or any other means, describing the nature of the content.

Recital 20

The appropriate measures for the protection of minors applicable to television broadcasting services should also apply to on-demand audiovisual media services. That should increase the level of protection. The minimum harmonisation approach allows Member States to develop a higher degree of protection for content which may impair the physical, mental or moral development of minors. The most harmful content, which may impair the physical, mental or moral development of minors, but is not necessarily a criminal offence, should be subject to the strictest measures such as encryption and effective parental controls, without prejudice to the adoption of stricter measures by Member States.

Recital 38

A Member State, when assessing, on a case-by-case basis, whether an on-demand audiovisual media service established in another Member State is targeting audiences in its territory, should refer to indicators such as advertisement or other promotions specifically aiming at customers in its territory, the main language of the service or the existence of content or commercial communications aiming specifically at the audience in the Member State of reception.

Recital 44

The video-sharing platform providers covered by Directive 2010/13/EU provide information society services within the meaning of Directive 2000/31/EC of the European Parliament and of the Council (11). Those providers are consequently subject to the provisions on the internal market set out in that Directive, if they are established in a Member State. It is appropriate to ensure that the same rules also

apply to video-sharing platform providers which are not established in a Member State with a view to safeguarding the effectiveness of the measures to protect minors and the general public set out in Directive 2010/13/EU and ensuring as much as possible a level playing field, in so far as those providers have either a parent undertaking or a subsidiary undertaking which is established in a Member State or where those providers are part of a group and another undertaking of that group is established in a Member State. Therefore, the definitions set out in Directive 2010/13/EU should be principles-based and should ensure that it is not possible for an undertaking to exclude itself from the scope of that Directive by creating a group structure containing multiple layers of undertakings established inside or outside the Union. The Commission should be informed of the providers under each Member State's jurisdiction pursuant to the rules on establishment set out in Directives 2000/31/EC and 2010/13/EU.

Recital 45

There are new challenges, in particular in connection with video-sharing platforms, on which users, particularly minors, increasingly consume audiovisual content. In this context, harmful content and hate speech provided on video-sharing platform services have increasingly given rise to concern. In order to protect minors and the general public from such content, it is necessary to set out proportionate rules on those matters.

Recital 47

A significant share of the content provided on video-sharing platform services is not under the editorial responsibility of the video-sharing platform provider. However, those providers typically determine the organisation of the content, namely programmes, user-generated videos and audiovisual commercial communications, including by automatic means or algorithms. Therefore, those providers should be required to take appropriate measures to protect minors from content that may impair their physical, mental or moral development. They should also be required to take appropriate measures to protect the general public from content that contains incitement to violence or hatred directed against a group or a member of a group on any of the grounds referred to in Article 21 of the Charter of Fundamental Rights of the European Union (the ‘Charter’), or the dissemination of which constitutes a criminal offence under Union law.

Recital 48

In light of the nature of the providers' involvement with the content provided on video-sharing platform services, the appropriate measures to protect minors and the general public should relate to the organisation of the content and not to the content as such. The requirements in this regard as set out in Directive 2010/13/EU should therefore apply without prejudice to Articles 12 to 14 of Directive 2000/31/EC, which provide for an exemption from liability for illegal information transmitted, or automatically, intermediately and temporarily stored, or stored by certain providers of information society services. When providing services covered by Articles 12 to 14 of Directive 2000/31/EC, those requirements should also apply without prejudice to Article 15 of that Directive, which precludes general obligations to monitor such information and to actively seek facts or circumstances indicating illegal activity from being imposed on those providers, without however concerning monitoring obligations in specific cases and, in particular, without affecting orders by national authorities in accordance with national law.

Article 1 para. 1 lit. aa

“video-sharing platform service” means a service as defined by Articles 56 and 57 of the Treaty on the Functioning of the European Union, where the principal purpose of the service or of a dissociable section thereof or an essential functionality of the service is devoted to providing programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility, in order to inform, entertain or educate, by means of electronic communications networks within the meaning of point (a) of Article 2 of Directive 2002/21/EC and the organisation of which is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing.’;

Article 2

1. Each Member State shall ensure that all audiovisual media services transmitted by media service providers under its jurisdiction comply with the rules of the system of law applicable to audiovisual media services intended for the public in that Member State.
2. For the purposes of this Directive, the media service providers under the jurisdiction of a Member State are any of the following:
(a) those established in that Member State in accordance with paragraph 3;
(b) those to whom paragraph 4 applies.

3. For the purposes of this Directive, a media service provider shall be deemed to be established in a Member State in the following cases:
(a) the media service provider has its head office in that Member State and the editorial decisions about the audiovisual media service are taken in that Member State;
(b) if a media service provider has its head office in one Member State but editorial decisions on the audiovisual media service are taken in another Member State, the media service provider shall be deemed to be established in the Member State where a significant part of the workforce involved in the pursuit of the programme-related audiovisual media service activity operates. If a significant part of the workforce involved in the pursuit of the programme-related audiovisual media service activity operates in each of those Member States, the media service provider shall be deemed to be established in the Member State where it has its head office. If a significant part of the workforce involved in the pursuit of the programme-related audiovisual media service activity operates in neither of those Member States, the media service provider shall be deemed to be established in the Member State where it first began its activity in accordance with the law of that Member State, provided that it maintains a stable and effective link with the economy of that Member State;
(c) if a media service provider has its head office in a Member State but decisions on the audiovisual media service are taken in a third country, or vice versa, it shall be deemed to be established in the Member State concerned, provided that a significant part of the workforce involved in the pursuit of the audiovisual media service activity operates in that Member State.
4. Media service providers to whom the provisions of paragraph 3 are not applicable shall be deemed to be under the jurisdiction of a Member State in the following cases:
(a) they use a satellite up-link situated in that Member State;
(b) although they do not use a satellite up-link situated in that Member State, they use satellite capacity appertaining to that Member State.
5. If the question as to which Member State has jurisdiction cannot be determined in accordance with paragraphs 3 and 4, the competent Member State shall be that in which the media service provider is established within the meaning of Articles 49 to 55 of the Treaty on the Functioning of the European Union.
5a. Member States shall ensure that media service providers inform the competent national regulatory authorities or bodies about any changes that may affect the determination of jurisdiction in accordance with paragraphs 2, 3 and 4.
5b. Member States shall establish and maintain an up-to-date list of the media service providers under their jurisdiction and indicate on which of the criteria set out in paragraphs 2 to 5 their jurisdiction is based. Member States shall communicate that list, including any updates thereto, to the Commission. The Commission shall ensure that such lists are made available in a centralised database. In the event of inconsistencies between the lists, the Commission shall contact the Member States concerned in order to find a solution. The Commission shall ensure that the national regulatory authorities or bodies have access to that database. The Commission shall make information in the database publicly available.
5c. Where, in applying Article 3 or 4, the Member States concerned do not agree on which Member State has jurisdiction, they shall bring the matter to the Commission's attention without undue delay. The Commission may request the European Regulators Group for Audiovisual Media Services (ERGA) to provide an opinion on the matter in accordance with point (d) of Article 30b(3). ERGA shall provide such an opinion within 15 working days from the submission of the Commission's request. The Commission shall keep the Contact Committee established by Article 29 duly informed. When the Commission adopts a decision pursuant to Article 3(2) or (3), or Article 4(5), it shall also decide which Member State has jurisdiction.
6. This Directive does not apply to audiovisual media services intended exclusively for reception in third countries and which are not received with standard consumer equipment directly or indirectly by the public in one or more Member States

Article 3 Directive 2010/13/EU	Article 3 Directive (EU) 2018/1808
1. Member States shall ensure freedom of reception and shall not restrict retransmissions on their territory of audiovisual media services from other Member States for reasons which fall within the fields coordinated by this Directive.	1. Member States shall ensure freedom of reception and shall not restrict retransmissions on their territory of audiovisual media services from other Member States for reasons which fall within the fields coordinated by this Directive.
2. In respect of television broadcasting, Member States may provisionally derogate from paragraph 1 if the following conditions are fulfilled: (a) a television broadcast coming from another Member State manifestly, seriously and gravely infringes Art. 27(1) or (2) and/or Art. 6;	2. **A Member State** may provisionally derogate from paragraph 1 **of this Art. where an audiovisual media service provided by a media service provider under the jurisdiction of another Member State** manifestly, seriously and gravely infringes **point (a) of Art. 6(1) or Art. 6a(1) or prejudices or presents a serious and grave risk of prejudice to public health.** The derogation referred to in the first subparagraph **shall be subject to** the following conditions:

(b) during the previous 12 months, the broadcaster has infringed the provision(s) referred to in point (a) on at least two prior occasions;	**(a)** during the previous 12 months**, the media service provider** has on at least two prior occasions **already performed one or more instances of conduct described in the first subparagraph**;
(c) the Member State concerned has notified the broadcaster and the Commission in writing of the alleged infringements and of the measures it intends to take should any such infringement occur again;	(b) the Member State concerned has notified **the media service provider, the Member State having jurisdiction over that provider** and the Commission in writing of the alleged infringements and of the **proportionate** measures it intends to take should any such infringement occur again; **(c) the Member State concerned has respected the right of defence of the media service provider and, in particular, has given that provider the opportunity to express its views on the alleged infringements; and**
(d) consultations with the transmitting Member State and the Commission have not produced an amicable settlement within 15 days of the notification provided for in point (c), and the alleged infringement persists. The Commission shall, within 2 months following notification of the measures taken by the Member State, take a decision on whether the measures are compatible with Union law. If it decides that they are not, the Member State will be required to put an end to the measures in question as a matter of urgency.	(d) consultations with the **[…]** Member **State having jurisdiction over the media service provider** and the Commission have not **resulted in** an amicable settlement within **one month** of the **Commission"s receipt of the** notification **referred to** in point (**b**) **[…].** Within **three** months **of the receipt of the** notification of the measures taken by the Member State **concerned and after having requested ERGA to provide an opinion in accordance with point (d) of Art. 30b(3),** the Commission shall take a decision on whether **those** measures are compatible with Union law. **The Commission shall keep the Contact Committee duly informed. Where the Commission** decides that **those measures** are not **compatible with Union law, it shall require** the Member State **concerned** to put an end to the measures in question as a matter of urgency.
3. Paragraph 2 shall be without prejudice to the application of any procedure, remedy or sanction to the infringements in question in the Member State which has jurisdiction over the broadcaster concerned. 4. In respect of on-demand audiovisual media services, Member States may take measures to derogate from paragraph 1 in respect of a given service if the following conditions are fulfilled: (a) the measures are: (i) necessary for one of the following reasons: — public policy, in particular the prevention, investigation, detection and prosecution of criminal offences, including the protection of minors and the fight against any incitement to hatred on grounds of race, sex, religion or nationality, and violations of human dignity concerning individual persons, — the protection of public health, — public security, including the safeguarding of national security and defence, — the protection of consumers, including investors; (ii) taken against an on-demand audiovisual media service which prejudices the objectives referred to in point (i) or which presents a serious and grave risk of prejudice to those objectives; (iii) proportionate to those objectives;	**4.** Paragraphs 2 **and 3** shall be without prejudice to the application of any procedure, remedy or sanction to the infringements in question in the Member State which has jurisdiction over the **media service provider** concerned. **3. A Member State** may provisionally derogate from paragraph **1 of this Art. where an audiovisual media service provided by a media service provider under the jurisdiction of another Member State manifestly, seriously and gravely infringes point (b) of Art. 6(1) or prejudices […]** or presents a serious and grave risk of prejudice to public security, including the safeguarding of national security and defence. **The derogation referred to in the first subparagraph shall be subject to the** following conditions: **(a) during the previous 12 months the conduct referred to in the first subparagraph occurred at least on one prior occasion; and**
(b) before taking the measures in question and without prejudice to court proceedings, including preliminary proceedings and acts carried out in the framework of a criminal investigation, the	(b) the Member State **concerned** has notified **the media service provider**, the Member State **having** jurisdiction **over that […]** provider and the Commission **in writing of the alleged**

Member State has: (i) asked the Member State under whose jurisdiction the media service provider falls to take measures and the latter did not take such measures, or they were inadequate; (ii) notified the Commission and the Member State under whose jurisdiction the media service provider falls of its intention to take such measures.	**infringement and of the proportionate** measures **it intends** to take **should any such infringement occur again.** **The Member State concerned shall respect the rights of defence of the media service provider concerned and, in particular, give that provider the opportunity to express its views on the alleged infringements.** **Within three months of the receipt of the notification of the measures taken by the Member State concerned and after having requested ERGA to provide an opinion in accordance with point (d) of Art. 30b(3), the Commission shall take a decision on whether those measures are compatible with Union law. The Commission shall keep the Contact Committee duly informed. Where the Commission decides that those measures are not compatible with Union law, it shall require the Member State concerned to put an end to the measures in question as a matter of urgency.**
5. Member States may, in urgent cases, derogate from the conditions laid down in point (b) of paragraph 4.	5. Member States may, in urgent cases**, no later than one month after the alleged infringement,** derogate from the conditions laid down in **points (a) and (b) of paragraph 3.**
Where this is the case, the measures shall be notified in the shortest possible time to the Commission and to the Member State under whose jurisdiction the media service provider falls, indicating the reasons for which the Member State considers that there is urgency. 6. Without prejudice to the Member State's possibility of proceeding with the measures referred to in paragraphs 4 and 5, the Commission shall examine the compatibility of the notified measures with Union law in the shortest possible time. Where it comes to the conclusion that the measures are incompatible with Union law, the Commission shall ask the Member State in question to refrain from taking any proposed measures or urgently to put an end to the measures in question.	Where this is the case, the measures **taken** shall be notified in the shortest possible time to the Commission and to the Member State under whose jurisdiction the media service provider falls, indicating the reasons for which the Member State considers that there is urgency. **[…]** The Commission shall examine the compatibility of the notified measures with Union law in the shortest possible time. Where it comes to the conclusion that the measures are incompatible with Union law, the Commission shall **[…] require** the Member State in question to urgently put an end to **those** measures.
	6. If the Commission lacks information necessary to take a decision pursuant to paragraph 2 or 3, it shall, within one month of the receipt of the notification, request from the Member State concerned all information necessary to reach that decision. The time limit within which the Commission is to take the decision shall be suspended until that Member State has provided such necessary information. In any case, the suspension of the time limit shall not last longer than one month. **7. Member States and the Commission shall regularly exchange experiences and best practices regarding the procedure set out in this Art. in the framework of the Contact Committee and ERGA.**
Article 4 Directive 2010/13/EU	Article 4 Directive (EU) 2018/1808
1. Member States shall remain free to require media service providers under their jurisdiction to comply with more detailed or stricter rules in the fields coordinated by this Directive provided that such rules are in compliance with Union law.	1. Member States shall remain free to require media service providers under their jurisdiction to comply with more detailed or stricter rules in the fields coordinated by this Directive, provided that such rules are in compliance with Union law.

2. In cases where a Member State: (a) has exercised its freedom under paragraph 1 to adopt more detailed or stricter rules of general public interest; and (b) assesses that a broadcaster under the jurisdiction of another Member State provides a television broadcast which is wholly or mostly directed towards its territory;	2. **[…]** Where a Member State: (a) has exercised its freedom under paragraph 1 to adopt more detailed or stricter rules of general public interest, and (b) assesses that a **media service provider** under the jurisdiction of another Member State provides **an audiovisual media service** which is wholly or mostly directed towards its territory,
it may contact the Member State having jurisdiction with a view to achieving a mutually satisfactory solution to any problems posed. On receipt of a substantiated request by the first Member State, the Member State having jurisdiction shall request the broadcaster to comply with the rules of general public interest in question. The Member State having jurisdiction shall inform the first Member State of the results obtained following this request within 2 months. Either Member State may invite the contact committee established pursuant to Article 29 to examine the case.	it may request the Member State having **jurisdiction to address any problems identified in relation to this paragraph. Both Member States shall cooperate sincerely and swiftly with a view to achieving a mutually satisfactory solution.** **Upon receiving** a substantiated request **under the first subparagraph**, the Member State having jurisdiction shall request the **media service provider** to comply with the rules of general public interest in question. **The Member State having jurisdiction shall regularly inform the requesting Member State of the steps taken to address the problems identified.** Within two months **of the receipt of the request**, the Member State having jurisdiction shall inform the **requesting** Member State **and the Commission** of the results obtained **and explain the reasons where a solution could not be found**. Either Member State may invite the Contact Committee **[…]** to examine the case at any time.
3. The first Member State may adopt appropriate measures against the broadcaster concerned where it assesses that: (a) the results achieved through the application of paragraph 2 are not satisfactory; and (b) the broadcaster in question has established itself in the Member State having jurisdiction in order to circumvent the stricter rules, in the fields coordinated by this Directive, which would be applicable to it if it were established in the first Member State	3. The Member State **concerned** may adopt appropriate measures against the **media service provider** concerned where: (a) it assesses that the results achieved through the application of paragraph 2 are not satisfactory; and (b) **it has adduced evidence showing that** the **media service provider** in question has established itself in the Member State having jurisdiction in order to circumvent the stricter rules, in the fields coordinated by this Directive, which would be applicable to it if it were established in the Member State **concerned**; **such evidence shall allow for such circumvention to be reasonably established, without the need to prove the media service provider's intention to circumvent those stricter rules**.
Such measures shall be objectively necessary, applied in a non-discriminatory manner and proportionate to the objectives which they pursue.	Such measures shall be objectively necessary, applied in a non-discriminatory manner and proportionate to the objectives which they pursue.
4. A Member State may take measures pursuant to paragraph 3 only if the following conditions are met: (a) it has notified the Commission and the Member State in which the broadcaster is established of its intention to take such measures while substantiating the grounds on which it bases its assessment; and	4. A Member State may take measures pursuant to paragraph 3 only where the following conditions are met: (a) it has notified the Commission and the Member State in which the media service provider is established of its intention to take such measures while substantiating the grounds on which it bases its assessment; **(b) it has respected the rights of defence of the media service provider concerned and, in particular, has given that media service provider the opportunity to express its views on the alleged circumvention and the measures the notifying Member State intends to take; and**
(b) the Commission has decided that the measures are compatible with Union law, and in particular that assessments made by the	**(c)** the Commission has decided**, after having requested ERGA to provide an opinion in accordance with point (d) of Article 30b(3),** that the measures are compatible with Union law, **[…]** in particular that assessments made by the Member State taking **the**

Member State taking those measures under paragraphs 2 and 3 are correctly founded.	measures under paragraphs 2 and 3 **of this Article** are correctly founded**; the Commission shall keep the Contact Committee duly informed**.
5. The Commission shall decide within 3 months following the notification provided for in point (a) of paragraph 4. If the Commission decides that the measures are incompatible with Union law, the Member State in question shall refrain from taking the proposed measures.	5. **W**ithin three months **of the receipt of** the notification provided for in point (a) of paragraph 4, the Commission shall **take the decision on whether those measures are compatible with Union law. Where** the Commission decides that **those** measures are **not compatible** with Union law, **it shall require** the Member State **concerned to** refrain from taking the **intended** measures. **If the Commission lacks information necessary to take the decision pursuant to the first subparagraph, it shall, within one month of the receipt of the notification, request from the Member State concerned all information necessary to reach that decision. The time limit within which the Commission is to take the decision shall be suspended until that Member State has provided such necessary information. In any case, the suspension of the time limit shall not last longer than one month.**
6. Member States shall, by appropriate means, ensure, within the framework of their legislation, that media service providers under their jurisdiction effectively comply with the provisions of this Directive.	6. Member States shall, by appropriate means, ensure, within the framework of their **national law**, that media service providers under their jurisdiction effectively comply with **[…]** this Directive.
7. Member States shall encourage co-regulation and/or self-regulatory regimes at national level in the fields coordinated by this Directive to the extent permitted by their legal systems. These regimes shall be such that they are broadly accepted by the main stakeholders in the Member States concerned and provide for effective enforcement.	**[…]**
8. Directive 2000/31/EC shall apply unless otherwise provided for in this Directive. In the event of a conflict between a provision of Directive 2000/31/EC and a provision of this Directive, the provisions of this Directive shall prevail, unless otherwise provided for in this Directive.	**7**. Directive 2000/31/EC shall apply unless otherwise provided for in this Directive. In the event of a conflict between **[…]** Directive 2000/31/EC and **[…]** this Directive, **[…]** this Directive shall prevail, unless otherwise provided for in this Directive.

Article 4a

1. Member States shall encourage the use of co-regulation and the fostering of self-regulation through codes of conduct adopted at national level in the fields coordinated by this Directive to the extent permitted by their legal systems. Those codes shall:
(a) be such that they are broadly accepted by the main stakeholders in the Member States concerned;
(b) clearly and unambiguously set out their objectives;
(c) provide for regular, transparent and independent monitoring and evaluation of the achievement of the objectives aimed at; and
(d) provide for effective enforcement including effective and proportionate sanctions.
2. Member States and the Commission may foster self-regulation through Union codes of conduct drawn up by media service providers, video-sharing platform service providers or organisations representing them, in cooperation, as necessary, with other sectors such as industry, trade, professional and consumer associations or organisations. Those codes shall be such that they are broadly accepted by the main stakeholders at Union level and shall comply with points (b) to (d) of paragraph 1. The Union codes of conduct shall be without prejudice to the national codes of conduct.
In cooperation with the Member States, the Commission shall facilitate the development of Union codes of conduct, where appropriate, in accordance with the principles of subsidiarity and proportionality.
The signatories of Union codes of conduct shall submit the drafts of those codes and amendments thereto to the Commission. The Commission shall consult the Contact Committee on those draft codes or amendments thereto.
The Commission shall make the Union codes of conduct publicly available and may give them appropriate publicity.

3. Member States shall remain free to require media service providers under their jurisdiction to comply with more detailed or stricter rules in compliance with this Directive and Union law, including where their national independent regulatory authorities or bodies conclude that any code of conduct or parts thereof have proven not to be sufficiently effective. Member States shall report such rules to the Commission without undue delay.

Article 6 Directive 2010/13/EU	Article 6 Directive (EU) 2018/1808
Member States shall ensure by appropriate means that audiovisual media services provided by media service providers under their jurisdiction do not contain any incitement to hatred based on race, sex, religion or nationality.	**1. Without prejudice to the obligation of Member States to respect and protect human dignity,** Member States shall ensure by appropriate means that audiovisual media services provided by media service providers under their jurisdiction do not contain any: **(a)** incitement to **violence or** hatred **directed against a group of persons or a member of a group based on any of the grounds referred to in Art. 21 of the Charter;** **(b) public provocation to commit a terrorist offence as set out in Art. 5 of Directive (EU) 2017/541.** **2. The measures taken for the purposes of this Art. shall be necessary and proportionate and shall respect the rights and observe principles set out in the Charter.**

Article 6a
1. Member States shall take appropriate measures to ensure that audiovisual media services provided by media service providers under their jurisdiction which may impair the physical, mental or moral development of minors are only made available in such a way as to ensure that minors will not normally hear or see them. Such measures may include selecting the time of the broadcast, age verification tools or other technical measures. They shall be proportionate to the potential harm of the programme. The most harmful content, such as gratuitous violence and pornography, shall be subject to the strictest measures. 2. Personal data of minors collected or otherwise generated by media service providers pursuant to paragraph 1 shall not be processed for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising. 3. Member States shall ensure that media service providers provide sufficient information to viewers about content which may impair the physical, mental or moral development of minors. For this purpose, media service providers shall use a system describing the potentially harmful nature of the content of an audiovisual media service. For the implementation of this paragraph, Member States shall encourage the use of co-regulation as provided for in Article 4a(1). 4. The Commission shall encourage media service providers to exchange best practices on co-regulatory codes of conduct. Member States and the Commission may foster self-regulation, for the purposes of this Article, through Union codes of conduct as referred to in Article 4a(2).

Article 9 Directive 2010/13/EU	Article 9 Directive (EU) 2018/1808
1. Member States shall ensure that audiovisual commercial communications provided by media service providers under their jurisdiction comply with the following requirements: (a) audiovisual commercial communications shall be readily recognisable as such; surreptitious audiovisual commercial communication shall be prohibited; (b) audiovisual commercial communications shall not use subliminal techniques; (c) audiovisual commercial communications shall not: (i) prejudice respect for human dignity; (ii) include or promote any discrimination based on sex, racial or ethnic origin, nationality, religion or belief, disability, age or sexual orientation; (iii) encourage behaviour prejudicial to health or safety; (iv) encourage behaviour grossly prejudicial to the protection of the environment;	1. Member States shall ensure that audiovisual commercial communications provided by media service providers under their jurisdiction comply with the following requirements: (a) audiovisual commercial communications shall be readily recognisable as such; surreptitious audiovisual commercial communication shall be prohibited; (b) audiovisual commercial communications shall not use subliminal techniques; (c) audiovisual commercial communications shall not: (i) prejudice respect for human dignity; (ii) include or promote any discrimination based on sex, racial or ethnic origin, nationality, religion or belief, disability, age or sexual orientation; (iii) encourage behaviour prejudicial to health or safety; (iv) encourage behaviour grossly prejudicial to the protection of the environment;

(d) all forms of audiovisual commercial communications for cigarettes and other tobacco products shall be prohibited;	(d) all forms of audiovisual commercial communications for cigarettes and other tobacco products, **as well as for electronic cigarettes and refill containers** shall be prohibited;
(e) audiovisual commercial communications for alcoholic beverages shall not be aimed specifically at minors and shall not encourage immoderate consumption of such beverages; (f) audiovisual commercial communications for medicinal products and medical treatment available only on prescription in the Member State within whose jurisdiction the media service provider falls shall be prohibited; (g) audiovisual commercial communications shall not cause physical, mental or moral detriment to minors; therefore, they shall not directly exhort minors to buy or hire a product or service by exploiting their inexperience or credulity, directly encourage them to persuade their parents or others to purchase the goods or services being advertised, exploit the special trust minors place in parents, teachers or other persons, or unreasonably show minors in dangerous situations.	(e) audiovisual commercial communications for alcoholic beverages shall not be aimed specifically at minors and shall not encourage immoderate consumption of such beverages; (f) audiovisual commercial communications for medicinal products and medical treatment available only on prescription in the Member State within whose jurisdiction the media service provider falls shall be prohibited; (g) audiovisual commercial communications shall not cause physical, mental or moral detriment to minors; therefore, they shall not directly exhort minors to buy or hire a product or service by exploiting their inexperience or credulity, directly encourage them to persuade their parents or others to purchase the goods or services being advertised, exploit the special trust minors place in parents, teachers or other persons, or unreasonably show minors in dangerous situations.
	2. Audiovisual commercial communications for alcoholic beverages in on-demand audiovisual media services, with the exception of sponsorship and product placement, shall comply with the criteria set out in Art. 22. **3. Member States shall encourage the use of co-regulation and the fostering of self-regulation through codes of conduct as provided for in Art. 4a(1) regarding inappropriate audiovisual commercial communications for alcoholic beverages. Those codes shall aim to effectively reduce the exposure of minors to audiovisual commercial communications for alcoholic beverages**

Article 28a

1. For the purposes of this Directive, a video-sharing platform provider established on the territory of a Member State within the meaning of Article 3(1) of Directive 2000/31/EC shall be under the jurisdiction of that Member State.
2. A video-sharing platform provider which is not established on the territory of a Member State pursuant to paragraph 1 shall be deemed to be established on the territory of a Member State for the purposes of this Directive if that video-sharing platform provider:
(a) has a parent undertaking or a subsidiary undertaking that is established on the territory of that Member State; or
(b) is part of a group and another undertaking of that group is established on the territory of that Member State.
For the purposes of this Article:
(a) “parent undertaking” means an undertaking which controls one or more subsidiary undertakings;
(b) “subsidiary undertaking” means an undertaking controlled by a parent undertaking, including any subsidiary undertaking of an ultimate parent undertaking;
(c) “group” means a parent undertaking, all its subsidiary undertakings and all other undertakings having economic and legal organisational links to them.
3. For the purposes of applying paragraph 2, where the parent undertaking, the subsidiary undertaking or the other undertakings of the group are each established in different Member States, the video-sharing platform provider shall be deemed to be established in the Member State where its parent undertaking is established or, in the absence of such an establishment, in the Member State where its subsidiary undertaking is established or, in the absence of such an establishment, in the Member State where the other undertaking of the group is established.
4. For the purposes of applying paragraph 3, where there are several subsidiary undertakings and each of them is established in a different Member State, the video-sharing platform provider shall be deemed to be established in the Member State where one of the subsidiary undertakings first began its activity, provided that it maintains a stable and effective link with the economy of that Member State.
Where there are several other undertakings which are part of the group and each of them is established in a different Member State, the video-sharing platform provider shall be deemed to be established in the Member State where one of these undertakings first began its

activity, provided that it maintains a stable and effective link with the economy of that Member State.
5. For the purposes of this Directive, Article 3 and Articles 12 to 15 of Directive 2000/31/EC shall apply to video-sharing platform providers deemed to be established in a Member State in accordance with paragraph 2 of this Article.
6. Member States shall establish and maintain an up-to-date list of the video-sharing platform providers established or deemed to be established on their territory and indicate on which of the criteria set out in paragraphs 1 to 4 their jurisdiction is based. Member States shall communicate that list, including any updates thereto, to the Commission.
The Commission shall ensure that such lists are made available in a centralised database. In the event of inconsistencies between the lists, the Commission shall contact the Member States concerned in order to find a solution. The Commission shall ensure that the national regulatory authorities or bodies have access to that database. The Commission shall make information in the database publicly available.
7. Where, in applying this Article, the Member States concerned do not agree on which Member State has jurisdiction, they shall bring the matter to the Commission's attention without undue delay. The Commission may request ERGA to provide an opinion on the matter in accordance with point (d) of Article 30b(3). ERGA shall provide such an opinion within 15 working days from the submission of the Commission's request. The Commission shall keep the Contact Committee duly informed.

Article 28b para. 1 and 2

1. Without prejudice to Articles 12 to 15 of Directive 2000/31/EC, Member States shall ensure that video-sharing platform providers under their jurisdiction take appropriate measures to protect:
(a) minors from programmes, user-generated videos and audiovisual commercial communications which may impair their physical, mental or moral development in accordance with Article 6a(1);
(b) the general public from programmes, user-generated videos and audiovisual commercial communications containing incitement to violence or hatred directed against a group of persons or a member of a group based on any of the grounds referred to in Article 21 of the Charter;
(c) the general public from programmes, user-generated videos and audiovisual commercial communications containing content the dissemination of which constitutes an activity which is a criminal offence under Union law, namely public provocation to commit a terrorist offence as set out in Article 5 of Directive (EU) 2017/541, offences concerning child pornography as set out in Article 5(4) of Directive 2011/93/EU of the European Parliament and of the Council (*1) and offences concerning racism and xenophobia as set out in Article 1 of Framework Decision 2008/913/JHA.
2. Member States shall ensure that video-sharing platform providers under their jurisdiction comply with the requirements set out in Article 9(1) with respect to audiovisual commercial communications that are marketed, sold or arranged by those video-sharing platform providers.
Member States shall ensure that the video-sharing platform providers under their jurisdiction take appropriate measures to comply with the requirements set out in Article 9(1) with respect to audiovisual commercial communications that are not marketed, sold or arranged by those video-sharing platform providers, taking into account the limited control exercised by those video-sharing platforms over those audiovisual commercial communications.
Member States shall ensure that video-sharing platform providers clearly inform users where programmes and user-generated videos contain audiovisual commercial communications, provided that such communications are declared under point (c) of the third subparagraph of paragraph 3 or the provider has knowledge of that fact.
Member States shall encourage the use of co-regulation and the fostering of self-regulation through codes of conduct as provided for in Article 4a(1) aiming at effectively reducing the exposure of children to audiovisual commercial communications for foods and beverages containing nutrients and substances with a nutritional or physiological effect, in particular fat, trans-fatty acids, salt or sodium and sugars, of which excessive intakes in the overall diet are not recommended. Those codes shall aim to provide that such audiovisual commercial communications do not emphasise the positive quality of the nutritional aspects of such foods and beverages.

Article 30a

1. Member States shall ensure that national regulatory authorities or bodies take appropriate measures to provide each other and the Commission with the information necessary for the application of this Directive, in particular Articles 2, 3 and 4.
2. In the context of the information exchange under paragraph 1, when national regulatory authorities or bodies receive information from a media service provider under their jurisdiction that it will provide a service wholly or mostly directed at the audience of another Member State, the national regulatory authority or body in the Member State having jurisdiction shall inform the national regulatory authority or body of the targeted Member State.
3. If the regulatory authority or body of a Member State whose territory is targeted by a media service provider under the jurisdiction of another Member State sends a request concerning the activities of that provider to the regulatory authority or body of the Member State having jurisdiction over it, the latter regulatory authority or body shall do its utmost to address the request within two months, without prejudice to stricter time limits applicable pursuant to this Directive. When requested, the regulatory authority or body of the targeted

Member State shall provide any information to the regulatory authority or body of the Member State having jurisdiction that may assist it in addressing the request.
Article 30b
1. The European Regulators Group for Audiovisual Media Services (ERGA) is hereby established. 2. It shall be composed of representatives of national regulatory authorities or bodies in the field of audiovisual media services with primary responsibility for overseeing audiovisual media services, or where there is no national regulatory authority or body, by other representatives as chosen through their procedures. A Commission representative shall participate in ERGA meetings. 3. ERGA shall have the following tasks: (a) to provide technical expertise to the Commission: - in its task to ensure a consistent implementation of this Directive in all Member States, - on matters related to audiovisual media services within its competence; (b) to exchange experience and best practices on the application of the regulatory framework for audiovisual media services, including on accessibility and media literacy; (c) to cooperate and provide its members with the information necessary for the application of this Directive, in particular as regards Articles 3, 4 and 7; (d) to give opinions, when requested by the Commission, on the technical and factual aspects of the issues pursuant to Article 2(5c), Article 3(2) and (3), point (c) of Article 4(4) and Article 28a(7). 4. ERGA shall adopt its rules of procedure.’;

C. General Data Protection Regulation

Regulation (EU) 2016/679, *OJ L 119, 4.5.2016, p. 1–88*

https://eur-lex.europa.eu/eli/reg/2016/679/oj

Recital 5

The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.

Recital 21

This Regulation is without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States.

Recital 22

Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

Recital 23

In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

Recital 24

The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

Recital 125

The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the supervisory

authorities concerned in the decision-making process. Where the decision is to reject the complaint by the data subject in whole or in part, that decision should be adopted by the supervisory authority with which the complaint has been lodged.

Recital 126

The decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned and should be directed towards the main or single establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.

Recital 127

Each supervisory authority not acting as the lead supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involves only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay about the matter. After being informed, the lead supervisory authority should decide, whether it will handle the case pursuant to the provision on cooperation between the lead supervisory authority and other supervisory authorities concerned (‘one-stop-shop mechanism’), or whether the supervisory authority which informed it should handle the case at local level. When deciding whether it will handle the case, the lead supervisory authority should take into account whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it in order to ensure effective enforcement of a decision vis-à-vis the controller or processor. Where the lead supervisory authority decides to handle the case, the supervisory authority which informed it should have the possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in that one-stop-shop mechanism.

Recital 136

In applying the consistency mechanism, the Board should, within a determined period of time, issue an opinion, if a majority of its members so decides or if so requested by any supervisory authority concerned or the Commission. The Board should also be empowered to adopt legally binding decisions where there are disputes between supervisory authorities. For that purpose, it should issue, in principle by a two-thirds majority of its members, legally binding decisions in clearly specified cases where there are conflicting views among supervisory authorities, in particular in the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned on the merits of the case, in particular whether there is an infringement of this Regulation.

Recital 137

There may be an urgent need to act in order to protect the rights and freedoms of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. A supervisory authority should therefore be able to adopt duly justified provisional measures on its territory with a specified period of validity which should not exceed three months.

Recital 138

The application of such mechanism should be a condition for the lawfulness of a measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned should be applied and mutual assistance and joint operations might be carried out between the supervisory authorities concerned on a bilateral or multilateral basis without triggering the consistency mechanism.

Article 3
Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Art. 51
Supervisory authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union (‘supervisory authority’).
2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.
3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.
4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 52
Independence

1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.
2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.
3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.
4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.
5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.
6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

Article 53
General conditions for the members of the supervisory authority

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:
- their parliament;
- their government;
- their head of State; or
- an independent body entrusted with the appointment under Member State law.
2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.
4. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

Article 55
Competence

1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.
2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.
3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Article 56
Competence of the lead supervisory authority

1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.
2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.
3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.
4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).
5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.
6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

Article 60
Cooperation between the lead supervisory authority and the other supervisory authorities concerned

1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.
2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.
3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.
4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.
5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.
6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be

deemed to be in agreement with that draft decision and shall be bound by it.
7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.
8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.
9. Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.
10. After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.
11. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.
12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.

Article 61
Mutual assistance

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.
2. Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.
3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.
4. The requested supervisory authority shall not refuse to comply with the request unless:
(a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or
(b) compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.
5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.
6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.
7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.
8. Where a supervisory authority does not provide the information referred to in paragraph 5 of this Article within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).
9. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Article 62
Joint operations of supervisory authorities

1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.
2. Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. The supervisory authority which is competent pursuant to Article 56(1) or (4) shall invite the supervisory authority of each of those Member States to take part in the joint operations and shall respond without delay to the request of a supervisory authority to participate.
3. A supervisory authority may, in accordance with Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the Member State law of the host supervisory authority.
4. Where, in accordance with paragraph 1, staff of a seconding supervisory authority operate in another Member State, the Member State of the host supervisory authority shall assume responsibility for their actions, including liability, for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.
5. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse that other Member State in full any sums it has paid to the persons entitled on their behalf.
6. Without prejudice to the exercise of its rights vis-à-vis third parties and with the exception of paragraph 5, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement from another Member State in relation to damage referred to in paragraph 4.
7. Where a joint operation is intended and a supervisory authority does not, within one month, comply with the obligation laid down in the second sentence of paragraph 2 of this Article, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 55. In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an opinion or an urgent binding decision from the Board pursuant to Article 66(2).

Article 63
Consistency mechanism

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

Article 65
Dispute resolution by the Board

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:
(a) where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;
(b) where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;
(c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.
2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-thirds majority of the members of the Board. That period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.
3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where

the members of the Board are split, the decision shall by adopted by the vote of its Chair.
4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.
5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.
6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.

Article 66
Urgency procedure

1. In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.
2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.
3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.
4. By derogation from Article 64(3) and Article 65(2), an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the Board.

Article 67
Exchange of information

The Commission may adopt implementing acts of general scope in order to specify the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in Article 64.
Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Article 68
European Data Protection Board

1. The European Data Protection Board (the ‘Board’) is hereby established as a body of the Union and shall have legal personality.
2. The Board shall be represented by its Chair.
3. The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.
4. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with that Member State's law.
5. The Commission shall have the right to participate in the activities and meetings of the Board without voting right. The Commission shall designate a representative. The Chair of the Board shall communicate to the Commission the activities of the Board.
6. In the cases referred to in Article 65, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation.

Article 69
Independence

1. The Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 70 and 71.
2. Without prejudice to requests by the Commission referred to in point (b) of Article 70(1) and in Article 70(2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.

Article 85
Processing and freedom of expression and information

1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.
2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.
3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

Article 95
Relationship with Directive 2002/58/EC

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

D. DSM Directive

Directive 2019/790, *OJ L 130, 17.5.2019, p. 92–125*

https://eur-lex.europa.eu/eli/dir/2019/790/oj

Recital 61

In recent years, the functioning of the online content market has gained in complexity. Online content-sharing services providing access to a large amount of copyright-protected content uploaded by their users have become a main source of access to content online. Online services are a means of providing wider access to cultural and creative works and offer great opportunities for cultural and creative industries to develop new business models. However, although they enable diversity and ease of access to content, they also generate challenges when copyright-protected content is uploaded without prior authorisation from rightholders. Legal uncertainty exists as to whether the providers of such services engage in copyright-relevant acts, and need to obtain authorisation from rightholders for content uploaded by their users who do not hold the relevant rights in the uploaded content, without prejudice to the application of exceptions and limitations provided for in Union law. That uncertainty affects the ability of rightholders to determine whether, and under which conditions, their works and other subject matter are used, as well as their ability to obtain appropriate remuneration for such use. It is therefore important to foster the development of the licensing market between rightholders and online content-sharing service providers. Those licensing agreements should be fair and keep a reasonable balance between both parties. Rightholders should receive appropriate remuneration for the use of their works or other subject matter. However, as contractual freedom should not be affected by those provisions, rightholders should not be obliged to give an authorisation or to conclude licensing agreements.

Recital 62

Certain information society services, as part of their normal use, are designed to give access to the public to copyright-protected content or other subject matter uploaded by their users. The definition of an online content-sharing service provider laid down in this Directive should target only online services that play an important role on the online content market by competing with other online content services, such as online audio and video streaming services, for the same audiences. The services covered by this Directive are services, the main or one of the main purposes of which is to store and enable users to upload and share a large amount of copyright-protected content with the purpose of obtaining profit therefrom, either directly or indirectly, by organising it and promoting it in order to attract a larger audience, including by categorising it and using targeted promotion within it. Such services should not include services that have a main purpose other than that of enabling users to upload and share a large amount of copyright-protected content with the purpose of obtaining profit from that activity. The latter services include, for instance, electronic communication services within the meaning of Directive (EU) 2018/1972 of the European Parliament and of the Council, as well as providers of business-to-business cloud services and cloud services, which allow users to upload content for their own use, such as cyberlockers, or online marketplaces the main activity of which is online retail, and not giving access to copyright-protected content.
Providers of services such as open source software development and sharing platforms, not-for-profit scientific or educational repositories as well as not-for-profit online encyclopedias should also be excluded from the definition of online content-sharing service provider. Finally, in order to ensure a high level of copyright protection, the liability exemption mechanism provided for in this Directive should not apply to service providers the main purpose of which is to engage in or to facilitate copyright piracy.

Recital 63

The assessment of whether an online content-sharing service provider stores and gives access to a large amount of copyright-protected content should be made on a case-by-case basis and should take account of a combination of elements, such as the audience of the service and the number of files of copyright-protected content uploaded by the users of the service.

Recital 64

It is appropriate to clarify in this Directive that online content-sharing service providers perform an act of communication to the public or of making available to the public when they give the public access to copyright-protected works or other protected subject matter uploaded by their users. Consequently, online content-sharing service providers should obtain an authorisation, including via a licensing agreement, from the relevant rightholders. This does not affect the concept of communication to the public or of making available to the public

elsewhere under Union law, nor does it affect the possible application of Article 3(1) and (2) of Directive 2001/29/EC to other service providers using copyright-protected content.

Recital 65

When online content-sharing service providers are liable for acts of communication to the public or making available to the public under the conditions laid down in this Directive, Article 14(1) of Directive 2000/31/EC should not apply to the liability arising from the provision of this Directive on the use of protected content by online content-sharing service providers. That should not affect the application of Article 14(1) of Directive 2000/31/EC to such service providers for purposes falling outside the scope of this Directive.

Recital 66

Taking into account the fact that online content-sharing service providers give access to content which is not uploaded by them but by their users, it is appropriate to provide for a specific liability mechanism for the purposes of this Directive for cases in which no authorisation has been granted. That should be without prejudice to remedies under national law for cases other than liability for copyright infringements and to national courts or administrative authorities being able to issue injunctions in compliance with Union law. In particular, the specific regime applicable to new online content-sharing service providers with an annual turnover below EUR 10 million, of which the average number of monthly unique visitors in the Union does not exceed 5 million, should not affect the availability of remedies under Union and national law. Where no authorisation has been granted to service providers, they should make their best efforts in accordance with high industry standards of professional diligence to avoid the availability on their services of unauthorised works and other subject matter, as identified by the relevant rightholders. For that purpose, rightholders should provide the service providers with relevant and necessary information taking into account, among other factors, the size of rightholders and the type of their works and other subject matter. The steps taken by online content-sharing service providers in cooperation with rightholders should not lead to the prevention of the availability of non-infringing content, including works or other protected subject matter the use of which is covered by a licensing agreement, or an exception or limitation to copyright and related rights. Steps taken by such service providers should, therefore, not affect users who are using the online content-sharing services in order to lawfully upload and access information on such services.

In addition, the obligations established in this Directive should not lead to Member States imposing a general monitoring obligation. When assessing whether an online content-sharing service provider has made its best efforts in accordance with the high industry standards of professional diligence, account should be taken of whether the service provider has taken all the steps that would be taken by a diligent operator to achieve the result of preventing the availability of unauthorised works or other subject matter on its website, taking into account best industry practices and the effectiveness of the steps taken in light of all relevant factors and developments, as well as the principle of proportionality. For the purposes of that assessment, a number of elements should be considered, such as the size of the service, the evolving state of the art as regards existing means, including potential future developments, to avoid the availability of different types of content and the cost of such means for the services. Different means to avoid the availability of unauthorised copyright-protected content could be appropriate and proportionate depending on the type of content, and, therefore, it cannot be excluded that in some cases availability of unauthorised content can only be avoided upon notification of rightholders. Any steps taken by service providers should be effective with regard to the objectives pursued but should not go beyond what is necessary to achieve the objective of avoiding and discontinuing the availability of unauthorised works and other subject matter.

If unauthorised works and other subject matter become available despite the best efforts made in cooperation with rightholders, as required by this Directive, the online content-sharing service providers should be liable in relation to the specific works and other subject matter for which they have received the relevant and necessary information from rightholders, unless those providers demonstrate that they have made their best efforts in accordance with high industry standards of professional diligence.

In addition, where specific unauthorised works or other subject matter have become available on online content-sharing services, including irrespective of whether the best efforts were made and regardless of whether rightholders have made available the relevant and necessary information in advance, the online content-sharing service providers should be liable for unauthorised acts of communication to the public of works or other subject matter, when, upon receiving a sufficiently substantiated notice, they fail to act expeditiously to disable access to, or to remove from their websites, the notified works or other subject matter. Additionally, such online content-sharing service providers should also be liable if they fail to demonstrate that they have made their best efforts to prevent the future uploading of specific unauthorised works, based on relevant and necessary information provided by rightholders for that purpose.

Where rightholders do not provide online content-sharing service providers with the relevant and necessary information on their specific works or other subject matter, or where no notification concerning the disabling of access to, or the removal of, specific unauthorised works or other subject matter has been provided by rightholders, and, as a result, those service providers cannot make their best efforts to avoid the availability of unauthorised content on their services, in accordance with high industry standards of professional diligence, such service providers should not be liable for unauthorised acts of communication to the public or of making available to the public of such unidentified works or other subject matter.

Article 2 para. 6
6. ‘online content-sharing service provider’ means a provider of an information society service of which the main or one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes. Providers of services, such as not-for-profit online encyclopedias, not-for-profit educational and scientific repositories, open source software-developing and-sharing platforms, providers of electronic communications services as defined in Directive (EU) 2018/1972, online marketplaces, business-to-business cloud services and cloud services that allow users to upload content for their own use, are not ‘online content-sharing service providers’ within the meaning of this Directive.
Article 17 para. 3 and 4
3. When an online content-sharing service provider performs an act of communication to the public or an act of making available to the public under the conditions laid down in this Directive, the limitation of liability established in Article 14(1) of Directive 2000/31/EC shall not apply to the situations covered by this Article. The first subparagraph of this paragraph shall not affect the possible application of Article 14(1) of Directive 2000/31/EC to those service providers for purposes falling outside the scope of this Directive. 4. If no authorisation is granted, online content-sharing service providers shall be liable for unauthorised acts of communication to the public, including making available to the public, of copyright-protected works and other subject matter, unless the service providers demonstrate that they have: (a) made best efforts to obtain an authorisation, and (b) made, in accordance with high industry standards of professional diligence, best efforts to ensure the unavailability of specific works and other subject matter for which the rightholders have provided the service providers with the relevant and necessary information; and in any event (c) acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from their websites, the notified works or other subject matter, and made best efforts to prevent their future uploads in accordance with point (b).

E. P2B-Regulation

Regulation (EU) 2019/1150, *OJ L 186, 11.7.2019, p. 57–79*

https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019R1150

Recital 1

Online intermediation services are key enablers of entrepreneurship and new business models, trade and innovation, which can also improve consumer welfare and which are increasingly used by both the private and public sectors. They offer access to new markets and commercial opportunities allowing undertakings to exploit the benefits of the internal market. They allow consumers in the Union to exploit those benefits, in particular by increasing their choice of goods and services, as well as by contributing to offering competitive pricing online, but they also raise challenges that need to be addressed in order to ensure legal certainty.

Recital 3

Consumers have embraced the use of online intermediation services. A competitive, fair, and transparent online ecosystem where companies behave responsibly is also essential for consumer welfare. Ensuring the transparency of, and trust in, the online platform economy in business-to-business relations could also indirectly help to improve consumer trust in the online platform economy. Direct impacts of the development of the online platform economy on consumers are, however, addressed by other Union law, especially the consumer acquis.

Recital 9

Since online intermediation services and online search engines typically have a global dimension, this Regulation should apply to providers of those services regardless of whether they are established in a Member State or outside the Union, provided that two cumulative conditions are met. Firstly, the business users or corporate website users should be established in the Union. Secondly, the business users or corporate website users should, through the provision of those services, offer their goods or services to consumers located in the Union at least for part of the transaction. In order to determine whether business users or corporate website users are offering goods or services to consumers located in the Union, it is necessary to ascertain whether it is apparent that the business users or corporate website users direct their activities to consumers located in one or more Member States. This criterion should be interpreted in accordance with the relevant case law of the Court of Justice of the European Union on point (c) of Article 17(1) of Regulation (EU) No 1215/2012 of the European Parliament and of the Council and point (b) of Article 6(1) of Regulation (EC) No 593/2008 of the European Parliament and of the Council. Such consumers should be located in the Union, but do not need to have their place of residence in the Union nor have the nationality of any Member State. Accordingly, this Regulation should not apply where business users or corporate websites users are not established in the Union or where they are established in the Union but where they use online intermediation services or online search engines to offer goods or services exclusively to consumers located outside the Union or to persons who are not consumers. Furthermore, this Regulation should apply irrespective of the law otherwise applicable to a contract.

Recital 10

A wide variety of business-to-consumer relations are intermediated online by providers operating multi-sided services that are essentially based on the same ecosystem-building business model. In order to capture the relevant services, online intermediation services should be defined in a precise and technologically-neutral manner. In particular, the services should consist of information society services, which are characterised by the fact that they aim to facilitate the initiating of direct transactions between business users and consumers, irrespective of whether the transactions are ultimately concluded online, on the online portal of the provider of online intermediation services in question or that of the business user, offline or in fact not at all, meaning that there should be no requirement for any contractual relationship between the business users and consumers as a precondition for online intermediation services falling within the scope of this Regulation. The mere inclusion of a service of a marginal character only should not be seen as making the aim of a website or service the facilitation of transactions within the meaning of online intermediation services. In addition, the services should be provided on the basis of contractual relationships between the providers and business users which offer goods or services to consumers. Such a contractual relationship should be deemed to

exist where both parties concerned express their intention to be bound in an unequivocal manner on a durable medium, without an express written agreement necessarily being required.

Article 2 para. 1 and 2

For the purposes of this Regulation, the following definitions apply:
(1) 'business user' means any private individual acting in a commercial or professional capacity who, or any legal person which, through online intermediation services offers goods or services to consumers for purposes relating to its trade, business, craft or profession;
(2) 'online intermediation services' means services which meet all of the following requirements:
(a) they constitute information society services within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council;
(b) they allow business users to offer goods or services to consumers, with a view to facilitating the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded;
(c) they are provided to business users on the basis of contractual relationships between the provider of those services and business users which offer goods or services to consumers;

Article 15
Enforcement

1. Each Member State shall ensure adequate and effective enforcement of this Regulation.
2. Member States shall lay down the rules setting out the measures applicable to infringements of this Regulation and shall ensure that they are implemented. The measures provided for shall be effective, proportionate and dissuasive.

Article 16
Monitoring

The Commission, in close cooperation with Member States, shall closely monitor the impact of this Regulation on relationships between online intermediation services and their business users and between online search engines and corporate website users. To this end, the Commission shall gather relevant information to monitor changes in these relationships, including by carrying out relevant studies. Member States shall assist the Commission by providing, upon request, any relevant information gathered including about specific cases. The Commission may, for the purpose of this Article and Article 18, seek to gather information from providers of online intermediation services.

F. TERREG Proposal

COM/2018/640 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0640
Recital 1
This Regulation aims at ensuring the smooth functioning of the digital single market in an open and democratic society, by preventing the misuse of hosting services for terrorist purposes. The functioning of the digital single market should be improved by reinforcing legal certainty for hosting service providers, reinforcing users' trust in the online environment, and by strengthening safeguards to the freedom of expression and information.
Recital 2
Hosting service providers active on the internet play an essential role in the digital economy by connecting business and citizens and by facilitating public debate and the distribution and receipt of information, opinions and ideas, contributing significantly to innovation, economic growth and job creation in the Union. However, their services are in certain cases abused by third parties to carry out illegal activities online. Of particular concern is the misuse of hosting service providers by terrorist groups and their supporters to disseminate terrorist content online in order to spread their message, to radicalise and recruit and to facilitate and direct terrorist activity.
Recital 5
The application of this Regulation should not affect the application of Article 14 of Directive 2000/31/EC. In particular, any measures taken by the hosting service provider in compliance with this Regulation, including any proactive measures, should not in themselves lead to that service provider losing the benefit of the liability exemption provided for in that provision. This Regulation leaves unaffected the powers of national authorities and courts to establish liability of hosting service providers in specific cases where the conditions under Article 14 of Directive 2000/31/EC for liability exemption are not met.
Recital 6
Rules to prevent the misuse of hosting services for the dissemination of terrorist content online in order to guarantee the smooth functioning of the internal market are set out in this Regulation in full respect of the fundamental rights protected in the Union's legal order and notably those guaranteed in the Charter of Fundamental Rights of the European Union.
Recital 7
This Regulation contributes to the protection of public security while establishing appropriate and robust safeguards to ensure protection of the fundamental rights at stake. This includes the rights to respect for private life and to the protection of personal data, the right to effective judicial protection, the right to freedom of expression, including the freedom to receive and impart information, the freedom to conduct a business, and the principle of non-discrimination. Competent authorities and hosting service providers should only adopt measures which are necessary, appropriate and proportionate within a democratic society, taking into account the particular importance accorded to the freedom of expression and information, which constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which the Union is founded. Measures constituting interference in the freedom of expression and information should be strictly targeted, in the sense that they must serve to prevent the dissemination of terrorist content, but without thereby affecting the right to lawfully receive and impart information, taking into account the central role of hosting service providers in facilitating public debate and the distribution and receipt of facts, opinions and ideas in accordance with the law.

Recital 10
In order to cover those online hosting services where terrorist content is disseminated, this Regulation should apply to information society services which store information provided by a recipient of the service at his or her request and in making the information stored available to third parties, irrespective of whether this activity is of a mere technical, automatic and passive nature. By way of example such providers of information society services include social media platforms, video streaming services, video, image and audio sharing services, file sharing and other cloud services to the extent they make the information available to third parties and websites where users can make comments or post reviews. The Regulation should also apply to hosting service providers established outside the Union but offering services within the Union, since a significant proportion of hosting service providers exposed to terrorist content on their services are established in third countries. This should ensure that all companies operating in the Digital Single Market comply with the same requirements, irrespective of their country of establishment. The determination as to whether a service provider offers services in the Union requires an assessment whether the service provider enables legal or natural persons in one or more Member States to use its services. However, the mere accessibility of a service provider's website or of an email address and of other contact details in one or more Member States taken in isolation should not be a sufficient condition for the application of this Regulation.
Recital 11
A substantial connection to the Union should be relevant to determine the scope of this Regulation. Such a substantial connection to the Union should be considered to exist where the service provider has an establishment in the Union or, in its absence, on the basis of the existence of a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States. The targeting of activities towards one or more Member States can be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in that Member State, or the possibility of ordering goods or services. The targeting of activities towards a Member State could also be derived from the availability of an application in the relevant national application store, from providing local advertising or advertising in the language used in that Member State, or from the handling of customer relations such as by providing customer service in the language generally used in that Member State. A substantial connection should also be assumed where a service provider directs its activities towards one or more Member State as set out in Article 17(1)(c) of Regulation 1215/2012 of the European Parliament and of the Council. On the other hand, provision of the service in view of mere compliance with the prohibition to discriminate laid down in Regulation (EU) 2018/302 of the European Parliament and of the Council 11 cannot, on that ground alone, be considered as directing or targeting activities towards a given territory within the Union.
Recital 12
Hosting service providers should apply certain duties of care, in order to prevent the dissemination of terrorist content on their services. These duties of care should not amount to a general monitoring obligation. Duties of care should include that, when applying this Regulation, hosting services providers act in a diligent, proportionate and non-discriminatory manner in respect of content that they store, in particular when implementing their own terms and conditions, with a view to avoiding removal of content which is not terrorist. The removal or disabling of access has to be undertaken in the observance of freedom of expression and information.
Recital 13
The procedure and obligations resulting from legal orders requesting hosting service providers to remove terrorist content or disable access to it, following an assessment by the competent authorities, should be harmonised. Member States should remain free as to the choice of the competent authorities allowing them to designate administrative, law enforcement or judicial authorities with that task. Given the speed at which terrorist content is disseminated across online services, this provision imposes obligations on hosting service providers to ensure that terrorist content identified in the removal order is removed or access to it is disabled within one hour from receiving the removal order. It is for the hosting service providers to decide whether to remove the content in question or disable access to the content for users in the Union.
Recital 17
When putting in place proactive measures, hosting service providers should ensure that users' right to freedom of expression and information - including to freely receive and impart information - is preserved. In addition to any requirement laid down in the law, including the legislation on protection of personal data, hosting service providers should act with due diligence and implement safeguards,

including notably human oversight and verifications, where appropriate, to avoid any unintended and erroneous decision leading to removal of content that is not terrorist content. This is of particular relevance when hosting service providers use automated means to detect terrorist content. Any decision to use automated means, whether taken by the hosting service provider itself or pursuant to a request by the competent authority, should be assessed with regard to the reliability of the underlying technology and the ensuing impact on fundamental rights.

Recital 34

In the absence of a general requirement for service providers to ensure a physical presence within the territory of the Union, there is a need to ensure clarity under which Member State's jurisdiction the hosting service provider offering services within the Union falls. As a general rule, the hosting service provider falls under the jurisdiction of the Member State in which it has its main establishment or in which it has designated a legal representative. Nevertheless, where another Member State issues a removal order, its authorities should be able to enforce their orders by taking coercive measures of a non-punitive nature, such as penalty payments. With regards to a hosting service provider which has no establishment in the Union and does not designate a legal representative, any Member State should, nevertheless, be able to issue penalties, provided that the principle of ne bis in idem is respected.

Recital 35

Those hosting service providers which are not established in the Union, should designate in writing a legal representative in order to ensure the compliance with and enforcement of the obligations under this Regulation.

Article 1
Subject matter and scope

1.This Regulation lays down uniform rules to prevent the misuse of hosting services for the dissemination of terrorist content online. It lays down in particular:
(a)rules on duties of care to be applied by hosting service providers in order to prevent the dissemination of terrorist content through their services and ensure, where necessary, its swift removal;
(b)a set of measures to be put in place by Member States to identify terrorist content, to enable its swift removal by hosting service providers and to facilitate cooperation with the competent authorities in other Member States, hosting service providers and where appropriate relevant Union bodies.
2.This Regulation shall apply to hosting service providers offering services in the Union, irrespective of their place of main establishment.

Article 2
Definitions

For the purposes of this Regulation, the following definitions shall apply:
(1) 'hosting service provider' means a provider of information society services consisting in the storage of information provided by and at the request of the content provider and in making the information stored available to third parties;
(2) 'content provider' means a user who has provided information that is, or that has been, stored at the request of the user by a hosting service provider;
(3) 'to offer services in the Union' means: enabling legal or natural persons in one or more Member States to use the services of the hosting service provider which has a substantial connection to that Member State or Member States, such as
(a) establishment of the hosting service provider in the Union;
(b) significant number of users in one or more Member States;
(c) targeting of activities towards one or more Member States.
(4) 'terrorist offences' means offences as defined in Article 3(1) of Directive (EU) 2017/541;
(5) 'terrorist content' means one or more of the following information:
(a) inciting or advocating, including by glorifying, the commission of terrorist offences, thereby causing a danger that such acts be committed;
(b) encouraging the contribution to terrorist offences;

(c) promoting the activities of a terrorist group, in particular by encouraging the participation in or support to a terrorist group within the meaning of Article 2(3) of Directive (EU) 2017/541;
(d) instructing on methods or techniques for the purpose of committing terrorist offences.
(6) ‘dissemination of terrorist content’ means making terrorist content available to third parties on the hosting service providers’ services;
(7) ‘terms and conditions' means all terms, conditions and clauses, irrespective of their name or form, which govern the contractual relationship between the hosting service provider and their users;
(8) 'referral' means a notice by a competent authority or, where applicable, a relevant Union body to a hosting service provider about information that may be considered terrorist content, for the provider’s voluntary consideration of the compatibility with its own terms and conditions aimed to prevent dissemination of terrorism content;
(9) ‘main establishment’ means the head office or registered office within which the principal financial functions and operational control are exercised.

Article 3
Duties of care

1.Hosting service providers shall take appropriate, reasonable and proportionate actions in accordance with this Regulation, against the dissemination of terrorist content and to protect users from terrorist content. In doing so, they shall act in a diligent, proportionate and non-discriminatory manner, and with due regard to the fundamental rights of the users and take into account the fundamental importance of the freedom of expression and information in an open and democratic society.
2.Hosting service providers shall include in their terms and conditions, and apply, provisions to prevent the dissemination of terrorist content.

Article 6
Proactive measures

1. Hosting service providers shall, where appropriate, take proactive measures to protect their services against the dissemination of terrorist content. The measures shall be effective and proportionate, taking into account the risk and level of exposure to terrorist content, the fundamental rights of the users, and the fundamental importance of the freedom of expression and information in an open and democratic society.
2. Where it has been informed according to Article 4(9), the competent authority referred to in Article 17(1)(c) shall request the hosting service provider to submit a report, within three months after receipt of the request and thereafter at least on an annual basis, on the specific proactive measures it has taken, including by using automated tools, with a view to:
(a) preventing the re-upload of content which has previously been removed or to which access has been disabled because it is considered to be terrorist content;
(b) detecting, identifying and expeditiously removing or disabling access to terrorist content.
Such a request shall be sent to the main establishment of the hosting service provider or to the legal representative designated by the service provider.
The reports shall include all relevant information allowing the competent authority referred to in Article 17(1)(c) to assess whether the proactive measures are effective and proportionate, including to evaluate the functioning of any automated tools used as well as the human oversight and verification mechanisms employed.
3. Where the competent authority referred to in Article 17(1)(c) considers that the proactive measures taken and reported under paragraph 2 are insufficient in mitigating and managing the risk and level of exposure, it may request the hosting service provider to take specific additional proactive measures. For that purpose, the hosting service provider shall cooperate with the competent authority referred to in Article 17(1)(c) with a view to identifying the specific measures that the hosting service provider shall put in place, establishing key objectives and benchmarks as well as timelines for their implementation.
4. Where no agreement can be reached within the three months from the request pursuant to paragraph 3, the competent authority referred to in Article 17(1)(c) may issue a decision imposing specific additional necessary and proportionate proactive measures. The decision shall take into account, in particular, the economic capacity of the hosting service provider and the effect of such measures on the fundamental rights of the users and the fundamental importance of the freedom of expression and information. Such a decision shall be sent to the main establishment of the hosting service provider or to the legal representative designated by the service provider. The hosting service provider shall regularly report on the implementation of such measures as specified by the competent authority referred to in Article 17(1)(c).

5. A hosting service provider may, at any time, request the competent authority referred to in Article 17(1)(c) a review and, where appropriate, to revoke a request or decision pursuant to paragraphs 2, 3, and 4 respectively. The competent authority shall provide a reasoned decision within a reasonable period of time after receiving the request by the hosting service provider.

Article 8
Transparency obligations

1. Hosting service providers shall set out in their terms and conditions their policy to prevent the dissemination of terrorist content, including, where appropriate, a meaningful explanation of the functioning of proactive measures including the use of automated tools.
2. Hosting service providers shall publish annual transparency reports on action taken against the dissemination of terrorist content.
3. Transparency reports shall include at least the following information:
(a) information about the hosting service provider's measures in relation to the detection, identification and removal of terrorist content;
(b) information about the hosting service provider's measures to prevent the re-upload of content which has previously been removed or to which access has been disabled because it is considered to be terrorist content;
(c) number of pieces of terrorist content removed or to which access has been disabled, following removal orders, referrals, or proactive measures, respectively;
(d) overview and outcome of complaint procedures.

Article 9
Safeguards regarding the use and implementation of proactive measures

1. Where hosting service providers use automated tools pursuant to this Regulation in respect of content that they store, they shall provide effective and appropriate safeguards to ensure that decisions taken concerning that content, in particular decisions to remove or disable content considered to be terrorist content, are accurate and well-founded.
2. Safeguards shall 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 terrorist content.

Article 12
Capabilities of competent authorities

Member States shall ensure that their competent authorities have the necessary capability and sufficient resources to achieve the aims and fulfil their obligations under this Regulation.

Article 13
Cooperation between hosting service providers, competent authorities and where appropriate relevant Union bodies

1. Competent authorities in Member States shall inform, coordinate and cooperate with each other and, where appropriate, with relevant Union bodies such as Europol with regard to removal orders and referrals to avoid duplication, enhance coordination and avoid interference with investigations in different Member States.
2. Competent authorities in Member States shall inform, coordinate and cooperate with the competent authority referred to in Article 17(1)(c) and (d) with regard to measures taken pursuant to Article 6 and enforcement actions pursuant to Article 18. Member States shall make sure that the competent authority referred to in Article 17(1)(c) and (d) is in possession of all the relevant information. For that purpose, Member States shall provide for the appropriate communication channels or mechanisms to ensure that the relevant information is shared in a timely manner.
3. Member States and hosting service providers may choose to make use of dedicated tools, including, where appropriate, those established by relevant Union bodies such as Europol, to facilitate in particular:
(a) the processing and feedback relating to removal orders pursuant to Article 4;
(b) the processing and feedback relating to referrals pursuant to Article 5;
(c) co-operation with a view to identify and implement proactive measures pursuant to Article 6.

4. Where hosting service providers become aware of any evidence of terrorist offences, they shall promptly inform authorities competent for the investigation and prosecution in criminal offences in the concerned Member State or the point of contact in the Member State pursuant to Article 14(2), where they have their main establishment or a legal representative. Hosting service providers may, in case of doubt, transmit this information to Europol for appropriate follow up.

Article 15
Jurisdiction

1. The Member State in which the main establishment of the hosting service provider is located shall have the jurisdiction for the purposes of Articles 6, 18, and 21. A hosting service provider which does not have its main establishment within one of the Member States shall be deemed to be under the jurisdiction of the Member State where the legal representative referred to in Article 16 resides or is established.
2. Where a hosting service provider fails to designate a legal representative, all Member States shall have jurisdiction.
3.Where an authority of another Member State has issued a removal order according to Article 4(1), that Member State has jurisdiction to take coercive measures according to its national law in order to enforce the removal order.

Article 16
Legal representative

1. A hosting service provider which does not have an establishment in the Union but offers services in the Union, shall designate, in writing, a legal or natural person as its legal representative in the Union for the receipt of, compliance with and enforcement of removal orders, referrals, requests and decisions issued by the competent authorities on the basis of this Regulation. The legal representative shall reside or be established in one of the Member States where the hosting service provider offers the services.
2. The hosting service provider shall entrust the legal representative with the receipt, compliance and enforcement of the removal orders, referrals, requests and decisions referred to in paragraph 1 on behalf of the hosting service provider concerned. Hosting service providers shall provide their legal representative with the necessary powers and resource to cooperate with the competent authorities and comply with these decisions and orders.
3.The designated legal representative can be held liable for non-compliance with obligations under this Regulation, without prejudice to the liability and legal actions that could be initiated against the hosting service provider.
4.The hosting service provider shall notify the competent authority referred to in Article 17(1)(d) in the Member State where the legal representative resides or is established about the designation. Information about the legal representative shall be publicly available.

III. Recommendations on EU Level

A. 2006 Recommendation on the Protection of Minors and Human Dignity

Recommendation 2006/952/EC, *OJ L 378, 27.12.2006, p. 72–77*

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006H0952

The European Parliament and the Council of the European Union recommend that:

I. The Member States, in the interests of promoting the development of the audiovisual and on-line information services industry, take the necessary measures to ensure the protection of minors and human dignity in all audiovisual and on-line information services by:

1. considering the introduction of measures into their domestic law or practice regarding the right of reply or equivalent remedies in relation to on-line media, with due regard for their domestic and constitutional legislative provisions, and without prejudice to the possibility of adapting the manner in which it is exercised to take into account the particularities of each type of medium;

2. promoting, in order to encourage the take-up of technological developments, in addition to and consistently with existing legal and other measures regarding broadcasting services, and in close cooperation with the parties concerned:

(a) action to enable minors to make responsible use of audiovisual and on-line information services, notably by improving the level of awareness among parents, teachers and trainers of the potential of the new services and of the means whereby they may be made safe for minors, in particular through media literacy or media education programmes and, for instance, by continuous training within school education,

(b) action to facilitate, where appropriate and necessary, the identification of, and access to, quality content and services for minors, including through the provision of means of access in educational establishments and public places,

(c) action to inform citizens more about the possibilities offered by the Internet;

examples of possible actions concerning media literacy are outlined in Annex II;

3. promoting a responsible attitude on the part of professionals, intermediaries and users of new communication media such as the Internet by:

(a) encouraging the audiovisual and on-line information services industry, without infringing freedom of expression or of the press, to avoid all discrimination based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation, in all audiovisual and on-line information services, and to combat such discrimination,

(b) encouraging vigilance and the reporting of pages considered illegal, without prejudice to Directive 2000/31/EC,

(c) drawing up a code of conduct in cooperation with professionals and regulatory authorities at national and Community level;

4. promoting measures to combat all illegal activities harmful to minors on the Internet and make the Internet a much more secure medium; consideration could be given inter alia to the following measures:

(a) adopting a quality label for service providers, so that users can easily check whether or not a given provider subscribes to a code of conduct,

(b) establishing appropriate means for the reporting of illegal and/or suspicious activities on the Internet.

II. The audiovisual and on-line information services industry and other parties concerned:

1. develop positive measures for the benefit of minors, including initiatives to facilitate their wider access to audiovisual and on-line information services, while avoiding potentially harmful content, for instance by means of filtering systems. Such measures could include harmonisation through cooperation between the regulatory, self-regulatory and co-regulatory bodies of the Member States, and through the exchange of best practices concerning such issues as a system of common descriptive symbols or warning messages indicating the age category and/or which aspects of the content have led to a certain age recommendation, which would help users to assess the content of audiovisual and on-line information services. This could take place, for instance, through the actions outlined in Annex III;

2. examine the possibility of creating filters which would prevent information offending against human dignity from passing through the Internet;

3. develop measures to increase the use of content labelling systems for material distributed over the Internet;

4. consider effective means of avoiding and combating discrimination based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation in audiovisual and on-line information services and of promoting a diversified and realistic picture of the skills and potential of men and women in society.

B. Recommendation on Tackling Illegal Content Online

Recommendation (EU) 2018/334, *OJ L 63, 6.3.2018, p. 50–61*

https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32018H0334

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.

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.