

## I

(Legislative acts)

## REGULATIONS

**REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL****of 19 October 2022****on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)****(Text with EEA relevance)**

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee <sup>(1)</sup>,

Having regard to the opinion of the Committee of the Regions <sup>(2)</sup>,

Acting in accordance with the ordinary legislative procedure <sup>(3)</sup>,

Whereas:

- (1) Information society services and especially intermediary services have become an important part of the Union's economy and the daily life of Union citizens. Twenty years after the adoption of the existing legal framework applicable to such services laid down in Directive 2000/31/EC of the European Parliament and of the Council <sup>(4)</sup>, new and innovative business models and services, such as online social networks and online platforms allowing consumers to conclude distance contracts with traders, have allowed business users and consumers to impart and access information and engage in transactions in novel ways. A majority of Union citizens now uses those services on a daily basis. However, the digital transformation and increased use of those services has also resulted in new risks and challenges for individual recipients of the relevant service, companies and society as a whole.
- (2) Member States are increasingly introducing, or are considering introducing, national laws on the matters covered by this Regulation, imposing, in particular, diligence requirements for providers of intermediary services as regards the way they should tackle illegal content, online disinformation or other societal risks. Those diverging national laws negatively affect the internal market, which, pursuant to Article 26 of the Treaty on the Functioning of the European Union (TFEU), comprises an area without internal frontiers in which the free movement of goods and services and freedom of establishment are ensured, taking into account the inherently cross-border nature of the internet, which is generally used to provide those services. The conditions for the provision of intermediary services

<sup>(1)</sup> OJ C 286, 16.7.2021, p. 70.

<sup>(2)</sup> OJ C 440, 29.10.2021, p. 67.

<sup>(3)</sup> Position of the European Parliament of 5 July 2022 (not yet published in the Official Journal) and decision of the Council of 4 October 2022.

<sup>(4)</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

across the internal market should be harmonised, so as to provide businesses with access to new markets and opportunities to exploit the benefits of the internal market, while allowing consumers and other recipients of the services to have increased choice. Business users, consumers and other users are considered to be 'recipients of the service' for the purpose of this Regulation.

- (3) Responsible and diligent behaviour by providers of intermediary services is essential for a safe, predictable and trustworthy online environment and for allowing Union citizens and other persons to exercise their fundamental rights guaranteed in the Charter of Fundamental Rights of the European Union (the 'Charter'), in particular the freedom of expression and of information, the freedom to conduct a business, the right to non-discrimination and the attainment of a high level of consumer protection.
- (4) Therefore, in order to safeguard and improve the functioning of the internal market, a targeted set of uniform, effective and proportionate mandatory rules should be established at Union level. This Regulation provides the conditions for innovative digital services to emerge and to scale up in the internal market. The approximation of national regulatory measures at Union level concerning the requirements for providers of intermediary services is necessary to avoid and put an end to fragmentation of the internal market and to ensure legal certainty, thus reducing uncertainty for developers and fostering interoperability. By using requirements that are technology neutral, innovation should not be hampered but instead be stimulated.
- (5) This Regulation should apply to providers of certain information society services as defined in Directive (EU) 2015/1535 of the European Parliament and of the Council <sup>(7)</sup>, that is, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient. Specifically, this Regulation should apply to providers of intermediary services, and in particular intermediary services consisting of services known as 'mere conduit', 'caching' and 'hosting' services, given that the exponential growth of the use made of those services, mainly for legitimate and socially beneficial purposes of all kinds, has also increased their role in the intermediation and spread of unlawful or otherwise harmful information and activities.
- (6) In practice, certain providers of intermediary services intermediate in relation to services that may or may not be provided by electronic means, such as remote information technology services, transport, accommodation or delivery services. This Regulation should apply only to intermediary services and not affect requirements set out in Union or national law relating to products or services intermediated through intermediary services, including in situations where the intermediary service constitutes an integral part of another service which is not an intermediary service as recognised in the case-law of the Court of Justice of the European Union.
- (7) In order to ensure the effectiveness of the rules laid down in this Regulation and a level playing field within the internal market, those rules should apply to providers of intermediary services irrespective of their place of establishment or their location, in so far as they offer services in the Union, as evidenced by a substantial connection to the Union.
- (8) Such a substantial connection to the Union should be considered to exist where the service provider has an establishment in the Union or, in the absence of such an establishment, where the number of recipients of the service in one or more Member States is significant in relation to the population thereof, or on the basis of 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 products or services, or the use of a relevant top-level domain. 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 the provision of local advertising or

---

<sup>(7)</sup> Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

advertising in a language used in that Member State, or from the handling of customer relations such as by providing customer service in a language generally used in that Member State. A substantial connection should also be assumed where a service provider directs its activities to one or more Member States within the meaning of Article 17(1), point (c), of Regulation (EU) No 1215/2012 of the European Parliament and of the Council <sup>(6)</sup>. In contrast, mere technical accessibility of a website from the Union cannot, on that ground alone, be considered as establishing a substantial connection to the Union.

- (9) This Regulation fully harmonises the rules applicable to intermediary services in the internal market with the objective of ensuring a safe, predictable and trusted online environment, addressing the dissemination of illegal content online and the societal risks that the dissemination of disinformation or other content may generate, and within which fundamental rights enshrined in the Charter are effectively protected and innovation is facilitated. Accordingly, Member States should not adopt or maintain additional national requirements relating to the matters falling within the scope of this Regulation, unless explicitly provided for in this Regulation, since this would affect the direct and uniform application of the fully harmonised rules applicable to providers of intermediary services in accordance with the objectives of this Regulation. This should not preclude the possibility of applying other national legislation applicable to providers of intermediary services, in compliance with Union law, including Directive 2000/31/EC, in particular its Article 3, where the provisions of national law pursue other legitimate public interest objectives than those pursued by this Regulation.
- (10) This Regulation should be without prejudice to other acts of Union law regulating the provision of information society services in general, regulating other aspects of the provision of intermediary services in the internal market or specifying and complementing the harmonised rules set out in this Regulation, such as Directive 2010/13/EU of the European Parliament and of the Council <sup>(7)</sup> including the provisions thereof regarding video-sharing platforms, Regulations (EU) 2019/1148 <sup>(8)</sup>, (EU) 2019/1150 <sup>(9)</sup>, (EU) 2021/784 <sup>(10)</sup> and (EU) 2021/1232 <sup>(11)</sup> of the European Parliament and of the Council and Directive 2002/58/EC of the European Parliament and of the Council <sup>(12)</sup>, and provisions of Union law set out in a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and in a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.

---

<sup>(6)</sup> Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

<sup>(7)</sup> Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (OJ L 95, 15.4.2010, p. 1).

<sup>(8)</sup> Regulation (EU) 2019/1148 of the European Parliament and of the Council of 20 June 2019 on the marketing and use of explosives precursors, amending Regulation (EC) No 1907/2006 and repealing Regulation (EU) No 98/2013 (OJ L 186, 11.7.2019, p. 1).

<sup>(9)</sup> Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (OJ L 186, 11.7.2019, p. 57).

<sup>(10)</sup> Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of the terrorist content online (OJ L 172, 17.5.2021, p. 79).

<sup>(11)</sup> Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse (OJ L 274, 30.7.2021, p. 41).

<sup>(12)</sup> Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

Similarly, for reasons of clarity, this Regulation should be without prejudice to Union law on consumer protection, in particular Regulations (EU) 2017/2394<sup>(13)</sup> and (EU) 2019/1020<sup>(14)</sup> of the European Parliament and of the Council, Directives 2001/95/EC<sup>(15)</sup>, 2005/29/EC<sup>(16)</sup>, 2011/83/EU<sup>(17)</sup> and 2013/11/EU<sup>(18)</sup> of the European Parliament and of the Council, and Council Directive 93/13/EEC<sup>(19)</sup>, and on the protection of personal data, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council<sup>(20)</sup>.

This Regulation should also be without prejudice to Union rules on private international law, in particular rules regarding jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, as Regulation (EU) No 1215/2012, and rules on the law applicable to contractual and non-contractual obligations. The protection of individuals with regard to the processing of personal data is governed solely by the rules of Union law on that subject, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC. This Regulation should also be without prejudice to Union law on working conditions and Union law in the field of judicial cooperation in civil and criminal matters. However, to the extent that those Union legal acts pursue the same objectives as those laid down in this Regulation, the rules of this Regulation should apply in respect of issues that are not addressed or not fully addressed by those other legal acts as well as issues on which those other legal acts leave Member States the possibility of adopting certain measures at national level.

- (11) It should be clarified that this Regulation is without prejudice to Union law on copyright and related rights, including Directives 2001/29/EC<sup>(21)</sup>, 2004/48/EC<sup>(22)</sup> and (EU) 2019/790<sup>(23)</sup> of the European Parliament and of the Council, which establish specific rules and procedures that should remain unaffected.
- (12) In order to achieve the objective of ensuring a safe, predictable and trustworthy online environment, for the purpose of this Regulation the concept of 'illegal content' should broadly reflect the existing rules in the offline environment. In particular, the concept of 'illegal content' should be defined broadly to cover information relating to illegal content, products, services and activities. In particular, that concept should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that the applicable rules render illegal in view of the fact that it relates to illegal activities. Illustrative examples include the sharing of images depicting child sexual abuse, the

<sup>(13)</sup> Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 (OJ L 345, 27.12.2017, p. 1).

<sup>(14)</sup> Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, p. 1).

<sup>(15)</sup> Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (OJ L 11, 15.1.2002, p. 4).

<sup>(16)</sup> Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (OJ L 149, 11.6.2005, p. 22).

<sup>(17)</sup> Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (OJ L 304, 22.11.2011, p. 64).

<sup>(18)</sup> Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (OJ L 165, 18.6.2013, p. 63).

<sup>(19)</sup> Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29).

<sup>(20)</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

<sup>(21)</sup> Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ L 167, 22.6.2001, p. 10).

<sup>(22)</sup> Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30.4.2004, p. 45).

<sup>(23)</sup> Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (OJ L 130, 17.5.2019, p. 92).

unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit products, the sale of products or the provision of services in infringement of consumer protection law, the non-authorised use of copyright protected material, the illegal offer of accommodation services or the illegal sale of live animals. In contrast, an eyewitness video of a potential crime should not be considered to constitute illegal content, merely because it depicts an illegal act, where recording or disseminating such a video to the public is not illegal under national or Union law. In this regard, it is immaterial whether the illegality of the information or activity results from Union law or from national law that is in compliance with Union law and what the precise nature or subject matter is of the law in question.

- (13) Considering the particular characteristics of the services concerned and the corresponding need to make the providers thereof subject to certain specific obligations, it is necessary to distinguish, within the broader category of providers of hosting services as defined in this Regulation, the subcategory of online platforms. Online platforms, such as social networks or online platforms allowing consumers to conclude distance contracts with traders, should be defined as providers of hosting services that not only store information provided by the recipients of the service at their request, but that also disseminate that information to the public at the request of the recipients of the service. However, in order to avoid imposing overly broad obligations, providers of hosting services should not be considered as online platforms where the dissemination to the public is merely a minor and purely ancillary feature that is intrinsically linked to another service, or a minor functionality of the principal service, and that feature or functionality cannot, for objective technical reasons, be used without that other or principal service, and the integration of that feature or functionality is not a means to circumvent the applicability of the rules of this Regulation applicable to online platforms. For example, the comments section in an online newspaper could constitute such a feature, where it is clear that it is ancillary to the main service represented by the publication of news under the editorial responsibility of the publisher. In contrast, the storage of comments in a social network should be considered an online platform service where it is clear that it is not a minor feature of the service offered, even if it is ancillary to publishing the posts of recipients of the service. For the purposes of this Regulation, cloud computing or web-hosting services should not be considered to be an online platform where dissemination of specific information to the public constitutes a minor and ancillary feature or a minor functionality of such services.

Moreover, cloud computing services and web-hosting services, when serving as infrastructure, such as the underlying infrastructural storage and computing services of an internet-based application, website or online platform, should not in themselves be considered as disseminating to the public information stored or processed at the request of a recipient of the application, website or online platform which they host.

- (14) The concept of 'dissemination to the public', as used in this Regulation, should entail the making available of information to a potentially unlimited number of persons, meaning making the information easily accessible to recipients of the service in general without further action by the recipient of the service providing the information being required, irrespective of whether those persons actually access the information in question. Accordingly, where access to information requires registration or admittance to a group of recipients of the service, that information should be considered to be disseminated to the public only where recipients of the service seeking to access the information are automatically registered or admitted without a human decision or selection of whom to grant access. Interpersonal communication services, as defined in Directive (EU) 2018/1972 of the European Parliament and of the Council <sup>(24)</sup>, such as emails or private messaging services, fall outside the scope of the definition of online platforms as they are used for interpersonal communication between a finite number of persons determined by the sender of the communication. However, the obligations set out in this Regulation for providers of online platforms may apply to services that allow the making available of information to a potentially unlimited number of recipients, not determined by the sender of the communication, such as through public groups or open channels. Information should be considered disseminated to the public within the meaning of this Regulation only where that dissemination occurs upon the direct request by the recipient of the service that provided the information.

<sup>(24)</sup> Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).

- (15) Where some of the services provided by a provider are covered by this Regulation whilst others are not, or where the services provided by a provider are covered by different sections of this Regulation, the relevant provisions of this Regulation should apply only in respect of those services that fall within their scope.
- (16) The legal certainty provided by the horizontal framework of conditional exemptions from liability for providers of intermediary services, laid down in Directive 2000/31/EC, has allowed many novel services to emerge and scale up across the internal market. That framework should therefore be preserved. However, in view of the divergences when transposing and applying the relevant rules at national level, and for reasons of clarity and coherence, that framework should be incorporated in this Regulation. It is also necessary to clarify certain elements of that framework, having regard to the case-law of the Court of Justice of the European Union.
- (17) The rules on liability of providers of intermediary services set out in this Regulation should only establish when the provider of intermediary services concerned cannot be held liable in relation to illegal content provided by the recipients of the service. Those rules should not be understood to provide a positive basis for establishing when a provider can be held liable, which is for the applicable rules of Union or national law to determine. Furthermore, the exemptions from liability established in this Regulation should apply in respect of any type of liability as regards any type of illegal content, irrespective of the precise subject matter or nature of those laws.
- (18) The exemptions from liability established in this Regulation should not apply where, instead of confining itself to providing the services neutrally by a merely technical and automatic processing of the information provided by the recipient of the service, the provider of intermediary services plays an active role of such a kind as to give it knowledge of, or control over, that information. Those exemptions should accordingly not be available in respect of liability relating to information provided not by the recipient of the service but by the provider of the intermediary service itself, including where the information has been developed under the editorial responsibility of that provider.
- (19) In view of the different nature of the activities of ‘mere conduit’, ‘caching’ and ‘hosting’ and the different position and abilities of the providers of the services in question, it is necessary to distinguish the rules applicable to those activities, in so far as under this Regulation they are subject to different requirements and conditions and their scope differs, as interpreted by the Court of Justice of the European Union.
- (20) Where a provider of intermediary services deliberately collaborates with a recipient of the services in order to undertake illegal activities, the services should not be deemed to have been provided neutrally and the provider should therefore not be able to benefit from the exemptions from liability provided for in this Regulation. This should be the case, for instance, where the provider offers its service with the main purpose of facilitating illegal activities, for example by making explicit that its purpose is to facilitate illegal activities or that its services are suited for that purpose. The fact alone that a service offers encrypted transmissions or any other system that makes the identification of the user impossible should not in itself qualify as facilitating illegal activities.
- (21) A provider should be able to benefit from the exemptions from liability for ‘mere conduit’ and for ‘caching’ services when it is in no way involved with the information transmitted or accessed. This requires, among other things, that the provider does not modify the information that it transmits or to which it provides access. However, this requirement should not be understood to cover manipulations of a technical nature which take place in the course of the transmission or access, as long as those manipulations do not alter the integrity of the information transmitted or to which access is provided.
- (22) In order to benefit from the exemption from liability for hosting services, the provider should, upon obtaining actual knowledge or awareness of illegal activities or illegal content, act expeditiously to remove or to disable access to that content. The removal or disabling of access should be undertaken in the observance of the fundamental rights of the recipients of the service, including the right to freedom of expression and of information. The provider can obtain such actual knowledge or awareness of the illegal nature of the content, *inter alia* through its own-initiative investigations or through notices submitted to it by individuals or entities in accordance with this Regulation in so

far as such notices are sufficiently precise and adequately substantiated to allow a diligent economic operator to reasonably identify, assess and, where appropriate, act against the allegedly illegal content. However, such actual knowledge or awareness cannot be considered to be obtained solely on the ground that that provider is aware, in a general sense, of the fact that its service is also used to store illegal content. Furthermore, the fact that the provider automatically indexes information uploaded to its service, that it has a search function or that it recommends information on the basis of the profiles or preferences of the recipients of the service is not a sufficient ground for considering that provider to have 'specific' knowledge of illegal activities carried out on that platform or of illegal content stored on it.

- (23) The exemption of liability should not apply where the recipient of the service is acting under the authority or the control of the provider of a hosting service. For example, where the provider of an online platform that allows consumers to conclude distance contracts with traders determines the price of the goods or services offered by the trader, it could be considered that the trader acts under the authority or control of that online platform.
- (24) In order to ensure the effective protection of consumers when engaging in intermediated commercial transactions online, certain providers of hosting services, namely online platforms that allow consumers to conclude distance contracts with traders, should not be able to benefit from the exemption from liability for hosting service providers established in this Regulation, in so far as those online platforms present the relevant information relating to the transactions at issue in such a way as to lead consumers to believe that that information was provided by those online platforms themselves or by traders acting under their authority or control, and that those online platforms thus have knowledge of or control over the information, even if that may in reality not be the case. Examples of such behaviour could be where an online platform fails to display clearly the identity of the trader, as required by this Regulation, where an online platform withholds the identity or contact details of the trader until after the conclusion of the contract concluded between the trader and the consumer, or where an online platform markets the product or service in its own name rather than in the name of the trader who will supply that product or service. In that regard, it should be determined objectively, on the basis of all relevant circumstances, whether the presentation could lead an average consumer to believe that the information in question was provided by the online platform itself or by traders acting under its authority or control.
- (25) The exemptions from liability established in this Regulation should not affect the possibility of injunctions of different kinds against providers of intermediary services, even where they meet the conditions set out as part of those exemptions. Such injunctions could, in particular, consist of orders by courts or administrative authorities, issued in compliance with Union law, requiring the termination or prevention of any infringement, including the removal of illegal content specified in such orders, or the disabling of access to it.
- (26) In order to create legal certainty, and not to discourage activities that aim to detect, identify and act against illegal content that providers of all categories of intermediary services undertake on a voluntary basis, it should be clarified that the mere fact that providers undertake such activities does not render unavailable the exemptions from liability set out in this Regulation, provided those activities are carried out in good faith and in a diligent manner. The condition of acting in good faith and in a diligent manner should include acting in an objective, non-discriminatory and proportionate manner, with due regard to the rights and legitimate interests of all parties involved, and providing the necessary safeguards against unjustified removal of legal content, in accordance with the objective and requirements of this Regulation. To that aim, the providers concerned should, for example, take reasonable measures to ensure that, where automated tools are used to conduct such activities, the relevant technology is sufficiently reliable to limit to the maximum extent possible the rate of errors. In addition, it is appropriate to clarify that the mere fact that the providers take measures, in good faith, to comply with the requirements of Union law, including those set out in this Regulation as regards the implementation of their terms and conditions, should not render unavailable the exemptions from liability set out in this Regulation. Therefore, any such activities and measures that a provider may have taken should not be taken into account when determining whether the provider can rely on an exemption from liability, in particular as regards whether the provider provides its service neutrally and can therefore fall within the scope of the relevant provision, without this rule however implying that the provider can necessarily rely thereon. Voluntary actions should not be used to circumvent the obligations of providers of intermediary services under this Regulation.

- (27) Whilst the rules on liability of providers of intermediary services set out in this Regulation concentrate on the exemption from liability of providers of intermediary services, it is important to recall that, despite the generally important role played by such providers, the problem of illegal content and activities online should not be dealt with by solely focusing on their liability and responsibilities. Where possible, third parties affected by illegal content transmitted or stored online should attempt to resolve conflicts relating to such content without involving the providers of intermediary services in question. Recipients of the service should be held liable, where the applicable rules of Union and national law determining such liability so provide, for the illegal content that they provide and may disseminate to the public through intermediary services. Where appropriate, other actors, such as group moderators in closed online environments, in particular in the case of large groups, should also help to avoid the spread of illegal content online, in accordance with the applicable law. Furthermore, where it is necessary to involve information society services providers, including providers of intermediary services, any requests or orders for such involvement should, as a general rule, be directed to the specific provider that has the technical and operational ability to act against specific items of illegal content, so as to prevent and minimise any possible negative effects on the availability and accessibility of information that is not illegal content.
- (28) Since 2000, new technologies have emerged that improve the availability, efficiency, speed, reliability, capacity and security of systems for the transmission, 'findability' and storage of data online, leading to an increasingly complex online ecosystem. In this regard, it should be recalled that providers of services establishing and facilitating the underlying logical architecture and proper functioning of the internet, including technical auxiliary functions, can also benefit from the exemptions from liability set out in this Regulation, to the extent that their services qualify as 'mere conduit', 'caching' or 'hosting' services. Such services include, as the case may be, wireless local area networks, domain name system (DNS) services, top-level domain name registries, registrars, certificate authorities that issue digital certificates, virtual private networks, online search engines, cloud infrastructure services, or content delivery networks, that enable, locate or improve the functions of other providers of intermediary services. Likewise, services used for communications purposes, and the technical means of their delivery, have also evolved considerably, giving rise to online services such as Voice over IP, messaging services and web-based email services, where the communication is delivered via an internet access service. Those services, too, can benefit from the exemptions from liability, to the extent that they qualify as 'mere conduit', 'caching' or 'hosting' services.
- (29) Intermediary services span a wide range of economic activities which take place online and that develop continually to provide for transmission of information that is swift, safe and secure, and to ensure convenience of all participants of the online ecosystem. For example, 'mere conduit' intermediary services include generic categories of services, such as internet exchange points, wireless access points, virtual private networks, DNS services and resolvers, top-level domain name registries, registrars, certificate authorities that issue digital certificates, voice over IP and other interpersonal communication services, while generic examples of 'caching' intermediary services include the sole provision of content delivery networks, reverse proxies or content adaptation proxies. Such services are crucial to ensure the smooth and efficient transmission of information delivered on the internet. Examples of 'hosting services' include categories of services such as cloud computing, web hosting, paid referencing services or services enabling sharing information and content online, including file storage and sharing. Intermediary services may be provided in isolation, as a part of another type of intermediary service, or simultaneously with other intermediary services. Whether a specific service constitutes a 'mere conduit', 'caching' or 'hosting' service depends solely on its technical functionalities, which might evolve in time, and should be assessed on a case-by-case basis.
- (30) Providers of intermediary services should not be, neither *de jure*, nor *de facto*, subject to a monitoring obligation 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, in compliance with Union law, as interpreted by the Court of Justice of the European Union, and in accordance with the conditions established in this Regulation. Nothing in this Regulation should be construed as an imposition of a general monitoring obligation or a general active fact-finding obligation, or as a general obligation for providers to take proactive measures in relation to illegal content.

- (31) Depending on the legal system of each Member State and the field of law at issue, national judicial or administrative authorities, including law enforcement authorities, may order providers of intermediary services to act against one or more specific items of illegal content or to provide certain specific information. The national laws on the basis of which such orders are issued differ considerably and the orders are increasingly addressed in cross-border situations. In order to ensure that those orders can be complied with in an effective and efficient manner, in particular in a cross-border context, so that the public authorities concerned can carry out their tasks and the providers are not subject to any disproportionate burdens, without unduly affecting the rights and legitimate interests of any third parties, it is necessary to set certain conditions that those orders should meet and certain complementary requirements relating to the processing of those orders. Consequently, this Regulation should harmonise only certain specific minimum conditions that such orders should fulfil in order to give rise to the obligation of providers of intermediary services to inform the relevant authorities about the effect given to those orders. Therefore, this Regulation does not provide the legal basis for the issuing of such orders, nor does it regulate their territorial scope or cross-border enforcement.
- (32) The applicable Union or national law on the basis of which those orders are issued might require additional conditions and should be the basis for the enforcement of the respective orders. In the event of non-compliance with such orders, the issuing Member State should be able to enforce them in accordance with its national law. The applicable national law should be in compliance with Union law, including the Charter and the TFEU provisions on the freedom of establishment and the freedom to provide services within the Union, in particular with regard to online gambling and betting services. Similarly, the application of such national laws for the enforcement of the respective orders is without prejudice to applicable Union legal acts or international agreements concluded by the Union or by Member States relating to the cross-border recognition, execution and enforcement of those orders, in particular in civil and criminal matters. On the other hand, the enforcement of the obligation to inform the relevant authorities about the effect given to those orders, as opposed to the enforcement of the orders themselves, should be subject to the rules set out in this Regulation.
- (33) The provider of intermediary services should inform the issuing authority about any follow-up given to such orders without undue delay, in compliance with the time limits set out in relevant Union or national law.
- (34) Relevant national authorities should be able to issue such orders against content considered illegal or orders to provide information on the basis of Union law or national law in compliance with Union law, in particular the Charter, and to address them to providers of intermediary services, including those established in another Member State. However, this Regulation should be without prejudice to Union law in the field of judicial cooperation in civil or criminal matters, including Regulation (EU) No 1215/2012 and a Regulation on European production and preservation orders for electronic evidence in criminal matters, and to national criminal or civil procedural law. Therefore, where those laws in the context of criminal or civil proceedings provide for conditions that are additional to or incompatible with the conditions provided for in this Regulation in relation to orders to act against illegal content or to provide information, the conditions provided for in this Regulation might not apply or might be adapted. In particular, the obligation on the Digital Services Coordinator from the Member State of the issuing authority to transmit a copy of the orders to all other Digital Services Coordinators might not apply in the context of criminal proceedings or might be adapted, where the applicable national criminal procedural law so provides.

Furthermore, the obligation for the orders to contain a statement of reasons explaining why the information is illegal content should be adapted, where necessary, under the applicable national criminal procedural law for the prevention, investigation, detection and prosecution of criminal offences. Finally, the obligation on the providers of intermediary services to inform the recipient of the service might be delayed in accordance with applicable Union or national law, in particular in the context of criminal, civil or administrative proceedings. In addition, the orders should be issued in compliance with Regulation (EU) 2016/679 and the prohibition of general obligations to monitor information or to actively seek facts or circumstances indicating illegal activity laid down in this Regulation. The conditions and requirements laid down in this Regulation which apply to orders to act against illegal content are without prejudice to other Union acts providing for similar systems for acting against specific types of illegal content, such as Regulation (EU) 2021/784, Regulation (EU) 2019/1020, or Regulation (EU) 2017/2394 that confers specific powers to order the provision of information to Member State consumer law

enforcement authorities, whilst the conditions and requirements that apply to orders to provide information are without prejudice to other Union acts providing for similar relevant rules for specific sectors. Those conditions and requirements should be without prejudice to retention and preservation rules under applicable national law, in compliance with Union law and confidentiality requests by law enforcement authorities related to the non-disclosure of information. Those conditions and requirements should not affect the possibility for Member States to require a provider of intermediary services to prevent an infringement, in compliance with Union law including this Regulation, and in particular with the prohibition of general monitoring obligations.

- (35) The conditions and requirements laid down in this Regulation should be fulfilled at the latest when the order is transmitted to the provider concerned. Therefore, the order may be issued in one of the official languages of the issuing authority of the Member State concerned. However, where that language is different from the language declared by the provider of intermediary services, or from another official language of the Member States agreed between the authority issuing the order and the provider of intermediary services, the transmission of the order should be accompanied by a translation of at least the elements of the order which are set out in this Regulation. Where a provider of intermediary services has agreed with the authorities of a Member State to use a certain language, it should be encouraged to accept orders in the same language issued by authorities in other Member States. The orders should include elements that enable the addressee to identify the issuing authority, including the contact details of a contact point within that authority where appropriate, and to verify the authenticity of the order.
- (36) The territorial scope of such orders to act against illegal content should be clearly set out on the basis of the applicable Union or national law enabling the issuance of the order and should not exceed what is strictly necessary to achieve its objectives. In that regard, the national judicial or administrative authority, which might be a law enforcement authority, issuing the order should balance the objective that the order seeks to achieve, in accordance with the legal basis enabling its issuance, with the rights and legitimate interests of all third parties that may be affected by the order, in particular their fundamental rights under the Charter. In particular in a cross-border context, the effect of the order should in principle be limited to the territory of the issuing Member State, unless the illegality of the content derives directly from Union law or the issuing authority considers that the rights at stake require a wider territorial scope, in accordance with Union and international law, while taking into account the interests of international comity.
- (37) The orders to provide information regulated by this Regulation concern the production of specific information about individual recipients of the intermediary service concerned who are identified in those orders for the purposes of determining compliance by the recipients of the service with applicable Union or national rules. Such orders should request information with the aim of enabling the identification of the recipients of the service concerned. Therefore, orders regarding information on a group of recipients of the service who are not specifically identified, including orders to provide aggregate information required for statistical purposes or evidence-based policy-making, are not covered by the requirements of this Regulation on the provision of information.
- (38) Orders to act against illegal content and to provide information are subject to the rules safeguarding the competence of the Member State in which the service provider addressed is established and the rules laying down possible derogations from that competence in certain cases, set out in Article 3 of Directive 2000/31/EC, only if the conditions of that Article are met. Given that the orders in question relate to specific items of illegal content and information, respectively, where they are addressed to providers of intermediary services established in another Member State they do not in principle restrict those providers' freedom to provide their services across borders. Therefore, the rules set out in Article 3 of Directive 2000/31/EC, including those regarding the need to justify measures derogating from the competence of the Member State in which the service provider is established on certain specified grounds and regarding the notification of such measures, do not apply in respect of those orders.

- (39) The requirements to provide information on redress mechanisms available to the provider of the intermediary service and to the recipient of the service who provided the content include a requirement to provide information about administrative complaint-handling mechanisms and judicial redress including appeals against orders issued by judicial authorities. Moreover, Digital Services Coordinators could develop national tools and guidance as regards complaint and redress mechanisms applicable in their respective territory, in order to facilitate access to such mechanisms by recipients of the service. Finally, when applying this Regulation Member States should respect the fundamental right to an effective judicial remedy and to a fair trial as provided for in Article 47 of the Charter. This Regulation should therefore not prevent the relevant national judicial or administrative authorities from issuing, on the basis of the applicable Union or national law, an order to restore content, where such content was in compliance with the terms and conditions of the provider of the intermediary service but has been erroneously considered as illegal by that provider and has been removed.
- (40) In order to achieve the objectives of this Regulation, and in particular to improve the functioning of the internal market and ensure a safe and transparent online environment, it is necessary to establish a clear, effective, predictable and balanced set of harmonised due diligence obligations for providers of intermediary services. Those obligations should aim in particular to guarantee different public policy objectives such as the safety and trust of the recipients of the service, including consumers, minors and users at particular risk of being subject to hate speech, sexual harassment or other discriminatory actions, the protection of relevant fundamental rights enshrined in the Charter, the meaningful accountability of those providers and the empowerment of recipients and other affected parties, whilst facilitating the necessary oversight by competent authorities.
- (41) In that regard, it is important that the due diligence obligations are adapted to the type, size and nature of the intermediary service concerned. This Regulation therefore sets out basic obligations applicable to all providers of intermediary services, as well as additional obligations for providers of hosting services and, more specifically, providers of online platforms and of very large online platforms and of very large online search engines. To the extent that providers of intermediary services fall within a number of different categories in view of the nature of their services and their size, they should comply with all the corresponding obligations of this Regulation in relation to those services. Those harmonised due diligence obligations, which should be reasonable and non-arbitrary, are needed to address the identified public policy concerns, such as safeguarding the legitimate interests of the recipients of the service, addressing illegal practices and protecting the fundamental rights enshrined in the Charter. The due diligence obligations are independent from the question of liability of providers of intermediary services which need therefore to be assessed separately.
- (42) In order to facilitate smooth and efficient two-way communications, including, where relevant, by acknowledging the receipt of such communications, relating to matters covered by this Regulation, providers of intermediary services should be required to designate a single electronic point of contact and to publish and update relevant information relating to that point of contact, including the languages to be used in such communications. The electronic point of contact can also be used by trusted flaggers and by professional entities which are under a specific relationship with the provider of intermediary services. In contrast to the legal representative, the electronic point of contact should serve operational purposes and should not be required to have a physical location. Providers of intermediary services can designate the same single point of contact for the requirements of this Regulation as well as for the purposes of other acts of Union law. When specifying the languages of communication, providers of intermediary services are encouraged to ensure that the languages chosen do not in themselves constitute an obstacle to communication. Where necessary, it should be possible for providers of intermediary services and Member States' authorities to reach a separate agreement on the language of communication, or to seek alternative means to overcome the language barrier, including by using all available technological means or internal and external human resources.
- (43) Providers of intermediary services should also be required to designate a single point of contact for recipients of services, enabling rapid, direct and efficient communication in particular by easily accessible means such as telephone numbers, email addresses, electronic contact forms, chatbots or instant messaging. It should be explicitly indicated when a recipient of the service communicates with chatbots. Providers of intermediary services should allow recipients of services to choose means of direct and efficient communication which do not solely rely on automated tools. Providers of intermediary services should make all reasonable efforts to guarantee that sufficient human and financial resources are allocated to ensure that this communication is performed in a timely and efficient manner.

- (44) Providers of intermediary services that are established in a third country and that offer services in the Union should designate a sufficiently mandated legal representative in the Union and provide information relating to their legal representatives to the relevant authorities and make it publicly available. In order to comply with that obligation, such providers of intermediary services should ensure that the designated legal representative has the necessary powers and resources to cooperate with the relevant authorities. This could be the case, for example, where a provider of intermediary services appoints a subsidiary undertaking of the same group as the provider, or its parent undertaking, if that subsidiary or parent undertaking is established in the Union. However, it might not be the case, for instance, when the legal representative is subject to reconstruction proceedings, bankruptcy, or personal or corporate insolvency. That obligation should allow for the effective oversight and, where necessary, enforcement of this Regulation in relation to those providers. It should be possible for a legal representative to be mandated, in accordance with national law, by more than one provider of intermediary services. It should be possible for the legal representative to also function as a point of contact, provided the relevant requirements of this Regulation are complied with.
- (45) Whilst the freedom of contract of providers of intermediary services should in principle be respected, it is appropriate to set certain rules on the content, application and enforcement of the terms and conditions of those providers in the interests of transparency, the protection of recipients of the service and the avoidance of unfair or arbitrary outcomes. Providers of the intermediary services should clearly indicate and maintain up-to-date in their terms and conditions the information as to the grounds on the basis of which they may restrict the provision of their services. In particular, they should include information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review, as well as the rules of procedure of their internal complaint-handling system. They should also provide easily accessible information on the right to terminate the use of the service. Providers of intermediary services may use graphical elements in their terms of service, such as icons or images, to illustrate the main elements of the information requirements set out in this Regulation. Providers should inform recipients of their service through appropriate means of significant changes made to terms and conditions, for instance when they modify the rules on information that is permitted on their service, or other such changes which could directly impact the ability of the recipients to make use of the service.
- (46) Providers of intermediary services that are primarily directed at minors, for example through the design or marketing of the service, or which are used predominantly by minors, should make particular efforts to render the explanation of their terms and conditions easily understandable to minors.
- (47) When designing, applying and enforcing those restrictions, providers of intermediary services should act in a non-arbitrary and non-discriminatory manner and take into account the rights and legitimate interests of the recipients of the service, including fundamental rights as enshrined in the Charter. For example, providers of very large online platforms should in particular pay due regard to freedom of expression and of information, including media freedom and pluralism. All providers of intermediary services should also pay due regard to relevant international standards for the protection of human rights, such as the United Nations Guiding Principles on Business and Human Rights.
- (48) Given their special role and reach, it is appropriate to impose on very large online platforms and very large online search engines additional requirements regarding information and transparency of their terms and conditions. Consequently, providers of very large online platforms and very large online search engines should provide their terms and conditions in the official languages of all Member States in which they offer their services and should also provide recipients of the services with a concise and easily readable summary of the main elements of the terms and conditions. Such summaries should identify the main elements of the information requirements, including the possibility of easily opting out from optional clauses.

- (49) To ensure an adequate level of transparency and accountability, providers of intermediary services should make publicly available an annual report in a machine-readable format, in accordance with the harmonised requirements contained in this Regulation, on the content moderation in which they engage, including the measures taken as a result of the application and enforcement of their terms and conditions. However, in order to avoid disproportionate burdens, those transparency reporting obligations should not apply to providers that are micro or small enterprises as defined in Commission Recommendation 2003/361/EC <sup>(25)</sup> and which are not very large online platforms within the meaning of this Regulation.
- (50) Providers of hosting services play a particularly important role in tackling illegal content online, as they store information provided by and at the request of the recipients of the service and typically give other recipients access thereto, sometimes on a large scale. It is important that all providers of hosting services, regardless of their size, put in place easily accessible and user-friendly notice and action mechanisms that facilitate the notification of specific items of information that the notifying party considers to be illegal content to the provider of hosting services concerned ('notice'), pursuant to which that provider can decide whether or not it agrees with that assessment and wishes to remove or disable access to that content ('action'). Such mechanisms should be clearly identifiable, located close to the information in question and at least as easy to find and use as notification mechanisms for content that violates the terms and conditions of the hosting service provider. Provided the requirements on notices are met, it should be possible for individuals or entities to notify multiple specific items of allegedly illegal content through a single notice in order to ensure the effective operation of notice and action mechanisms. The notification mechanism should allow, but not require, the identification of the individual or the entity submitting a notice. For some types of items of information notified, the identity of the individual or the entity submitting a notice might be necessary to determine whether the information in question constitutes illegal content, as alleged. The obligation to put in place notice and action mechanisms should apply, for instance, to file storage and sharing services, web hosting services, advertising servers and paste bins, in so far as they qualify as hosting services covered by this Regulation.
- (51) Having regard to the need to take due account of the fundamental rights guaranteed under the Charter of all parties concerned, any action taken by a provider of hosting services pursuant to receiving a notice should be strictly targeted, in the sense that it should serve to remove or disable access to the specific items of information considered to constitute illegal content, without unduly affecting the freedom of expression and of information of recipients of the service. Notices should therefore, as a general rule, be directed to the providers of hosting services that can reasonably be expected to have the technical and operational ability to act against such specific items. The providers of hosting services who receive a notice for which they cannot, for technical or operational reasons, remove the specific item of information should inform the person or entity who submitted the notice.
- (52) The rules on such notice and action mechanisms should be harmonised at Union level, so as to provide for the timely, diligent and non-arbitrary processing of notices on the basis of rules that are uniform, transparent and clear and that provide for robust safeguards to protect the right and legitimate interests of all affected parties, in particular their fundamental rights guaranteed by the Charter, irrespective of the Member State in which those parties are established or reside and of the field of law at issue. Those fundamental rights include but are not limited to: for the recipients of the service, the right to freedom of expression and of information, the right to respect for private and family life, the right to protection of personal data, the right to non-discrimination and the right to an effective remedy; for the service providers, the freedom to conduct a business, including the freedom of contract; for parties affected by illegal content, the right to human dignity, the rights of the child, the right to protection of property, including intellectual property, and the right to non-discrimination. Providers of hosting services should act upon notices in a timely manner, in particular by taking into account the type of illegal content being notified and the urgency of taking action. For instance, such providers can be expected to act without delay when allegedly illegal content involving a threat to life or safety of persons is being notified. The provider of hosting services should inform the individual or entity notifying the specific content without undue delay after taking a decision whether or not to act upon the notice.

---

<sup>(25)</sup> Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

- (53) The notice and action mechanisms should allow for the submission of notices which are sufficiently precise and adequately substantiated to enable the provider of hosting services concerned to take an informed and diligent decision, compatible with the freedom of expression and of information, 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 to be removed or access thereto is to be disabled. Those mechanisms should be such as to facilitate the provision of notices that contain an explanation of the reasons why the individual or the entity submitting a notice considers that content to be illegal content, and a clear indication of the location of that content. Where a notice contains sufficient information to enable a diligent provider of hosting services to identify, without a detailed legal examination, that it is clear that the content is illegal, the notice should be considered to give rise to actual knowledge or awareness of illegality. Except for the submission of notices relating to offences referred to in Articles 3 to 7 of Directive 2011/93/EU of the European Parliament and of the Council <sup>(26)</sup>, those mechanisms should ask the individual or the entity submitting a notice to disclose its identity in order to avoid misuse.
- (54) Where a provider of hosting services decides, on the ground that the information provided by the recipients is illegal content or is incompatible with its terms and conditions, to remove or disable access to information provided by a recipient of the service or to otherwise restrict its visibility or monetisation, for instance following receipt of a notice or acting on its own initiative, including exclusively by automated means, that provider should inform in a clear and easily comprehensible way the recipient of its decision, the reasons for its decision and the available possibilities for redress to contest the decision, in view of the negative consequences that such decisions may have for the recipient, including as regards the exercise of its fundamental right to freedom of expression. That obligation should apply irrespective of the reasons for the decision, in particular whether the action has been taken because the information notified is considered to be illegal content or incompatible with the applicable terms and conditions. Where the decision was taken following receipt of a notice, the provider of hosting services should only reveal the identity of the person or entity who submitted the notice to the recipient of the service where this information is necessary to identify the illegality of the content, such as in cases of infringements of intellectual property rights.
- (55) Restriction of visibility may consist in demotion in ranking or in recommender systems, as well as in limiting accessibility by one or more recipients of the service or blocking the user from an online community without the user being aware ('shadow banning'). The monetisation via advertising revenue of information provided by the recipient of the service can be restricted by suspending or terminating the monetary payment or revenue associated to that information. The obligation to provide a statement of reasons should however not apply with respect to deceptive high-volume commercial content disseminated through intentional manipulation of the service, in particular inauthentic use of the service such as the use of bots or fake accounts or other deceptive uses of the service. Irrespective of other possibilities to challenge the decision of the provider of hosting services, the recipient of the service should always have a right to effective remedy before a court in accordance with the national law.
- (56) A provider of hosting services may in some instances become aware, such as through a notice by a notifying party or through its own voluntary measures, of information relating to certain activity of a recipient of the service, such as the provision of certain types of illegal content, that reasonably justify, having regard to all relevant circumstances of which the provider of hosting services is aware, the suspicion that that recipient may have committed, may be committing or is likely to commit a criminal offence involving a threat to the life or safety of person or persons, such as offences specified in Directive 2011/36/EU of the European Parliament and of the Council <sup>(27)</sup>, Directive 2011/93/EU or Directive (EU) 2017/541 of the European Parliament and of the Council <sup>(28)</sup>. For example, specific items of content could give rise to a suspicion of a threat to the public, such as incitement to terrorism within the meaning of Article 21 of Directive (EU) 2017/541. In such instances, the provider of hosting services

<sup>(26)</sup> Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).

<sup>(27)</sup> Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA (OJ L 101, 15.4.2011, p. 1).

<sup>(28)</sup> Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).

should inform without delay the competent law enforcement authorities of such suspicion. The provider of hosting services should provide all relevant information available to it, including, where relevant, the content in question and, if available, the time when the content was published, including the designated time zone, an explanation of its suspicion and the information necessary to locate and identify the relevant recipient of the service. This Regulation does not provide the legal basis for profiling of recipients of the services with a view to the possible identification of criminal offences by providers of hosting services. Providers of hosting services should also respect other applicable rules of Union or national law for the protection of the rights and freedoms of individuals when informing law enforcement authorities.

- (57) To avoid disproportionate burdens, the additional obligations imposed under this Regulation on providers of online platforms, including platforms allowing consumers to conclude distance contracts with traders, should not apply to providers that qualify as micro or small enterprises as defined in Recommendation 2003/361/EC. For the same reason, those additional obligations should also not apply to providers of online platforms that previously qualified as micro or small enterprises during a period of 12 months after they lose that status. Such providers should not be excluded from the obligation to provide information on the average monthly active recipients of the service at the request of the Digital Services Coordinator of establishment or the Commission. However, considering that very large online platforms or very large online search engines have a larger reach and a greater impact in influencing how recipients of the service obtain information and communicate online, such providers should not benefit from that exclusion, irrespective of whether they qualify or recently qualified as micro or small enterprises. The consolidation rules laid down in Recommendation 2003/361/EC help ensure that any circumvention of those additional obligations is prevented. Nothing in this Regulation precludes providers of online platforms that are covered by that exclusion from setting up, on a voluntary basis, a system that complies with one or more of those obligations.
- (58) Recipients of the service should be able to easily and effectively contest certain decisions of providers of online platforms concerning the illegality of content or its incompatibility with the terms and conditions that negatively affect them. Therefore, providers of online platforms should be required to provide for internal complaint-handling systems, which meet certain conditions that aim to ensure that the systems are easily accessible and lead to swift, non-discriminatory, non-arbitrary and fair outcomes, and are subject to human review where automated means are used. Such systems should enable all recipients of the service to lodge a complaint and should not set formal requirements, such as referral to specific, relevant legal provisions or elaborate legal explanations. Recipients of the service who submitted a notice through the notice and action mechanism provided for in this Regulation or through the notification mechanism for content that violate the terms and conditions of the provider of online platforms should be entitled to use the complaint mechanism to contest the decision of the provider of online platforms on their notices, including when they consider that the action taken by that provider was not adequate. The possibility to lodge a complaint for the reversal of the contested decisions should be available for at least six months, to be calculated from the moment at which the provider of online platforms informed the recipient of the service of the decision.
- (59) In addition, provision should be made for the possibility of engaging, in good faith, in the out-of-court dispute settlement of such disputes, including those that could not be resolved in a satisfactory manner through the internal complaint-handling systems, by certified bodies that have the requisite independence, means and expertise to carry out their activities in a fair, swift and cost-effective manner. The independence of the out-of-court dispute settlement bodies should be ensured also at the level of the natural persons in charge of resolving disputes, including through rules on conflict of interest. The fees charged by the out-of-court dispute settlement bodies should be reasonable, accessible, attractive, inexpensive for consumers and proportionate, and assessed on a case-by-case basis. Where an out-of-court dispute settlement body is certified by the competent Digital Services Coordinator, that certification should be valid in all Member States. Providers of online platforms should be able to refuse to engage in out-of-court dispute settlement procedures under this Regulation when the same dispute, in particular as regards the information concerned and the grounds for taking the contested decision, the effects of the decision and the grounds raised for contesting the decision, has already been resolved by or is already subject to an

ongoing procedure before the competent court or before another competent out-of-court dispute settlement body. Recipients of the service should be able to choose between the internal complaint mechanism, an out-of-court dispute settlement and the possibility to initiate, at any stage, judicial proceedings. Since the outcome of the out-of-court dispute settlement procedure is not binding, the parties should not be prevented from initiating judicial proceedings in relation to the same dispute. The possibilities to contest decisions of providers of online platforms thus created should leave unaffected in all respects the possibility to seek judicial redress in accordance with the laws of the Member State concerned, and therefore should not affect the exercise of the right to an effective judicial remedy under Article 47 of the Charter. The provisions in this Regulation on out-of-court dispute settlement should not require Member States to establish such out-of-court settlement bodies.

- (60) For contractual consumer-to-business disputes regarding the purchase of goods or services, Directive 2013/11/EU ensures that Union consumers and businesses in the Union have access to quality-certified alternative dispute resolution entities. In this regard, it should be clarified that the rules of this Regulation on out-of-court dispute settlement are without prejudice to that Directive, including the right of consumers under that Directive to withdraw from the procedure at any stage if they are dissatisfied with the performance or the operation of the procedure.
- (61) Action against illegal content can be taken more quickly and reliably where providers of online platforms take the necessary measures to ensure that notices submitted by trusted flaggers, acting within their designated area of expertise, through the notice and action mechanisms required by this Regulation are treated with priority, without prejudice to the requirement to process and decide upon all notices submitted under those mechanisms in a timely, diligent and non-arbitrary manner. Such trusted flagger status should be awarded by the Digital Services Coordinator of the Member State in which the applicant is established and should be recognised by all providers of online platforms within the scope of this Regulation. Such trusted flagger status should only be awarded to entities, and not individuals, that have demonstrated, among other things, that they have particular expertise and competence in tackling illegal content and that they work in a diligent, accurate and objective manner. Such entities can be public in nature, such as, for terrorist content, internet referral units of national law enforcement authorities or of the European Union Agency for Law Enforcement Cooperation ('Europol') or they can be non-governmental organisations and private or semi-public bodies such as the organisations part of the INHOPE network of hotlines for reporting child sexual abuse material and organisations committed to notifying illegal racist and xenophobic expressions online. To avoid diminishing the added value of such mechanism, the overall number of trusted flaggers awarded in accordance with this Regulation should be limited. In particular, industry associations representing their members' interests are encouraged to apply for the status of trusted flaggers, without prejudice to the right of private entities or individuals to enter into bilateral agreements with the providers of online platforms.
- (62) Trusted flaggers should publish easily comprehensible and detailed reports on notices submitted in accordance with this Regulation. Those reports should indicate information such as the number of notices categorised by the provider of hosting services, the type of content, and the action taken by the provider. Given that trusted flaggers have demonstrated expertise and competence, the processing of notices submitted by trusted flaggers can be expected to be less burdensome and therefore faster compared to notices submitted by other recipients of the service. However, the average time taken to process may still vary depending on factors including the type of illegal content, the quality of notices, and the actual technical procedures put in place for the submission of such notices.

For example, while the Code of conduct on countering illegal hate speech online of 2016 sets a benchmark for the participating companies with respect to the time needed to process valid notifications for removal of illegal hate speech, other types of illegal content may take considerably different timelines for processing, depending on the specific facts and circumstances and types of illegal content at stake. In order to avoid abuses of the trusted flagger status, it should be possible to suspend such status when a Digital Services Coordinator of establishment opened an investigation based on legitimate reasons. The rules of this Regulation on trusted flaggers should not be understood

to prevent providers of online platforms from giving similar treatment to notices submitted by entities or individuals that have not been awarded trusted flagger status under this Regulation, from otherwise cooperating with other entities, in accordance with the applicable law, including this Regulation and Regulation (EU) 2016/794 of the European Parliament and of the Council <sup>(29)</sup>. The rules of this Regulation should not prevent the providers of online platforms from making use of such trusted flagger or similar mechanisms to take quick and reliable action against content that is incompatible with their terms and conditions, in particular against content that is harmful for vulnerable recipients of the service, such as minors.

- (63) The misuse of online platforms by frequently providing manifestly illegal content or by frequently submitting manifestly unfounded notices or complaints under the mechanisms and systems, respectively, established under this Regulation undermines trust and harms the rights and legitimate interests of the parties concerned. Therefore, there is a need to put in place appropriate, proportionate and effective safeguards against such misuse, that need to respect the rights and legitimate interests of all parties involved, including the applicable fundamental rights and freedoms as enshrined in the Charter, in particular the freedom of expression. Information should be considered to be manifestly illegal content and notices or complaints should be considered manifestly unfounded where it is evident to a layperson, without any substantive analysis, that the content is illegal or, respectively, that the notices or complaints are unfounded.
- (64) Under certain conditions, providers of online platforms should temporarily suspend their relevant activities in respect of the person engaged in abusive behaviour. This is without prejudice to the freedom by providers of online platforms to determine their terms and conditions and establish stricter measures in the case of manifestly illegal content related to serious crimes, such as child sexual abuse material. For reasons of transparency, this possibility should be set out, clearly and in sufficient detail, in the terms and conditions of the online platforms. Redress should always be open to the decisions taken in this regard by providers of online platforms and they should be subject to oversight by the competent Digital Services Coordinator. Providers of online platforms should send a prior warning before deciding on the suspension, which should include the reasons for the possible suspension and the means of redress against the decision of the providers of the online platform. When deciding on the suspension, providers of online platforms should send the statement of reasons in accordance with the rules set out in this Regulation. The rules of this Regulation on misuse should not prevent providers of online platforms from taking other measures to address the provision of illegal content by recipients of their service or other misuse of their services, including through the violation of their terms and conditions, in accordance with the applicable Union and national law. Those rules are without prejudice to any possibility to hold the persons engaged in misuse liable, including for damages, provided for in Union or national law.
- (65) In view of the particular responsibilities and obligations of providers of online platforms, they should be made subject to transparency reporting obligations, which apply in addition to the transparency reporting obligations applicable to all providers of intermediary services under this Regulation. For the purposes of determining whether online platforms and online search engines may be very large online platforms or very large online search engines, respectively, that are subject to certain additional obligations under this Regulation, the transparency reporting obligations for online platforms and online search engines should include certain obligations relating to the publication and communication of information on the average monthly active recipients of the service in the Union.
- (66) In order to ensure transparency and to enable scrutiny over the content moderation decisions of the providers of online platforms and monitoring the spread of illegal content online, the Commission should maintain and publish a database which contains the decisions and statements of reasons of the providers of online platforms when they remove or otherwise restrict availability of and access to information. In order to keep the database continuously

<sup>(29)</sup> Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

updated, the providers of online platforms should submit, in a standard format, the decisions and statement of reasons without undue delay after taking a decision, to allow for real-time updates where technically possible and proportionate to the means of the online platform in question. The structured database should allow access to, and queries for, the relevant information, in particular as regards the type of alleged illegal content at stake.

- (67) Dark patterns on online interfaces of online platforms are practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions. Those practices can be used to persuade the recipients of the service to engage in unwanted behaviours or into undesired decisions which have negative consequences for them. Providers of online platforms should therefore be prohibited from deceiving or nudging recipients of the service and from distorting or impairing the autonomy, decision-making, or choice of the recipients of the service via the structure, design or functionalities of an online interface or a part thereof. This should include, but not be limited to, exploitative design choices to direct the recipient to actions that benefit the provider of online platforms, but which may not be in the recipients' interests, presenting choices in a non-neutral manner, such as giving more prominence to certain choices through visual, auditory, or other components, when asking the recipient of the service for a decision.

It should also include repeatedly requesting a recipient of the service to make a choice where such a choice has already been made, making the procedure of cancelling a service significantly more cumbersome than signing up to it, or making certain choices more difficult or time-consuming than others, making it unreasonably difficult to discontinue purchases or to sign out from a given online platform allowing consumers to conclude distance contracts with traders, and deceiving the recipients of the service by nudging them into decisions on transactions, or by default settings that are very difficult to change, and so unreasonably bias the decision making of the recipient of the service, in a way that distorts and impairs their autonomy, decision-making and choice. However, rules preventing dark patterns should not be understood as preventing providers to interact directly with recipients of the service and to offer new or additional services to them. Legitimate practices, for example in advertising, that are in compliance with Union law should not in themselves be regarded as constituting dark patterns. Those rules on dark patterns should be interpreted as covering prohibited practices falling within the scope of this Regulation to the extent that those practices are not already covered under Directive 2005/29/EC or Regulation (EU) 2016/679.

- (68) Online advertising plays an important role in the online environment, including in relation to the provision of online platforms, where the provision of the service is sometimes in whole or in part remunerated directly or indirectly, through advertising revenues. Online advertising can contribute to significant risks, ranging from advertisements that are themselves illegal content, to contributing to financial incentives for the publication or amplification of illegal or otherwise harmful content and activities online, or the discriminatory presentation of advertisements with an impact on the equal treatment and opportunities of citizens. In addition to the requirements resulting from Article 6 of Directive 2000/31/EC, providers of online platforms should therefore be required to ensure that the recipients of the service have certain individualised information necessary for them to understand when and on whose behalf the advertisement is presented. They should ensure that the information is salient, including through standardised visual or audio marks, clearly identifiable and unambiguous for the average recipient of the service, and should be adapted to the nature of the individual service's online interface. In addition, recipients of the service should have information directly accessible from the online interface where the advertisement is presented, on the main parameters used for determining that a specific advertisement is presented to them, providing meaningful explanations of the logic used to that end, including when this is based on profiling.

Such explanations should include information on the method used for presenting the advertisement, for example whether it is contextual or other type of advertising, and, where applicable, the main profiling criteria used; it should also inform the recipient about any means available for them to change such criteria. The requirements of this Regulation on the provision of information relating to advertising is without prejudice to the application of the relevant provisions of Regulation (EU) 2016/679, in particular those regarding the right to object, automated individual decision-making, including profiling, and specifically the need to obtain consent of the data subject prior to the processing of personal data for targeted advertising. Similarly, it is without prejudice to the provisions laid

down in Directive 2002/58/EC in particular those regarding the storage of information in terminal equipment and the access to information stored therein. Finally, this Regulation complements the application of the Directive 2010/13/EU which imposes measures to enable users to declare audiovisual commercial communications in user-generated videos. It also complements the obligations for traders regarding the disclosure of commercial communications deriving from Directive 2005/29/EC.

- (69) When recipients of the service are presented with advertisements based on targeting techniques optimised to match their interests and potentially appeal to their vulnerabilities, this can have particularly serious negative effects. In certain cases, manipulative techniques can negatively impact entire groups and amplify societal harms, for example by contributing to disinformation campaigns or by discriminating against certain groups. Online platforms are particularly sensitive environments for such practices and they present a higher societal risk. Consequently, providers of online platforms should not present advertisements based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679, using special categories of personal data referred to in Article 9(1) of that Regulation, including by using profiling categories based on those special categories. This prohibition is without prejudice to the obligations applicable to providers of online platforms or any other service provider or advertiser involved in the dissemination of the advertisements under Union law on protection of personal data.
- (70) A core part of the online platform's business is the manner in which information is prioritised and presented on its online interface to facilitate and optimise access to information for the recipients of the service. This is done, for example, by algorithmically suggesting, ranking and prioritising information, distinguishing through text or other visual representations, or otherwise curating information provided by recipients. Such recommender systems can have a significant impact on the ability of recipients to retrieve and interact with information online, including to facilitate the search of relevant information for recipients of the service and contribute to an improved user experience. They also play an important role in the amplification of certain messages, the viral dissemination of information and the stimulation of online behaviour. Consequently, online platforms should consistently ensure that recipients of their service are appropriately informed about how recommender systems impact the way information is displayed, and can influence how information is presented to them. They should clearly present the parameters for such recommender systems in an easily comprehensible manner to ensure that the recipients of the service understand how information is prioritised for them. Those parameters should include at least the most important criteria in determining the information suggested to the recipient of the service and the reasons for their respective importance, including where information is prioritised based on profiling and their online behaviour.
- (71) The protection of minors is an important policy objective of the Union. An online platform can be considered to be accessible to minors when its terms and conditions permit minors to use the service, when its service is directed at or predominantly used by minors, or where the provider is otherwise aware that some of the recipients of its service are minors, for example because it already processes personal data of the recipients of its service revealing their age for other purposes. Providers of online platforms used by minors should take appropriate and proportionate measures to protect minors, for example by designing their online interfaces or parts thereof with the highest level of privacy, safety and security for minors by default where appropriate or adopting standards for protection of minors, or participating in codes of conduct for protecting minors. They should consider best practices and available guidance, such as that provided by the communication of the Commission on A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+). Providers of online platforms should not present advertisements based on profiling using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor. In accordance with Regulation (EU) 2016/679, notably the principle of data minimisation as provided for in Article 5(1), point (c), thereof, this prohibition should not lead the provider of the online platform to maintain, acquire or process more personal data than it already has in order to assess if the recipient of the service is a minor. Thus, this obligation should not incentivize providers of online platforms to collect the age of the recipient of the service prior to their use. It should be without prejudice to Union law on protection of personal data.

- (72) In order to contribute to a safe, trustworthy and transparent online environment for consumers, as well as for other interested parties such as competing traders and holders of intellectual property rights, and to deter traders from selling products or services in violation of the applicable rules, online platforms allowing consumers to conclude distance contracts with traders should ensure that such traders are traceable. The trader should therefore be required to provide certain essential information to the providers of online platforms allowing consumers to conclude distance contracts with traders, including for purposes of promoting messages on or offering products. That requirement should also be applicable to traders that promote messages on products or services on behalf of brands, based on underlying agreements. Those providers of online platforms should store all information in a secure manner for the duration of their contractual relationship with the trader and 6 months thereafter, to allow any claims to be filed against the trader or orders related to the trader to be complied with.

This obligation is necessary and proportionate, so that the information can be accessed, in accordance with the applicable law, including on the protection of personal data, by public authorities and private parties with a legitimate interest, including through the orders to provide information referred to in this Regulation. This obligation leaves unaffected potential obligations to preserve certain content for longer periods of time, on the basis of other Union law or national laws, in compliance with Union law. Without prejudice to the definition provided for in this Regulation, any trader, irrespective of whether it is a natural or legal person, identified on the basis of Article 6a(1), point (b), of Directive 2011/83/EU and Article 7(4), point (f), of Directive 2005/29/EC should be traceable when offering a product or service through an online platform. Directive 2000/31/EC obliges all information society services providers to render easily, directly and permanently accessible to the recipients of the service and competent authorities certain information allowing the identification of all providers. The traceability requirements for providers of online platforms allowing consumers to conclude distance contracts with traders set out in this Regulation do not affect the application of Council Directive (EU) 2021/514<sup>(30)</sup>, which pursues other legitimate public interest objectives.

- (73) To ensure an efficient and adequate application of that obligation, without imposing any disproportionate burdens, providers of online platforms allowing consumers to conclude distance contracts with traders should make best efforts to assess the reliability of the information provided by the traders concerned, in particular by using freely available official online databases and online interfaces, such as national trade registers and the VAT Information Exchange System, or request the traders concerned to provide trustworthy supporting documents, such as copies of identity documents, certified payment accounts' statements, company certificates and trade register certificates. They may also use other sources, available for use at a distance, which offer a similar degree of reliability for the purpose of complying with this obligation. However, the providers of online platforms concerned should not be required to engage in excessive or costly online fact-finding exercises or to carry out disproportionate verifications on the spot. Nor should such providers, which have made the best efforts required by this Regulation, be understood as guaranteeing the reliability of the information towards consumer or other interested parties.

- (74) Providers of online platforms allowing consumers to conclude distance contracts with traders should design and organise their online interface in a way that enables traders to comply with their obligations under relevant Union law, in particular the requirements set out in Articles 6 and 8 of Directive 2011/83/EU, Article 7 of Directive 2005/29/EC, Articles 5 and 6 of Directive 2000/31/EC and Article 3 of Directive 98/6/EC of the European Parliament and of the Council<sup>(31)</sup>. For that purpose, the providers of online platforms concerned should make best efforts to assess whether the traders using their services have uploaded complete information on their online interfaces, in line with relevant applicable Union law. The providers of online platforms should ensure that products or services are not offered as long as such information is not complete. This should not amount to an obligation for the providers of online platforms concerned to generally monitor the products or services offered by traders through their services nor a general fact-finding obligation, in particular to assess the accuracy of the information provided by traders. The

<sup>(30)</sup> Council Directive (EU) 2021/514 of 22 March 2021 amending Directive 2011/16/EU on administrative cooperation in the field of taxation (OJ L 104, 25.3.2021, p. 1).

<sup>(31)</sup> Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers (OJ L 80, 18.3.1998, p. 27).

online interfaces should be user-friendly and easily accessible for traders and consumers. Additionally and after allowing the offering of the product or service by the trader, the providers of online platforms concerned should make reasonable efforts to randomly check whether the products or services offered have been identified as being illegal in any official, freely accessible and machine-readable online databases or online interfaces available in a Member State or in the Union. The Commission should also encourage traceability of products through technology solutions such as digitally signed Quick Response codes (or 'QR codes') or non-fungible tokens. The Commission should promote the development of standards and, in the absence of them, of market led solutions which can be acceptable to the parties concerned.

- (75) Given the importance of very large online platforms, due to their reach, in particular as expressed in the number of recipients of the service, in facilitating public debate, economic transactions and the dissemination to the public of information, opinions and ideas and in influencing how recipients obtain and communicate information online, it is necessary to impose specific obligations on the providers of those platforms, in addition to the obligations applicable to all online platforms. Due to their critical role in locating and making information retrievable online, it is also necessary to impose those obligations, to the extent they are applicable, on the providers of very large online search engines. Those additional obligations on providers of very large online platforms and of very large online search engines are necessary to address those public policy concerns, there being no alternative and less restrictive measures that would effectively achieve the same result.
- (76) Very large online platforms and very large online search engines may cause societal risks, different in scope and impact from those caused by smaller platforms. Providers of such very large online platforms and of very large online search engines should therefore bear the highest standard of due diligence obligations, proportionate to their societal impact. Once the number of active recipients of an online platform or of active recipients of an online search engine, calculated as an average over a period of six months, reaches a significant share of the Union population, the systemic risks the online platform or online search engine poses may have a disproportionate impact in the Union. Such significant reach should be considered to exist where such number exceeds an operational threshold set at 45 million, that is, a number equivalent to 10 % of the Union population. This operational threshold should be kept up to date and therefore the Commission should be empowered to supplement the provisions of this Regulation by adopting delegated acts, where necessary.
- (77) In order to determine the reach of a given online platform or online search engine, it is necessary to establish the average number of active recipients of each service individually. Accordingly, the number of average monthly active recipients of an online platform should reflect all the recipients actually engaging with the service at least once in a given period of time, by being exposed to information disseminated on the online interface of the online platform, such as viewing it or listening to it, or by providing information, such as traders on an online platforms allowing consumers to conclude distance contracts with traders.

For the purposes of this Regulation, engagement is not limited to interacting with information by clicking on, commenting, linking, sharing, purchasing or carrying out transactions on an online platform. Consequently, the concept of active recipient of the service does not necessarily coincide with that of a registered user of a service. As regards online search engines, the concept of active recipients of the service should cover those who view information on their online interface, but not, for example, the owners of the websites indexed by an online search engine, as they do not actively engage with the service. The number of active recipients of a service should include all unique recipients of the service that engage with the specific service. To this effect, a recipient of the service that uses different online interfaces, such as websites or applications, including where the services are accessed through different uniform resource locators (URLs) or domain names, should, where possible, be counted only once. However, the concept of active recipient of the service should not include incidental use of the service by recipients of other providers of intermediary services that indirectly make available information hosted by the provider of online platforms through linking or indexing by a provider of online search engine. Further, this Regulation does not require providers of online platforms or of online search engines to perform specific tracking of individuals

online. Where such providers are able to discount automated users such as bots or scrapers without further processing of personal data and tracking, they may do so. The determination of the number of active recipients of the service can be impacted by market and technical developments and therefore the Commission should be empowered to supplement the provisions of this Regulation by adopting delegated acts laying down the methodology to determine the active recipients of an online platform or of an online search engine, where necessary, reflecting the nature of the service and the way recipients of the service interact with it.

- (78) In view of the network effects characterising the platform economy, the user base of an online platform or an online search engine may quickly expand and reach the dimension of a very large online platform or a very large online search engine, with the related impact on the internal market. This may be the case in the event of exponential growth experienced in short periods of time, or by a large global presence and turnover allowing the online platform or the online search engine to fully exploit network effects and economies of scale and of scope. A high annual turnover or market capitalisation can in particular be an indication of fast scalability in terms of user reach. In those cases, the Digital Services Coordinator of establishment or the Commission should be able to request more frequent reporting from the provider of the online platform or of the online search engine on the number of active recipients of the service to be able to timely identify the moment at which that platform or that search engine should be designated as a very large online platform or very large online search engine, respectively, for the purposes of this Regulation.
- (79) Very large online platforms and very large online search engines can be used in a way that strongly influences safety online, the shaping of public opinion and discourse, as well as online trade. The way they design their services is generally optimised to benefit their often advertising-driven business models and can cause societal concerns. Effective regulation and enforcement is necessary in order to effectively identify and mitigate the risks and the societal and economic harm that may arise. Under this Regulation, providers of very large online platforms and of very large online search engines should therefore assess the systemic risks stemming from the design, functioning and use of their services, as well as from potential misuses by the recipients of the service, and should take appropriate mitigating measures in observance of fundamental rights. In determining the significance of potential negative effects and impacts, providers should consider the severity of the potential impact and the probability of all such systemic risks. For example, they could assess whether the potential negative impact can affect a large number of persons, its potential irreversibility, or how difficult it is to remedy and restore the situation prevailing prior to the potential impact.
- (80) Four categories of systemic risks should be assessed in-depth by the providers of very large online platforms and of very large online search engines. A first category concerns the risks associated with the dissemination of illegal content, such as the dissemination of child sexual abuse material or illegal hate speech or other types of misuse of their services for criminal offences, and the conduct of illegal activities, such as the sale of products or services prohibited by Union or national law, including dangerous or counterfeit products, or illegally-traded animals. For example, such dissemination or activities may constitute a significant systemic risk where access to illegal content may spread rapidly and widely through accounts with a particularly wide reach or other means of amplification. Providers of very large online platforms and of very large online search engines should assess the risk of dissemination of illegal content irrespective of whether or not the information is also incompatible with their terms and conditions. This assessment is without prejudice to the personal responsibility of the recipient of the service of very large online platforms or of the owners of websites indexed by very large online search engines for possible illegality of their activity under the applicable law.
- (81) A second category concerns the actual or foreseeable impact of the service on the exercise of fundamental rights, as protected by the Charter, including but not limited to human dignity, freedom of expression and of information, including media freedom and pluralism, the right to private life, data protection, the right to non-discrimination, the rights of the child and consumer protection. Such risks may arise, for example, in relation to the design of the algorithmic systems used by the very large online platform or by the very large online search engine or the misuse

of their service through the submission of abusive notices or other methods for silencing speech or hampering competition. When assessing risks to the rights of the child, providers of very large online platforms and of very large online search engines should consider for example how easy it is for minors to understand the design and functioning of the service, as well as how minors can be exposed through their service to content that may impair minors' health, physical, mental and moral development. Such risks may arise, for example, in relation to the design of online interfaces which intentionally or unintentionally exploit the weaknesses and inexperience of minors or which may cause addictive behaviour.

- (82) A third category of risks concerns the actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, as well as public security.
- (83) A fourth category of risks stems from similar concerns relating to the design, functioning or use, including through manipulation, of very large online platforms and of very large online search engines with an actual or foreseeable negative effect on the protection of public health, minors and serious negative consequences to a person's physical and mental well-being, or on gender-based violence. Such risks may also stem from coordinated disinformation campaigns related to public health, or from online interface design that may stimulate behavioural addictions of recipients of the service.
- (84) When assessing such systemic risks, providers of very large online platforms and of very large online search engines should focus on the systems or other elements that may contribute to the risks, including all the algorithmic systems that may be relevant, in particular their recommender systems and advertising systems, paying attention to the related data collection and use practices. They should also assess whether their terms and conditions and the enforcement thereof are appropriate, as well as their content moderation processes, technical tools and allocated resources. When assessing the systemic risks identified in this Regulation, those providers should also focus on the information which is not illegal, but contributes to the systemic risks identified in this Regulation. Such providers should therefore pay particular attention on how their services are used to disseminate or amplify misleading or deceptive content, including disinformation. Where the algorithmic amplification of information contributes to the systemic risks, those providers should duly reflect this in their risk assessments. Where risks are localised or there are linguistic differences, those providers should also account for this in their risk assessments. Providers of very large online platforms and of very large online search engines should, in particular, assess how the design and functioning of their service, as well as the intentional and, oftentimes, coordinated manipulation and use of their services, or the systemic infringement of their terms of service, contribute to such risks. Such risks may arise, for example, through the inauthentic use of the service, such as the creation of fake accounts, the use of bots or deceptive use of a service, and other automated or partially automated behaviours, which may lead to the rapid and widespread dissemination to the public of information that is illegal content or incompatible with an online platform's or online search engine's terms and conditions and that contributes to disinformation campaigns.
- (85) In order to make it possible that subsequent risk assessments build on each other and show the evolution of the risks identified, as well as to facilitate investigations and enforcement actions, providers of very large online platforms and of very large online search engines should preserve all supporting documents relating to the risk assessments that they carried out, such as information regarding the preparation thereof, underlying data and data on the testing of their algorithmic systems.
- (86) Providers of very large online platforms and of very large online search engines should deploy the necessary means to diligently mitigate the systemic risks identified in the risk assessments, in observance of fundamental rights. Any measures adopted should respect the due diligence requirements of this Regulation and be reasonable and effective in mitigating the specific systemic risks identified. They should be proportionate in light of the economic capacity of the provider of the very large online platform or of the very large online search engine and the need to avoid unnecessary restrictions on the use of their service, taking due account of potential negative effects on those fundamental rights. Those providers should give particular consideration to the impact on freedom of expression.

- (87) Providers of very large online platforms and of very large online search engines should consider under such mitigating measures, for example, adapting any necessary design, feature or functioning of their service, such as the online interface design. They should adapt and apply their terms and conditions, as necessary, and in accordance with the rules of this Regulation on terms and conditions. Other appropriate measures could include adapting their content moderation systems and internal processes or adapting their decision-making processes and resources, including the content moderation personnel, their training and local expertise. This concerns in particular the speed and quality of processing of notices. In this regard, for example, the Code of conduct on countering illegal hate speech online of 2016 sets a benchmark to process valid notifications for removal of illegal hate speech in less than 24 hours. Providers of very large online platforms, in particular those primarily used for the dissemination to the public of pornographic content, should diligently meet all their obligations under this Regulation in respect of illegal content constituting cyber violence, including illegal pornographic content, especially with regard to ensuring that victims can effectively exercise their rights in relation to content representing non-consensual sharing of intimate or manipulated material through the rapid processing of notices and removal of such content without undue delay. Other types of illegal content may require longer or shorter timelines for processing of notices, which will depend on the facts, circumstances and types of illegal content at hand. Those providers may also initiate or increase cooperation with trusted flaggers and organise training sessions and exchanges with trusted flagger organisations.
- (88) Providers of very large online platforms and of very large online search engines should also be diligent in the measures they take to test and, where necessary, adapt their algorithmic systems, not least their recommender systems. They may need to mitigate the negative effects of personalised recommendations and correct the criteria used in their recommendations. The advertising systems used by providers of very large online platforms and of very large online search engines can also be a catalyser for the systemic risks. Those providers should consider corrective measures, such as discontinuing advertising revenue for specific information, or other actions, such as improving the visibility of authoritative information sources, or more structurally adapting their advertising systems. Providers of very large online platforms and of very large online search engines may need to reinforce their internal processes or supervision of any of their activities, in particular as regards the detection of systemic risks, and conduct more frequent or targeted risk assessments related to new functionalities. In particular, where risks are shared across different online platforms or online search engines, they should cooperate with other service providers, including by initiating or joining existing codes of conduct or other self-regulatory measures. They should also consider awareness-raising actions, in particular where risks relate to disinformation campaigns.
- (89) Providers of very large online platforms and of very large online search engines should take into account the best interests of minors in taking measures such as adapting the design of their service and their online interface, especially when their services are aimed at minors or predominantly used by them. They should ensure that their services are organised in a way that allows minors to access easily mechanisms provided for in this Regulation, where applicable, including notice and action and complaint mechanisms. They should also take measures to protect minors from content that may impair their physical, mental or moral development and provide tools that enable conditional access to such information. In selecting the appropriate mitigation measures, providers can consider, where appropriate, industry best practices, including as established through self-regulatory cooperation, such as codes of conduct, and should take into account the guidelines from the Commission.
- (90) Providers of very large online platforms and of very large online search engines should ensure that their approach to risk assessment and mitigation is based on the best available information and scientific insights and that they test their assumptions with the groups most impacted by the risks and the measures they take. To this end, they should, where appropriate, conduct their risk assessments and design their risk mitigation measures with the involvement of representatives of the recipients of the service, representatives of groups potentially impacted by their services,

independent experts and civil society organisations. They should seek to embed such consultations into their methodologies for assessing the risks and designing mitigation measures, including, as appropriate, surveys, focus groups, round tables, and other consultation and design methods. In the assessment on whether a measure is reasonable, proportionate and effective, special consideration should be given to the right to freedom of expression.

- (91) In times of crisis, there might be a need for certain specific measures to be taken urgently by providers of very large online platforms, in addition to measures they would be taking in view of their other obligations under this Regulation. In that regard, a crisis should be considered to occur when extraordinary circumstances occur that can lead to a serious threat to public security or public health in the Union or significant parts thereof. Such crises could result from armed conflicts or acts of terrorism, including emerging conflicts or acts of terrorism, natural disasters such as earthquakes and hurricanes, as well as from pandemics and other serious cross-border threats to public health. The Commission should be able to require, upon recommendation by the European Board for Digital Services ('the Board'), providers of very large online platforms and providers of very large search engines to initiate a crisis response as a matter of urgency. Measures that those providers may identify and consider applying may include, for example, adapting content moderation processes and increasing the resources dedicated to content moderation, adapting terms and conditions, relevant algorithmic systems and advertising systems, further intensifying cooperation with trusted flaggers, taking awareness-raising measures and promoting trusted information and adapting the design of their online interfaces. The necessary requirements should be provided for to ensure that such measures are taken within a very short time frame and that the crisis response mechanism is only used where, and to the extent that, this is strictly necessary and any measures taken under this mechanism are effective and proportionate, taking due account of the rights and legitimate interests of all parties concerned. The use of the mechanism should be without prejudice to the other provisions of this Regulation, such as those on risk assessments and mitigation measures and the enforcement thereof and those on crisis protocols.
- (92) Given the need to ensure verification by independent experts, providers of very large online platforms and of very large online search engines should be accountable, through independent auditing, for their compliance with the obligations laid down by this Regulation and, where relevant, any complementary commitments undertaken pursuant to codes of conduct and crises protocols. In order to ensure that audits are carried out in an effective, efficient and timely manner, providers of very large online platforms and of very large online search engines should provide the necessary cooperation and assistance to the organisations carrying out the audits, including by giving the auditor access to all relevant data and premises necessary to perform the audit properly, including, where appropriate, to data related to algorithmic systems, and by answering oral or written questions. Auditors should also be able to make use of other sources of objective information, including studies by vetted researchers. Providers of very large online platforms and of very large online search engines should not undermine the performance of the audit. Audits should be performed according to best industry practices and high professional ethics and objectivity, with due regard, as appropriate, to auditing standards and codes of practice. Auditors should guarantee the confidentiality, security and integrity of the information, such as trade secrets, that they obtain when performing their tasks. This guarantee should not be a means to circumvent the applicability of audit obligations in this Regulation. Auditors should have the necessary expertise in the area of risk management and technical competence to audit algorithms. They should be independent, in order to be able to perform their tasks in an adequate and trustworthy manner. They should comply with core independence requirements for prohibited non-auditing services, firm rotation and non-contingent fees. If their independence and technical competence is not beyond doubt, they should resign or abstain from the audit engagement.
- (93) The audit report should be substantiated, in order to give a meaningful account of the activities undertaken and the conclusions reached. It should help inform, and where appropriate suggest improvements to the measures taken by the providers of the very large online platform and of the very large online search engine to comply with their obligations under this Regulation. The audit report should be transmitted to the Digital Services Coordinator of establishment, the Commission and the Board following the receipt of the audit report. Providers should also transmit upon completion without undue delay each of the reports on the risk assessment and the mitigation measures, as well as the audit implementation report of the provider of the very large online platform or of the very large online search engine showing how they have addressed the audit's recommendations. The audit report should

include an audit opinion based on the conclusions drawn from the audit evidence obtained. A 'positive opinion' should be given where all evidence shows that the provider of the very large online platform or of the very large online search engine complies with the obligations laid down by this Regulation or, where applicable, any commitments it has undertaken pursuant to a code of conduct or crisis protocol, in particular by identifying, evaluating and mitigating the systemic risks posed by its system and services. A 'positive opinion' should be accompanied by comments where the auditor wishes to include remarks that do not have a substantial effect on the outcome of the audit. A 'negative opinion' should be given where the auditor considers that the provider of the very large online platform or of the very large online search engine does not comply with this Regulation or the commitments undertaken. Where the audit opinion could not reach a conclusion for specific elements that fall within the scope of the audit, an explanation of reasons for the failure to reach such a conclusion should be included in the audit opinion. Where applicable, the report should include a description of specific elements that could not be audited, and an explanation of why these could not be audited.

- (94) The obligations on assessment and mitigation of risks should trigger, on a case-by-case basis, the need for providers of very large online platforms and of very large online search engines to assess and, where necessary, adjust the design of their recommender systems, for example by taking measures to prevent or minimise biases that lead to the discrimination of persons in vulnerable situations, in particular where such adjustment is in accordance with data protection law and when the information is personalised on the basis of special categories of personal data referred to in Article 9 of the Regulation (EU) 2016/679. In addition, and complementing the transparency obligations applicable to online platforms as regards their recommender systems, providers of very large online platforms and of very large online search engines should consistently ensure that recipients of their service enjoy alternative options which are not based on profiling, within the meaning of Regulation (EU) 2016/679, for the main parameters of their recommender systems. Such choices should be directly accessible from the online interface where the recommendations are presented.
- (95) Advertising systems used by very large online platforms and very large online search engines pose particular risks and require further public and regulatory supervision on account of their scale and ability to target and reach recipients of the service based on their behaviour within and outside that platform's or search engine's online interface. Very large online platforms or very large online search engines should ensure public access to repositories of advertisements presented on their online interfaces to facilitate supervision and research into emerging risks brought about by the distribution of advertising online, for example in relation to illegal advertisements or manipulative techniques and disinformation with a real and foreseeable negative impact on public health, public security, civil discourse, political participation and equality. Repositories should include the content of advertisements, including the name of the product, service or brand and the subject matter of the advertisement, and related data on the advertiser, and, if different, the natural or legal person who paid for the advertisement, and the delivery of the advertisement, in particular where targeted advertising is concerned. This information should include both information about targeting criteria and delivery criteria, in particular when advertisements are delivered to persons in vulnerable situations, such as minors.
- (96) In order to appropriately monitor and assess the compliance of very large online platforms and of very large online search engines with the obligations laid down by this Regulation, the Digital Services Coordinator of establishment or the Commission may require access to or reporting of specific data, including data related to algorithms. Such a requirement may include, for example, the data necessary to assess the risks and possible harms brought about by the very large online platform's or the very large online search engine's systems, data on the accuracy, functioning and testing of algorithmic systems for content moderation, recommender systems or advertising systems, including, where appropriate, training data and algorithms, or data on processes and outputs of content moderation or of internal complaint-handling systems within the meaning of this Regulation. Such data access requests should not

include requests to produce specific information about individual recipients of the service for the purpose of determining compliance of such recipients with other applicable Union or national law. Investigations by researchers on the evolution and severity of online systemic risks are particularly important for bridging information asymmetries and establishing a resilient system of risk mitigation, informing providers of online platforms, providers of online search engines, Digital Services Coordinators, other competent authorities, the Commission and the public.

- (97) This Regulation therefore provides a framework for compelling access to data from very large online platforms and very large online search engines to vetted researchers affiliated to a research organisation within the meaning of Article 2 of Directive (EU) 2019/790, which may include, for the purpose of this Regulation, civil society organisations that are conducting scientific research with the primary goal of supporting their public interest mission. All requests for access to data under that framework should be proportionate and appropriately protect the rights and legitimate interests, including the protection of personal data, trade secrets and other confidential information, of the very large online platform or of the very large online search engine and any other parties concerned, including the recipients of the service. However, to ensure that the objective of this Regulation is achieved, consideration of the commercial interests of providers should not lead to a refusal to provide access to data necessary for the specific research objective pursuant to a request under this Regulation. In this regard, whilst without prejudice to Directive (EU) 2016/943 of the European Parliament and of the Council <sup>(32)</sup>, providers should ensure appropriate access for researchers, including, where necessary, by taking technical protections such as through data vaults. Data access requests could cover, for example, the number of views or, where relevant, other types of access to content by recipients of the service prior to its removal by the providers of very large online platforms or of very large online search engines.
- (98) In addition, where data is publicly accessible, such providers should not prevent researchers meeting an appropriate subset of criteria from using this data for research purposes that contribute to the detection, identification and understanding of systemic risks. They should provide access to such researchers including, where technically possible, in real-time, to the publicly accessible data, for example on aggregated interactions with content from public pages, public groups, or public figures, including impression and engagement data such as the number of reactions, shares, comments from recipients of the service. Providers of very large online platforms or of very large online search engines should be encouraged to cooperate with researchers and provide broader access to data for monitoring societal concerns through voluntary efforts, including through commitments and procedures agreed under codes of conduct or crisis protocols. Those providers and researchers should pay particular attention to the protection of personal data, and ensure that any processing of personal data complies with Regulation (EU) 2016/679. Providers should anonymise or pseudonymise personal data except in those cases that would render impossible the research purpose pursued.
- (99) Given the complexity of the functioning of the systems deployed and the systemic risks they present to society, providers of very large online platforms and of very large online search engines should establish a compliance function, which should be independent from the operational functions of those providers. The head of the compliance function should report directly to the management of those providers, including for concerns of non-compliance with this Regulation. The compliance officers that are part of the compliance function should have the necessary qualifications, knowledge, experience and ability to operationalise measures and monitor the compliance with this Regulation within the organisation of the providers of very large online platform or of very large online search engine. Providers of very large online platforms and of very large online search engines should ensure that the compliance function is involved, properly and in a timely manner, in all issues which relate to this Regulation including in the risk assessment and mitigation strategy and specific measures, as well as assessing compliance, where applicable, with commitments made by those providers under the codes of conduct and crisis protocols they subscribe to.

---

<sup>(32)</sup> Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (OJ L 157, 15.6.2016, p. 1).

- (100) In view of the additional risks relating to their activities and their additional obligations under this Regulation, additional transparency requirements should apply specifically to very large online platforms and very large online search engines, notably to report comprehensively on the risk assessments performed and subsequent measures adopted as provided by this Regulation.
- (101) The Commission should be in possession of all the necessary resources, in terms of staffing, expertise, and financial means, for the performance of its tasks under this Regulation. In order to ensure the availability of the resources necessary for the adequate supervision at Union level under this Regulation, and considering that Member States should be entitled to charge providers established in their territory a supervisory fee to in respect of the supervisory and enforcement tasks exercised by their authorities, the Commission should charge a supervisory fee, the level of which should be established on an annual basis, on very large online platforms and very large online search engines. The overall amount of the annual supervisory fee charged should be established on the basis of the overall amount of the costs incurred by the Commission to exercise its supervisory tasks under this Regulation, as reasonably estimated beforehand. Such amount should include costs relating to the exercise of the specific powers and tasks of supervision, investigation, enforcement and monitoring in respect of providers of very large online platforms and of very large online search engines, including costs related to the designation of very large online platforms and of very large online search engines or to the set up, maintenance and operation of the databases envisaged under this Regulation.

It should also include costs relating to the set-up, maintenance and operation of the basic information and institutional infrastructure for the cooperation among Digital Services Coordinators, the Board and the Commission, taking into account the fact that in view of their size and reach very large online platforms and very large online search engines have a significant impact on the resources needed to support such infrastructure. The estimation of the overall costs should take into account the supervisory costs incurred in the previous year including, where applicable, those costs exceeding the individual annual supervisory fee charged in the previous year. The external assigned revenues resulting from the annual supervisory fee could be used to finance additional human resources, such as contractual agents and seconded national experts, and other expenditure related to the fulfilment of the tasks entrusted to the Commission by this Regulation. The annual supervisory fee to be charged on providers of very large online platforms and of very large online search engines should be proportionate to the size of the service as reflected by the number of its active recipients of the service in the Union. Moreover, the individual annual supervisory fee should not exceed an overall ceiling for each provider of very large online platforms or of very large online search engines taking into account the economic capacity of the provider of the designated service or services.

- (102) To facilitate the effective and consistent application of the obligations in this Regulation that may require implementation through technological means, it is important to promote voluntary standards covering certain technical procedures, where the industry can help develop standardised means to support providers of intermediary services in complying with this Regulation, such as allowing the submission of notices, including through application programming interfaces, or standards related to terms and conditions or standards relating to audits, or standards related to the interoperability of advertisement repositories. In addition, such standards could include standards related to online advertising, recommender systems, accessibility and the protection of minors online. Providers of intermediary services are free to adopt the standards, but their adoption does not presume compliance with this Regulation. At the same time, by providing best practices, such standards could in particular be useful for relatively small providers of intermediary services. The standards could distinguish between different types of illegal content or different types of intermediary services, as appropriate.
- (103) The Commission and the Board should encourage the drawing-up of voluntary codes of conduct, as well as the implementation of the provisions of those codes in order to contribute to the application of this Regulation. The Commission and the Board should aim that the codes of conduct clearly define the nature of the public interest objectives being addressed, that they contain mechanisms for independent evaluation of the achievement of those objectives and that the role of relevant authorities is clearly defined. Particular attention should be given to avoiding negative effects on security, the protection of privacy and personal data, as well as to the prohibition on imposing

general monitoring obligations. While the implementation of codes of conduct should be measurable and subject to public oversight, this should not impair the voluntary nature of such codes and the freedom of interested parties to decide whether to participate. In certain circumstances, it is important that very large online platforms cooperate in the drawing-up and adhere to specific codes of conduct. Nothing in this Regulation prevents other service providers from adhering to the same standards of due diligence, adopting best practices and benefitting from the guidelines provided by the Commission and the Board, by participating in the same codes of conduct.

- (104) It is appropriate that this Regulation identify certain areas of consideration for such codes of conduct. In particular, risk mitigation measures concerning specific types of illegal content should be explored via self- and co-regulatory agreements. Another area for consideration is the possible negative impacts of systemic risks on society and democracy, such as disinformation or manipulative and abusive activities or any adverse effects on minors. This includes coordinated operations aimed at amplifying information, including disinformation, such as the use of bots or fake accounts for the creation of intentionally inaccurate or misleading information, sometimes with a purpose of obtaining economic gain, which are particularly harmful for vulnerable recipients of the service, such as minors. In relation to such areas, adherence to and compliance with a given code of conduct by a very large online platform or a very large online search engine may be considered as an appropriate risk mitigating measure. The refusal without proper explanations by a provider of an online platform or of an online search engine of the Commission's invitation to participate in the application of such a code of conduct could be taken into account, where relevant, when determining whether the online platform or the online search engine has infringed the obligations laid down by this Regulation. The mere fact of participating in and implementing a given code of conduct should not in itself presume compliance with this Regulation.
- (105) The codes of conduct should facilitate the accessibility of very large online platforms and very large online search engines, in compliance with Union and national law, in order to facilitate their foreseeable use by persons with disabilities. In particular, the codes of conduct could ensure that the information is presented in a perceivable, operable, understandable and robust way and that forms and measures provided pursuant to this Regulation are made available in a manner that is easy to find and accessible to persons with disabilities.
- (106) The rules on codes of conduct under this Regulation could serve as a basis for already established self-regulatory efforts at Union level, including the Product Safety Pledge, the Memorandum of understanding on the sale of counterfeit goods on the internet, the Code of conduct on countering illegal hate speech online, as well as the Code of Practice on Disinformation. In particular for the latter, following the Commission's guidance, the Code of Practice on Disinformation has been strengthened as announced in the European Democracy Action Plan.
- (107) The provision of online advertising generally involves several actors, including intermediary services that connect publishers of advertisements with advertisers. Codes of conduct should support and complement the transparency obligations relating to advertising for providers of online platforms, of very large online platforms and of very large online search engines set out in this Regulation in order to provide for flexible and effective mechanisms to facilitate and enhance the compliance with those obligations, notably as concerns the modalities of the transmission of the relevant information. This should include facilitating the transmission of the information on the advertiser who pays for the advertisement when they differ from the natural or legal person on whose behalf the advertisement is presented on the online interface of an online platform. The codes of conduct should also include measures to ensure that meaningful information about the monetisation of data is appropriately shared throughout the value chain. The involvement of a wide range of stakeholders should ensure that those codes of conduct are widely supported, technically sound, effective and offer the highest levels of user-friendliness to ensure that the transparency obligations achieve their objectives. In order to ensure the effectiveness of codes of conduct, the Commission should include evaluation mechanisms in drawing up the codes of conduct. Where appropriate, the Commission may invite the Fundamental Rights Agency or the European Data Protection Supervisor to express their opinions on the respective code of conduct.

- (108) In addition to the crisis response mechanism for very large online platforms and very large online search engines, the Commission may initiate the drawing up of voluntary crisis protocols to coordinate a rapid, collective and cross-border response in the online environment. Such can be the case, for example, where online platforms are misused for the rapid spread of illegal content or disinformation or where the need arises for rapid dissemination of reliable information. In light of the important role of very large online platforms in disseminating information in our societies and across borders, providers of such platforms should be encouraged in drawing up and applying specific crisis protocols. Such crisis protocols should be activated only for a limited period of time and the measures adopted should also be limited to what is strictly necessary to address the extraordinary circumstance. Those measures should be consistent with this Regulation, and should not amount to a general obligation for the participating providers of very large online platforms and of very large online search engines to monitor the information which they transmit or store, nor actively to seek facts or circumstances indicating illegal content.
- (109) In order to ensure adequate oversight and enforcement of the obligations laid down in this Regulation, Member States should designate at least one authority with the task to supervise the application and enforce this Regulation, without prejudice to the possibility to designate an existing authority and to its legal form in accordance with national law. Member States should, however, be able to entrust more than one competent authority, with specific supervisory or enforcement tasks and competences concerning the application of this Regulation, for example for specific sectors where existing authorities may also be empowered, such as electronic communications' regulators, media regulators or consumer protection authorities, reflecting their domestic constitutional, organisational and administrative structure. In the exercise of their tasks, all competent authorities should contribute to the achievement of the objectives of this Regulation, namely to the proper functioning of the internal market for intermediary services where the harmonised rules for a safe, predictable and trusted online environment that facilitates innovation, and in particular the due diligence obligations applicable to different categories of providers of intermediary services, are effectively supervised and enforced, with a view to ensure that fundamental rights, as enshrined in the Charter, including the principle of consumer protection, are effectively protected. This Regulation does not require Member States to confer on competent authorities the task to adjudicate on the lawfulness of specific items of content.
- (110) Given the cross-border nature of the services at stake and the horizontal range of obligations introduced by this Regulation, one authority appointed with the task of supervising the application and, where necessary, enforcing this Regulation should be identified as a Digital Services Coordinator in each Member State. Where more than one competent authority is appointed to supervise the application of, and enforce, this Regulation, only one authority in that Member State should be designated as a Digital Services Coordinator. The Digital Services Coordinator should act as the single contact point with regard to all matters related to the application of this Regulation for the Commission, the Board, the Digital Services Coordinators of other Member States, as well as for other competent authorities of the Member State in question. In particular, where several competent authorities are entrusted with tasks under this Regulation in a given Member State, the Digital Services Coordinator should coordinate and cooperate with those authorities in accordance with the national law setting their respective tasks and without prejudice to the independent assessment of the other competent authorities. While not entailing any hierarchical supraordination over other competent authorities in the exercise of their tasks, the Digital Services Coordinator should ensure effective involvement of all relevant competent authorities and should timely report their assessment in the context of cooperation on supervision and enforcement at Union level. Moreover, in addition to the specific mechanisms provided for in this Regulation as regards cooperation at Union level, Member State should also ensure cooperation among the Digital Services Coordinator and other competent authorities designated at national level, where applicable, through appropriate tools, such as by pooling of resources, joint task forces, joint investigations and mutual assistance mechanisms.
- (111) The Digital Services Coordinator, as well as other competent authorities designated under this Regulation, play a crucial role in ensuring the effectiveness of the rights and obligations laid down in this Regulation and the achievement of its objectives. Accordingly, it is necessary to ensure that those authorities have the necessary means, including financial and human resources, to supervise all the providers of intermediary services falling within their competence, in the interest of all Union citizens. Given the variety of providers of intermediary services and their use of advanced technology in providing their services, it is also essential that the Digital Services Coordinator and the relevant competent authorities are equipped with the necessary number of staff and experts with specialised

skills and advanced technical means, and that they autonomously manage financial resources to carry out their tasks. Furthermore, the level of resources should take into account the size, complexity and potential societal impact of the providers of intermediary services falling within their competence, as well as the reach of their services across the Union. This Regulation is without prejudice to the possibility for Member States to establish funding mechanisms based on a supervisory fee charged to providers of intermediary services under national law in compliance with Union law, to the extent that it is levied on providers of intermediary services having their main establishment in the Member State in question, that it is strictly limited to what is necessary and proportionate to cover the costs for the fulfilment of the tasks conferred upon the competent authorities pursuant to this Regulation, with the exclusion of the tasks conferred upon the Commission, and that adequate transparency is ensured regarding the levying and the use of such a supervisory fee.

- (112) The competent authorities designated under this Regulation should also act in complete independence from private and public bodies, without the obligation or possibility to seek or receive instructions, including from the government, and without prejudice to the specific duties to cooperate with other competent authorities, the Digital Services Coordinators, the Board and the Commission. On the other hand, the independence of those authorities should not mean that they cannot be subject, in accordance with national constitutions and without endangering the achievement of the objectives of this Regulation, to proportionate accountability mechanisms regarding the general activities of the Digital Services Coordinators, such as their financial expenditure or reporting to the national parliaments. The requirement of independence should also not prevent the exercise of judicial review, or the possibility to consult or regularly exchange views with other national authorities, including law enforcement authorities, crisis management authorities or consumer protection authorities, where appropriate, in order to inform each other about ongoing investigations, without affecting the exercise of their respective powers.
- (113) Member States can designate an existing national authority with the function of the Digital Services Coordinator, or with specific tasks to supervise the application and enforce this Regulation, provided that any such appointed authority complies with the requirements laid down in this Regulation, such as in relation to its independence. Moreover, Member States are in principle not precluded from merging functions within an existing authority, in accordance with Union law. The measures to that effect may include, *inter alia*, the preclusion to dismiss the president or a board member of a collegiate body of an existing authority before the expiry of their terms of office, on the sole ground that an institutional reform has taken place involving the merger of different functions within one authority, in the absence of any rules guaranteeing that such dismissals do not jeopardise the independence and impartiality of such members.
- (114) Member States should provide the Digital Services Coordinator, and any other competent authority designated under this Regulation, with sufficient powers and means to ensure effective investigation and enforcement, in accordance with the tasks conferred on them. This includes the power of competent authorities to adopt interim measures in accordance with national law in case of risk of serious harm. Such interim measures, which may include orders to terminate or remedy a given alleged infringement, should not go beyond what is necessary to ensure that serious harm is prevented pending the final decision. The Digital Services Coordinators should in particular be able to search for and obtain information which is located in its territory, including in the context of joint investigations, with due regard to the fact that oversight and enforcement measures concerning a provider under the jurisdiction of another Member State or the Commission should be adopted by the Digital Services Coordinator of that other Member State, where relevant in accordance with the procedures relating to cross-border cooperation, or, where applicable, by the Commission.
- (115) Member States should set out in their national law, in accordance with Union law and in particular this Regulation and the Charter, the detailed conditions and limits for the exercise of the investigatory and enforcement powers of their Digital Services Coordinators, and other competent authorities where relevant, under this Regulation.

- (116) In the course of the exercise of those powers, the competent authorities should comply with the applicable national rules regarding procedures and matters such as the need for a prior judicial authorisation to enter certain premises and legal professional privilege. Those provisions should in particular ensure respect for the fundamental rights to an effective remedy and to a fair trial, including the rights of defence, and, the right to respect for private life. In this regard, the guarantees provided for in relation to the proceedings of the Commission pursuant to this Regulation could serve as an appropriate point of reference. A prior, fair and impartial procedure should be guaranteed before taking any final decision, including the right to be heard of the persons concerned, and the right to have access to the file, while respecting confidentiality and professional and business secrecy, as well as the obligation to give meaningful reasons for the decisions. This should not preclude the taking of measures, however, in duly substantiated cases of urgency and subject to appropriate conditions and procedural arrangements. The exercise of powers should also be proportionate to, *inter alia* the nature and the overall actual or potential harm caused by the infringement or suspected infringement. The competent authorities should take all relevant facts and circumstances of the case into account, including information gathered by competent authorities in other Member States.
- (117) Member States should ensure that violations of the obligations laid down in this Regulation can be sanctioned in a manner that is effective, proportionate and dissuasive, taking into account the nature, gravity, recurrence and duration of the violation, in view of the public interest pursued, the scope and kind of activities carried out, as well as the economic capacity of the infringer. In particular, penalties should take into account whether the provider of intermediary services concerned systematically or recurrently fails to comply with its obligations stemming from this Regulation, as well as, where relevant, the number of recipients of the service affected, the intentional or negligent character of the infringement and whether the provider is active in several Member States. Where this Regulation provides for a maximum amount of fines or of a periodic penalty payment, this maximum amount should apply per infringement of this Regulation and without prejudice to the modulation of the fines or periodic penalty payments for specific infringements. Member States should ensure that the imposition of fines or periodic penalty payments in respect of infringements should in each individual case be effective, proportionate and dissuasive by setting up national rules and procedures in accordance with this Regulation, taking into account all the criteria concerning the general conditions for imposing the fines or periodic penalty payments.
- (118) In order to ensure effective enforcement of the obligations laid down in this Regulation, individuals or representative organisations should be able to lodge any complaint related to compliance with those obligations with the Digital Services Coordinator in the territory where they received the service, without prejudice to this Regulation's rules on allocation of competences and to the applicable rules on handling of complaints in accordance with national principles of good administration. Complaints could provide a faithful overview of concerns related to a particular intermediary service provider's compliance and could also inform the Digital Services Coordinator of any more cross-cutting issues. The Digital Services Coordinator should involve other national competent authorities as well as the Digital Services Coordinator of another Member State, and in particular the one of the Member State where the provider of intermediary services concerned is established, if the issue requires cross-border cooperation.
- (119) Member States should ensure that Digital Services Coordinators can take measures that are effective in addressing and proportionate to certain particularly serious and persistent infringements of this Regulation. Especially where those measures can affect the rights and interests of third parties, as may be the case in particular where the access to online interfaces is restricted, it is appropriate to require that the measures are subject to additional safeguards. In particular, third parties potentially affected should be afforded the opportunity to be heard and such orders should only be issued when powers to take such measures as provided by other acts of Union law or by national law, for instance to protect collective interests of consumers, to ensure the prompt removal of web pages containing or disseminating child pornography, or to disable access to services that are being used by a third party to infringe an intellectual property right, are not reasonably available.

- (120) Such an order to restrict access should not go beyond what is necessary to achieve its objective. For that purpose, it should be temporary and be addressed in principle to a provider of intermediary services, such as the relevant hosting service provider, internet service provider or domain registry or registrar, which is in a reasonable position to achieve that objective without unduly restricting access to lawful information.
- (121) Without prejudice to the provisions on the exemption from liability provided for in this Regulation as regards the information transmitted or stored at the request of a recipient of the service, a provider of intermediary services should be liable for the damages suffered by recipients of the service that are caused by an infringement of the obligations set out in this Regulation by that provider. Such compensation should be in accordance with the rules and procedures set out in the applicable national law and without prejudice to other possibilities for redress available under consumer protection rules.
- (122) The Digital Services Coordinator should regularly publish, for example on its website, a report on the activities carried out under this Regulation. In particular, the report should be published in a machine-readable format and include an overview of complaints received and of their follow-up, such as the overall number of complaints received and the number of complaints that led to the opening of a formal investigation or to the transmission to other Digital Services Coordinators, without referring to any personal data. Given that the Digital Services Coordinator is also made aware of orders to take action against illegal content or to provide information regulated by this Regulation through the information sharing system, the Digital Services Coordinator should include in its annual report the number and categories of such orders addressed to providers of intermediary services issued by judicial and administrative authorities in its Member State.
- (123) In the interest of clarity, simplicity and effectiveness, the powers to supervise and enforce the obligations under this Regulation should be conferred to the competent authorities in the Member State where the main establishment of the provider of intermediary services is located, that is, where the provider has its head office or registered office within which the principal financial functions and operational control are exercised. In respect of providers that are not established in the Union, but that offer services in the Union and therefore fall within the scope of this Regulation, the Member State where those providers appointed their legal representative should have competence, considering the function of legal representatives under this Regulation. In the interest of the effective application of this Regulation, all Member States or the Commission, where applicable, should, however, have competence in respect of providers that failed to designate a legal representative. That competence may be exercised by any of the competent authorities or the Commission, provided that the provider is not subject to enforcement proceedings for the same facts by another competent authority or the Commission. In order to ensure that the principle of *ne bis in idem* is respected, and in particular to avoid that the same infringement of the obligations laid down in this Regulation is sanctioned more than once, each Member State that intends to exercise its competence in respect of such providers should, without undue delay, inform all other authorities, including the Commission, through the information sharing system established for the purpose of this Regulation.
- (124) In view of their potential impact and the challenges involved in effectively supervising them, special rules are needed regarding the supervision and enforcement in respect of providers of very large online platforms and of very large online search engines. The Commission should be responsible, with the support of national competent authorities where relevant, for oversight and public enforcement of systemic issues, such as issues with a wide impact on collective interests of recipients of the service. Therefore, the Commission should have exclusive powers of supervision and enforcement of the additional obligations to manage systemic risks imposed on providers of very large online platforms and of very large online search engines by this Regulation. The exclusive powers of the Commission should be without prejudice to certain administrative tasks assigned by this Regulation to the competent authorities of the Member State of establishment, such as the vetting of researchers.

- (125) The powers of supervision and enforcement of due diligence obligations, other than the additional obligations to manage systemic risks imposed on providers of very large online platforms and of very large online search engines by this Regulation, should be shared by the Commission and by the national competent authorities. On the one hand, the Commission could in many instances be better placed to address systemic infringements committed by those providers, such as those affecting multiple Member States or serious repeated infringements or concerning a failure to establish effective mechanisms required by this Regulation. On the other hand, the competent authorities in the Member State where the main establishment of a provider of very large online platform or of very large online search engine is located could be better placed to address individual infringements committed by those providers, that do not raise any systemic or cross-border issues. In the interest of efficiency, to avoid duplication and to ensure compliance with the principle of *ne bis in idem*, it should be for the Commission to assess whether it deems it appropriate to exercise those shared competences in a given case and, once it has initiated proceedings, Member States should no longer have the ability to do so. Member States should cooperate closely both with each other and with the Commission, and the Commission should cooperate closely with the Member States, in order to ensure that the system of supervision and enforcement set up by this Regulation functions smoothly and effectively.
- (126) The rules of this Regulation on the allocation of competence should be without prejudice to the provisions of Union law and national rules on private international law concerning jurisdiction and applicable law in civil and commercial matters, such as proceedings brought by consumers in the courts of the Member State where they are domiciled in accordance with relevant provisions of Union law. Regarding the obligations imposed by this Regulation on providers of intermediary services to inform the issuing authority of the effect given to the orders to act against illegal content and orders to provide information, the rules on allocation of competence should only apply to the supervision of enforcement of those obligations, but not to other matters related to the order, such as the competence to issue the order.
- (127) Given the cross-border and cross-sectoral relevance of intermediary services, a high level of cooperation is necessary to ensure the consistent application of this Regulation and the availability of relevant information for the exercise of enforcement tasks through the information sharing system. Cooperation may take different forms depending on the issues at stake, without prejudice to specific joint investigation exercises. It is in any case necessary that the Digital Services Coordinator of establishment of a provider of intermediary services informs other Digital Services Coordinators about issues, investigations and actions which are going to be taken vis à vis such a provider. Moreover, when a competent authority in a Member State holds relevant information for an investigation carried out by the competent authorities in the Member State of establishment, or is able to gather such information located in its territory to which the competent authorities in the Member State of establishment do not have access, the Digital Services Coordinator of destination should assist the Digital Services Coordinator of establishment in a timely manner, including through the exercise of its powers of investigation in accordance with the applicable national procedures and the Charter. The addressee of such investigatory measures should comply with them and be liable in case of failure to comply, and the competent authorities in the Member State of establishment should be able to rely on the information gathered through mutual assistance, in order to ensure compliance with this Regulation.
- (128) The Digital Services Coordinator of destination, in particular on the basis of complaints received or of the input of other national competent authorities where appropriate, or the Board in case of issues involving at least three Member States, should be able to ask the Digital Services Coordinator of establishment to take investigatory or enforcement actions with regard to a provider under its competence. Such requests for action should be based on well-substantiated evidence showing the existence of an alleged infringement with negative impact on collective interests of the recipients of the service in its Member State or having a negative societal impact. The Digital Services Coordinator of establishment should be able to rely on mutual assistance or invite the requesting Digital Services Coordinator to a joint investigation in case further information is needed to take a decision, without prejudice to the possibility to request the Commission to assess the matter if it has reason to suspect that a systemic infringement by a very large online platform or a very large online search engine may be at stake.

- (129) The Board should be able to refer the matter to the Commission in case of any disagreement as to the assessments or the measures taken or proposed or of a failure to adopt any measures in accordance with this Regulation following a cross-border cooperation request or a joint investigation. Where the Commission, on the basis of the information made available by the concerned authorities, considers that the proposed measures, including the proposed level of fines, cannot ensure the effective enforcement of the obligations laid down in this Regulation, it should accordingly be able to express its serious doubts and request the competent Digital Services Coordinator to re-assess the matter and take the necessary measures to ensure compliance with this Regulation within a defined period. This possibility is without prejudice to the Commission's general duty to oversee the application of, and where necessary enforce, Union law under the control of the Court of Justice of the European Union in accordance with the Treaties.
- (130) In order to facilitate cross-border supervision and investigations of obligations laid down in this Regulation involving several Member States, the Digital Services Coordinators of establishment should be able, through the information sharing system, to invite other Digital Services Coordinators to a joint investigation concerning an alleged infringement of this Regulation. Other Digital Services Coordinators, and other competent authorities, where appropriate, should be able to join the investigation proposed by the Digital Services Coordinator of establishment, unless the latter considers that an excessive number of participating authorities may affect the effectiveness of the investigation taking into account the features of the alleged infringement and the lack of direct effects on the recipients of the service in those Member States. Joint investigation activities may include a variety of actions to be coordinated by the Digital Services Coordinator of establishment in accordance with the availabilities of the participating authorities, such as coordinated data gathering exercises, pooling of resources, task forces, coordinated requests for information or common inspections of premises. All competent authorities participating in a joint investigation should cooperate with the Digital Services Coordinator of establishment, including by exercising their powers of investigation within their territory, in accordance with the applicable national procedures. The joint investigation should be concluded within a given timeframe with a final report taking into account the contribution of all participating competent authorities. Also the Board, where this is requested by at least three Digital Services Coordinators of destination, may recommend to a Digital Services Coordinator of establishment to launch such joint investigation and give indications on its organisation. In order to avoid deadlocks, the Board should be able to refer the matter to the Commission in specific cases, including where the Digital Services Coordinator of establishment refuses to launch the investigation and the Board does not agree with the justification given.
- (131) In order to ensure a consistent application of this Regulation, it is necessary to set up an independent advisory group at Union level, a European Board for Digital Services, which should support the Commission and help coordinate the actions of Digital Services Coordinators. The Board should consist of the Digital Services Coordinators, where these have been appointed, without prejudice to the possibility for Digital Services Coordinators to invite in its meetings or appoint ad hoc delegates from other competent authorities entrusted with specific tasks under this Regulation, where that is required pursuant to their national allocation of tasks and competences. In case of multiple participants from one Member State, the voting right should remain limited to one representative per Member State.
- (132) The Board should contribute to achieving a common Union perspective on the consistent application of this Regulation and to the cooperation among competent authorities, including by advising the Commission and the Digital Services Coordinators about appropriate investigation and enforcement measures, in particular vis à vis the providers of very large online platforms or of very large online search engines and having regard, in particular, to the freedom of the providers of intermediary services to provide services across the Union. The Board should also contribute to the drafting of relevant templates and codes of conduct and to the analysis of emerging general trends in the development of digital services in the Union, including by issuing opinions or recommendations on matters related to standards.

- (133) For that purpose, the Board should be able to adopt opinions, requests and recommendations addressed to Digital Services Coordinators or other competent national authorities. While not legally binding, the decision to deviate therefrom should be properly explained and could be taken into account by the Commission in assessing the compliance of the Member State concerned with this Regulation.
- (134) The Board should bring together the representatives of the Digital Services Coordinators and possible other competent authorities under the chairmanship of the Commission, with a view to ensuring an assessment of matters submitted to it in a fully European dimension. In view of possible cross-cutting elements that may be of relevance for other regulatory frameworks at Union level, the Board should be allowed to cooperate with other Union bodies, offices, agencies and advisory groups with responsibilities in fields such as equality, including gender equality, and non-discrimination, data protection, electronic communications, audiovisual services, detection and investigation of frauds against the Union budget as regards custom duties, consumer protection, or competition law, as necessary for the performance of its tasks.
- (135) The Commission, through the Chair, should participate in the Board without voting rights. Through the Chair, the Commission should ensure that the agenda of the meetings is set in accordance with the requests of the members of the Board as laid down in the rules of procedure and in compliance with the duties of the Board laid down in this Regulation.
- (136) In view of the need to ensure support for the Board's activities, the Board should be able to rely on the expertise and human resources of the Commission and of the competent national authorities. The specific operational arrangements for the internal functioning of the Board should be further specified in the rules of procedure of the Board.
- (137) Given the importance of very large online platforms or very large online search engines, in view of their reach and impact, their failure to comply with the specific obligations applicable to them may affect a substantial number of recipients of the services across different Member States and may cause large societal harms, while such failures may also be particularly complex to identify and address. For this reason the Commission, in cooperation with the Digital Services Coordinators and the Board, should develop the Union expertise and capabilities as regards the supervision of very large online platforms or very large online search engines. The Commission should therefore be able to coordinate and rely on the expertise and resources of such authorities, for example by analysing, on a permanent or temporary basis, specific trends or issues emerging with regard to one or more very large online platforms or very large online search engines. Member States should cooperate with the Commission in developing such capabilities, including through secondment of personnel where appropriate, and contributing to the creation of a common Union supervisory capacity. In order to develop the Union expertise and capabilities, the Commission may also draw on the expertise and capabilities of the Observatory on the Online Platform Economy as set up in Commission Decision of 26 April 2018 on setting up the group of experts for the Observatory on the Online Platform Economy, relevant expert bodies, as well as centres of excellence. The Commission may invite experts with specific expertise, including in particular vetted researchers, representatives of Union agencies and bodies, industry representatives, associations representing users or civil society, international organisations, experts from the private sector, as well as other stakeholders.
- (138) The Commission should be able to investigate infringements on its own initiative in accordance with the powers provided for in this Regulation, including by asking access to data, by requesting information or by performing inspections, as well as by relying on the support of the Digital Services Coordinators. Where supervision by the competent national authorities of individual alleged infringements by providers of very large online platforms or very large online search engines points to systemic issues, such as issues with a wide impact on collective interests of recipients of the service, the Digital Services Coordinators should be able to, on the basis of a duly reasoned request, refer such issues to the Commission. Such a request should contain, at least, all the necessary facts and circumstances supporting the alleged infringement and its systemic nature. Depending on the outcome of its own assessment, the Commission should be able to take the necessary investigative and enforcement measures pursuant to this Regulation, including, where relevant, launching an investigation or adopting interim measures.

- (139) In order to effectively perform its tasks, the Commission should maintain a margin of discretion as to the decision to initiate proceedings against providers of very large online platforms or of very large online search engine. Once the Commission initiated the proceedings, the Digital Services Coordinators of establishment concerned should be precluded from exercising their investigative and enforcement powers in respect of the concerned conduct of the provider of the very large online platform or of very large online search engine, so as to avoid duplication, inconsistencies and risks from the viewpoint of the principle of *ne bis in idem*. The Commission, however, should be able to ask for the individual or joint contribution of the Digital Services Coordinators to the investigation. In accordance with the duty of sincere cooperation, the Digital Services Coordinator should make its best efforts in fulfilling justified and proportionate requests by the Commission in the context of an investigation. Moreover, the Digital Services Coordinator of establishment, as well as the Board and any other Digital Services Coordinators where relevant, should provide the Commission with all necessary information and assistance to allow it to perform its tasks effectively, including information gathered in the context of data gathering or data access exercises, to the extent that this is not precluded by the legal basis according to which the information has been gathered. Conversely, the Commission should keep the Digital Services Coordinator of establishment and the Board informed on the exercise of its powers and in particular when it intends to initiate the proceeding and exercise its investigatory powers. Moreover, when the Commission communicates its preliminary findings, including any matter to which it objects, to providers of very large online platforms or of very large online search engines concerned, it should also communicate them to the Board. The Board should provide its views on the objections and assessment made by the Commission, which should take this opinion into account in the reasoning underpinning Commission's final decision.
- (140) In view of both the particular challenges that may arise in seeking to ensure compliance by providers of very large online platforms or of very large online search engines and the importance of doing so effectively, considering their size and impact and the harms that they may cause, the Commission should have strong investigative and enforcement powers to allow it to investigate, enforce and monitor compliance with the rules laid down in this Regulation, in full respect of the fundamental right to be heard and to have access to the file in the context of enforcement proceedings, the principle of proportionality and the rights and interests of the affected parties.
- (141) The Commission should be able to request information necessary for the purpose of ensuring the effective implementation of and compliance with the obligations laid down in this Regulation, throughout the Union. In particular, the Commission should have access to any relevant documents, data and information necessary to open and conduct investigations and to monitor the compliance with the relevant obligations laid down in this Regulation, irrespective of who possesses the documents, data or information in question, and regardless of their form or format, their storage medium, or the precise place where they are stored. The Commission should be able to directly require by means of a duly substantiated request for information that the provider of the very large online platform or of the very large online search engine concerned as well as any other natural or legal persons acting for purposes related to their trade, business, craft or profession that may be reasonably aware of information relating to the suspected infringement or the infringement, as applicable, provide any relevant evidence, data and information. In addition, the Commission should be able to request any relevant information from any public authority, body or agency within the Member State for the purpose of this Regulation. The Commission should be able to require access to, and explanations by means of exercise of investigatory powers, such as requests for information or interviews, relating to documents, data, information, data-bases and algorithms of relevant persons, and to interview, with their consent, any natural or legal persons who may be in possession of useful information and to record the statements made by any technical means. The Commission should also be empowered to undertake such inspections as are necessary to enforce the relevant provisions of this Regulation. Those investigatory powers aim to complement the Commission's possibility to ask Digital Services Coordinators and other Member States' authorities for assistance, for instance by providing information or in the exercise of those powers.

- (142) Interim measures can be an important tool to ensure that, while an investigation is ongoing, the infringement being investigated does not lead to the risk of serious damage for the recipients of the service. This tool is important to avoid developments that could be very difficult to reverse by a decision taken by the Commission at the end of the proceedings. The Commission should therefore have the power to impose interim measures by decision in the context of proceedings opened in view of the possible adoption of a decision of non-compliance. This power should apply in cases where the Commission has made a *prima facie* finding of infringement of obligations under this Regulation by the provider of very large online platform or of very large online search engine. A decision imposing interim measures should only apply for a specified period, either one ending with the conclusion of the proceedings by the Commission, or for a fixed period which can be renewed insofar as it is necessary and appropriate.
- (143) The Commission should be able to take the necessary actions to monitor the effective implementation of and compliance with the obligations laid down in this Regulation. Such actions should include the ability to appoint independent external experts and auditors to assist the Commission in this process, including where applicable from competent authorities of the Member States, such as data or consumer protection authorities. When appointing auditors, the Commission should ensure sufficient rotation.
- (144) Compliance with the relevant obligations imposed under this Regulation should be enforceable by means of fines and periodic penalty payments. To that end, appropriate levels of fines and periodic penalty payments should also be laid down for non-compliance with the obligations and breach of the procedural rules, subject to appropriate limitation periods in accordance with the principles of proportionality and *ne bis in idem*. The Commission and the relevant national authorities should coordinate their enforcement efforts in order to ensure that those principles are respected. In particular, the Commission should take into account any fines and penalties imposed on the same legal person for the same facts through a final decision in proceedings relating to an infringement of other Union or national rules, so as to ensure that the overall fines and penalties imposed are proportionate and correspond to the seriousness of the infringements committed. All decisions taken by the Commission under this Regulation are subject to review by the Court of Justice of the European Union in accordance with the TFEU. The Court of Justice of the European Union should have unlimited jurisdiction in respect of fines and penalty payments in accordance with Article 261 TFEU.
- (145) Given the potential significant societal effects of an infringement of the additional obligations to manage systemic risks that solely apply to very large online platforms and very large online search engines and in order to address those public policy concerns, it is necessary to provide for a system of enhanced supervision of any action undertaken to effectively terminate and remedy infringements of this Regulation. Therefore, once an infringement of one of the provisions of this Regulation that solely apply to very large online platforms or very large online search engines has been ascertained and, where necessary, sanctioned, the Commission should request the provider of such platform or of such search engine to draw a detailed action plan to remedy any effect of the infringement for the future and communicate such action plan within a timeline set by the Commission, to the Digital Services Coordinators, the Commission and the Board. The Commission, taking into account the opinion of the Board, should establish whether the measures included in the action plan are sufficient to address the infringement, taking also into account whether adherence to relevant code of conduct is included among the measures proposed. The Commission should also monitor any subsequent measure taken by the provider of a very large online platform or of a very large online search engine concerned as set out in its action plan, taking into account also an independent audit of the provider. If following the implementation of the action plan the Commission still considers that the infringement has not been fully remedied, or if the action plan has not been provided or is not considered suitable, it should be able to use any investigative or enforcement powers pursuant to this Regulation, including the power to impose periodic penalty payments and initiating the procedure to disable access to the infringing service.

- (146) The provider of the very large online platform or of the very large online search engine concerned and other persons subject to the exercise of the Commission's powers whose interests may be affected by a decision should be given the opportunity of submitting their observations beforehand, and the decisions taken should be widely publicised. While ensuring the rights of defence of the parties concerned, in particular, the right of access to the file, it is essential that confidential information be protected. Furthermore, while respecting the confidentiality of the information, the Commission should ensure that any information relied on for the purpose of its decision is disclosed to an extent that allows the addressee of the decision to understand the facts and considerations that led up to the decision.
- (147) In order to safeguard the harmonised application and enforcement of this Regulation, it is important to ensure that national authorities, including national courts, have all necessary information to ensure that their decisions do not run counter to a decision adopted by the Commission under this Regulation. This is without prejudice to Article 267 TFEU.
- (148) The effective enforcement and monitoring of this Regulation requires a seamless and real-time exchange of information among the Digital Services Coordinators, the Board and the Commission, based on the information flows and procedures set out in this Regulation. This may also warrant access to this system by other competent authorities, where appropriate. At the same time, given that the information exchanged may be confidential or involving personal data, it should remain protected from unauthorised access, in accordance with the purposes for which the information has been gathered. For this reason, all communications between those authorities should take place on the basis of a reliable and secure information sharing system, whose details should be laid down in an implementing act. The information sharing system may be based on existing internal market tools, to the extent that they can meet the objectives of this Regulation in a cost-effective manner.
- (149) Without prejudice to the rights of recipients of services to turn to a representative in accordance with the Directive (EU) 2020/1828 of the European Parliament and of the Council <sup>(33)</sup> or to any other type of representation under national law, recipients of the services should also have the right to mandate a legal person or a public body to exercise their rights provided for in this Regulation. Such rights may include the rights related to the submission of notices, the challenging of the decisions taken by providers of intermediary services, and the lodging of complaints against the providers for infringing this Regulation. Certain bodies, organisations and associations have particular expertise and competence in detecting and flagging erroneous or unjustified content moderation decisions, and their complaints on behalf of recipients of the service may have a positive impact on freedom of expression and of information in general, therefore, providers of online platforms should treat those complaints without undue delay.
- (150) In the interest of effectiveness and efficiency, the Commission should carry out a general evaluation of this Regulation. In particular, that general evaluation should address, *inter alia*, the scope of the services covered by this Regulation, the interplay with other legal acts, the impact of this Regulation on the functioning of the internal market, in particular regarding digital services, the implementation of codes of conduct, the obligation to designate a legal representative established in the Union, the effect of the obligations on small and micro enterprises, the effectiveness of the supervision and enforcement mechanism and the impact on the right to freedom of expression and of information. In addition, to avoid disproportionate burdens and ensure the continued effectiveness of this Regulation, the Commission should perform an evaluation of the impact of the obligations set out in this Regulation on small and medium-sized enterprises within three years from the start of its application and an evaluation on the scope of the services covered by this Regulation, particularly for very large online platforms and for very large online search engines, and the interplay with other legal acts within three years from its entry into force.

---

<sup>(33)</sup> Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409, 4.12.2020, p. 1).

- (151) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to lay down templates concerning the form, content and other details of reports on content moderation, to establish the amount of the annual supervisory fee charged on providers of very large online platforms and of very large online search engines, to lay down the practical arrangements for the proceedings, the hearings and the negotiated disclosure of information carried out in the context of supervision, investigation, enforcement and monitoring in respect of providers of very large online platforms and of very large online search engines, as well as to lay down the practical and operational arrangements for the functioning of the information sharing system and its interoperability with other relevant systems. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council <sup>(34)</sup>.
- (152) In order to fulfil the objectives of this Regulation, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to supplement this Regulation, in respect of criteria for the identification of very large online platforms and of very large online search engines, the procedural steps, methodologies and reporting templates for the audits, the technical specifications for access requests and the detailed methodology and procedures for setting the supervisory fee. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making <sup>(35)</sup>. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.
- (153) This Regulation respects the fundamental rights recognised by the Charter and the fundamental rights constituting general principles of Union law. Accordingly, this Regulation should be interpreted and applied in accordance with those fundamental rights, including the freedom of expression and of information, as well as the freedom and pluralism of the media. When exercising the powers set out in this Regulation, all public authorities involved should achieve, in situations where the relevant fundamental rights conflict, a fair balance between the rights concerned, in accordance with the principle of proportionality.
- (154) Given the scope and impact of societal risks that may be caused by very large online platforms and very large online search engines, the need to address those risks as a matter of priority and the capacity to take the necessary measures, it is justified to limit the period after which this Regulation starts to apply to the providers of those services.
- (155) Since the objectives of this Regulation, namely to contribute to the proper functioning of the internal market and to ensure a safe, predictable and trusted online environment in which the fundamental rights enshrined in the Charter are duly protected, cannot be sufficiently achieved by the Member States because they cannot achieve the necessary harmonisation and cooperation by acting alone, but can rather, by reason of territorial and personal scope, be better achieved at the Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.
- (156) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council <sup>(36)</sup> and delivered an opinion on 10 February 2021 <sup>(37)</sup>,

<sup>(34)</sup> Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

<sup>(35)</sup> OJ L 123, 12.5.2016, p. 1.

<sup>(36)</sup> Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

<sup>(37)</sup> OJ C 149, 27.4.2021, p. 3.

HAVE ADOPTED THIS REGULATION:

## CHAPTER I

### GENERAL PROVISIONS

#### *Article 1*

##### **Subject matter**

1. The aim of this Regulation is to contribute to the proper functioning of the internal market for intermediary services by setting out harmonised rules for a safe, predictable and trusted online environment that facilitates innovation and in which fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected.
2. This Regulation lays down harmonised rules on the provision of intermediary services in the internal market. In particular, it establishes:
  - (a) a framework for the conditional exemption from liability of providers of intermediary services;
  - (b) rules on specific due diligence obligations tailored to certain specific categories of providers of intermediary services;
  - (c) rules on the implementation and enforcement of this Regulation, including as regards the cooperation of and coordination between the competent authorities.

#### *Article 2*

##### **Scope**

1. This Regulation shall apply to intermediary services offered to recipients of the service that have their place of establishment or are located in the Union, irrespective of where the providers of those intermediary services have their place of establishment.
2. This Regulation shall not apply to any service that is not an intermediary service or to any requirements imposed in respect of such a service, irrespective of whether the service is provided through the use of an intermediary service.
3. This Regulation shall not affect the application of Directive 2000/31/EC.
4. This Regulation is without prejudice to the rules laid down by other Union legal acts regulating other aspects of the provision of intermediary services in the internal market or specifying and complementing this Regulation, in particular, the following:
  - (a) Directive 2010/13/EU;
  - (b) Union law on copyright and related rights;
  - (c) Regulation (EU) 2021/784;
  - (d) Regulation (EU) 2019/1148;
  - (e) Regulation (EU) 2019/1150;
  - (f) Union law on consumer protection and product safety, including Regulations (EU) 2017/2394 and (EU) 2019/1020 and Directives 2001/95/EC and 2013/11/EU;
  - (g) Union law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC;

- (h) Union law in the field of judicial cooperation in civil matters, in particular Regulation (EU) No 1215/2012 or any Union legal act laying down the rules on law applicable to contractual and non-contractual obligations;
- (i) Union law in the field of judicial cooperation in criminal matters, in particular a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters;
- (j) a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.

### Article 3

#### Definitions

For the purpose of this Regulation, the following definitions shall apply:

- (a) ‘information society service’ means a ‘service’ as defined in Article 1(1), point (b), of Directive (EU) 2015/1535;
- (b) ‘recipient of the service’ means any natural or legal person who uses an intermediary service, in particular for the purposes of seeking information or making it accessible;
- (c) ‘consumer’ means any natural person who is acting for purposes which are outside his or her trade, business, craft, or profession;
- (d) ‘to offer services in the Union’ means enabling natural or legal persons in one or more Member States to use the services of a provider of intermediary services that has a substantial connection to the Union;
- (e) ‘substantial connection to the Union’ means a connection of a provider of intermediary services with the Union resulting either from its establishment in the Union or from specific factual criteria, such as:
  - a significant number of recipients of the service in one or more Member States in relation to its or their population; or
  - the targeting of activities towards one or more Member States;
- (f) ‘trader’ means any natural person, or any legal person irrespective of whether it is privately or publicly owned, who is acting, including through any person acting in his or her name or on his or her behalf, for purposes relating to his or her trade, business, craft or profession;
- (g) ‘intermediary service’ means one of the following information society services:
  - (i) a ‘mere conduit’ service, consisting 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;
  - (ii) a ‘caching’ service, consisting of the transmission in a communication network of information provided by a recipient of the service, involving 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 upon their request;
  - (iii) a ‘hosting’ service, consisting of the storage of information provided by, and at the request of, a recipient of the service;
- (h) ‘illegal content’ means any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law;

- (i) 'online platform' means a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation;
- (j) 'online search engine' means an intermediary service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found;
- (k) 'dissemination to the public' means making information available, at the request of the recipient of the service who provided the information, to a potentially unlimited number of third parties;
- (l) 'distance contract' means 'distance contract' as defined in Article 2, point (7), of Directive 2011/83/EU;
- (m) 'online interface' means any software, including a website or a part thereof, and applications, including mobile applications;
- (n) 'Digital Services Coordinator of establishment' means the Digital Services Coordinator of the Member State where the main establishment of a provider of an intermediary service is located or its legal representative resides or is established;
- (o) 'Digital Services Coordinator of destination' means the Digital Services Coordinator of a Member State where the intermediary service is provided;
- (p) 'active recipient of an online platform' means a recipient of the service that has engaged with an online platform by either requesting the online platform to host information or being exposed to information hosted by the online platform and disseminated through its online interface;
- (q) 'active recipient of an online search engine' means a recipient of the service that has submitted a query to an online search engine and been exposed to information indexed and presented on its online interface;
- (r) 'advertisement' means information designed to promote the message of a legal or natural person, irrespective of whether to achieve commercial or non-commercial purposes, and presented by an online platform on its online interface against remuneration specifically for promoting that information;
- (s) 'recommender system' means a fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service or prioritise that information, including as a result of a search initiated by the recipient of the service or otherwise determining the relative order or prominence of information displayed;
- (t) 'content moderation' means the activities, whether automated or not, undertaken by providers of intermediary services, that are aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetisation, disabling of access to, or removal thereof, or that affect the ability of the recipients of the service to provide that information, such as the termination or suspension of a recipient's account;
- (u) 'terms and conditions' means all clauses, irrespective of their name or form, which govern the contractual relationship between the provider of intermediary services and the recipients of the service;

- (v) 'persons with disabilities' means 'persons with disabilities' as referred to in Article 3, point (1), of Directive (EU) 2019/882 of the European Parliament and of the Council <sup>(38)</sup>;
- (w) 'commercial communication' means 'commercial communication' as defined in Article 2, point (f), of Directive 2000/31/EC;
- (x) 'turnover' means the amount derived by an undertaking within the meaning of Article 5(1) of Council Regulation (EC) No 139/2004 <sup>(39)</sup>.

## CHAPTER II

### LIABILITY OF PROVIDERS OF INTERMEDIARY SERVICES

#### *Article 4*

##### **'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, the service provider shall not be liable for the information transmitted or accessed, 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 shall 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 judicial or administrative authority, in accordance with a Member State's legal system, to require the service provider to terminate or prevent an infringement.

#### *Article 5*

##### **'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, the service provider shall not be liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient or more secure the information's onward transmission to other recipients of the service upon their request, on condition that the provider:

- (a) does not modify the information;
- (b) complies with conditions on access to the information;
- (c) complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;

<sup>(38)</sup> Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (OJ L 151, 7.6.2019, p. 70).

<sup>(39)</sup> Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (OJ L 24, 29.1.2004, p. 1).

- (d) 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) 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 judicial or an administrative authority has ordered such removal or disablement.

2. This Article shall not affect the possibility for a judicial or administrative authority, in accordance with a Member State's legal system, to require the service provider to terminate or prevent an infringement.

#### *Article 6*

#### **Hosting**

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

- (a) does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or
- (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content.

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

3. Paragraph 1 shall not apply with respect to the liability under consumer protection law of online platforms that allow consumers to conclude distance contracts with traders, where such an online platform presents the specific item of information or otherwise enables the specific transaction at issue in a way that would lead an average consumer to believe that the information, or the product or service that is the object of the transaction, is provided either by the online platform itself or by a recipient of the service who is acting under its authority or control.

4. This Article shall not affect the possibility for a judicial or administrative authority, in accordance with a Member State's legal system, to require the service provider to terminate or prevent an infringement.

#### *Article 7*

#### **Voluntary own-initiative investigations and legal compliance**

Providers of intermediary services shall not be deemed ineligible for the exemptions from liability referred to in Articles 4, 5 and 6 solely because they, in good faith and in a diligent manner, carry out voluntary own-initiative investigations into, or take other measures aimed at detecting, identifying and removing, or disabling access to, illegal content, or take the necessary measures to comply with the requirements of Union law and national law in compliance with Union law, including the requirements set out in this Regulation.

#### *Article 8*

#### **No general monitoring or active fact-finding obligations**

No general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers.

*Article 9***Orders to act against illegal content**

1. Upon the receipt of an order to act against one or more specific items of illegal content, issued by the relevant national judicial or administrative authorities, on the basis of the applicable Union law or national law in compliance with Union law, providers of intermediary services shall inform the authority issuing the order, or any other authority specified in the order, of any effect given to the order without undue delay, specifying if and when effect was given to the order.
2. Member States shall ensure that when an order referred to in paragraph 1 is transmitted to the provider, it meets at least the following conditions:
  - (a) that order contains the following elements:
    - (i) a reference to the legal basis under Union or national law for the order;
    - (ii) a statement of reasons explaining why the information is illegal content, by reference to one or more specific provisions of Union law or national law in compliance with Union law;
    - (iii) information identifying the issuing authority;
    - (iv) clear information enabling the provider of intermediary services to identify and locate the illegal content concerned, such as one or more exact URL and, where necessary, additional information;
    - (v) information about redress mechanisms available to the provider of intermediary services and to the recipient of the service who provided the content;
    - (vi) where applicable, information about which authority is to receive the information about the effect given to the orders;
  - (b) the territorial scope of that order, on the basis of the applicable rules of Union and national law, including the Charter, and, where relevant, general principles of international law, is limited to what is strictly necessary to achieve its objective;
  - (c) that order is transmitted in one of the languages declared by the provider of intermediary services pursuant to Article 11(3) or in another official language of the Member States, agreed between the authority issuing the order and that provider, and is sent to the electronic point of contact designated by that provider, in accordance with Article 11; where the order is not drafted in the language declared by the provider of intermediary services or in another bilaterally agreed language, the order may be transmitted in the language of the authority issuing the order, provided that it is accompanied by a translation into such declared or bilaterally agreed language of at least the elements set out in points (a) and (b) of this paragraph.
3. The authority issuing the order or, where applicable, the authority specified therein, shall transmit it, along with any information received from the provider of intermediary services concerning the effect given to that order to the Digital Services Coordinator from the Member State of the issuing authority.
4. After receiving the order from the judicial or administrative authority, the Digital Services Coordinator of the Member State concerned shall, without undue delay, transmit a copy of the order referred to in paragraph 1 of this Article to all other Digital Services Coordinators through the system established in accordance with Article 85.
5. At the latest when effect is given to the order or, where applicable, at the time provided by the issuing authority in its order, providers of intermediary services shall inform the recipient of the service concerned of the order received and to the effect given to it. Such information provided to the recipient of the service shall include a statement of reasons, the possibilities for redress that exist, and a description of the territorial scope of the order, in accordance with paragraph 2.

6. The conditions and requirements laid down in this Article shall be without prejudice to national civil and criminal procedural law.

#### Article 10

### Orders to provide information

1. Upon receipt of an order to provide specific information about one or more specific individual recipients of the service, issued by the relevant national judicial or administrative authorities on the basis of the applicable Union law or national law in compliance with Union law, providers of intermediary services shall, without undue delay inform the authority issuing the order, or any other authority specified in the order, of its receipt and of the effect given to the order, specifying if and when effect was given to the order.

2. Member States shall ensure that when an order referred to in paragraph 1 is transmitted to the provider, it meets at least the following conditions:

(a) that order contains the following elements:

- (i) a reference to the legal basis under Union or national law for the order;
- (ii) information identifying the issuing authority;
- (iii) clear information enabling the provider of intermediary services to identify the specific recipient or recipients on whom information is sought, such as one or more account names or unique identifiers;
- (iv) a statement of reasons explaining the objective for which the information is required and why the requirement to provide the information is necessary and proportionate to determine compliance by the recipients of the intermediary services with applicable Union law or national law in compliance with Union law, unless such a statement cannot be provided for reasons related to the prevention, investigation, detection and prosecution of criminal offences;
- (v) information about redress mechanisms available to the provider and to the recipients of the service concerned;
- (vi) where applicable, information about which authority is to receive the information about the effect given to the orders;

(b) that order only requires the provider to provide information already collected for the purposes of providing the service and which lies within its control;

(c) that order is transmitted in one of the languages declared by the provider of intermediary services pursuant to Article 11(3) or in another official language of the Member States, agreed between the authority issuing the order and the provider, and is sent to the electronic point of contact designated by that provider, in accordance with Article 11; where the order is not drafted in the language declared by the provider of intermediary services or in another bilaterally agreed language, the order may be transmitted in the language of the authority issuing the order, provided that it is accompanied by a translation into such declared or bilaterally agreed language of at least the elements set out in points (a) and (b) of this paragraph.

3. The authority issuing the order or, where applicable, the authority specified therein, shall transmit it, along with any information received from the provider of intermediary services concerning the effect given to that order to the Digital Services Coordinator from the Member State of the issuing authority.

4. After receiving the order from the judicial or administrative authority, the Digital Services Coordinator of the Member State concerned shall, without undue delay, transmit a copy of the order referred to in paragraph 1 of this Article to all Digital Services Coordinators through the system established in accordance with Article 85.

5. At the latest when effect is given to the order, or, where applicable, at the time provided by the issuing authority in its order, providers of intermediary services shall inform the recipient of the service concerned of the order received and the effect given to it. Such information provided to the recipient of the service shall include a statement of reasons and the possibilities for redress that exist, in accordance with paragraph 2.

6. The conditions and requirements laid down in this Article shall be without prejudice to national civil and criminal procedural law.

### CHAPTER III

#### DUE DILIGENCE OBLIGATIONS FOR A TRANSPARENT AND SAFE ONLINE ENVIRONMENT

##### SECTION 1

##### *Provisions applicable to all providers of intermediary services*

###### Article 11

##### **Points of contact for Member States' authorities, the Commission and the Board**

1. Providers of intermediary services shall designate a single point of contact to enable them to communicate directly, by electronic means, with Member States' authorities, the Commission and the Board referred to in Article 61 for the application of this Regulation.
2. Providers of intermediary services shall make public the information necessary to easily identify and communicate with their single points of contact. That information shall be easily accessible, and shall be kept up to date.
3. Providers of intermediary services shall specify in the information referred to in paragraph 2 the official language or languages of the Member States which, in addition to a language broadly understood by the largest possible number of Union citizens, can be used to communicate with their points of contact, and which shall include at least one of the official languages of the Member State in which the provider of intermediary services has its main establishment or where its legal representative resides or is established.

###### Article 12

##### **Points of contact for recipients of the service**

1. Providers of intermediary services shall designate a single point of contact to enable recipients of the service to communicate directly and rapidly with them, by electronic means and in a user-friendly manner, including by allowing recipients of the service to choose the means of communication, which shall not solely rely on automated tools.
2. In addition to the obligations provided under Directive 2000/31/EC, providers of intermediary services shall make public the information necessary for the recipients of the service in order to easily identify and communicate with their single points of contact. That information shall be easily accessible, and shall be kept up to date.

###### Article 13

##### **Legal representatives**

1. Providers of intermediary services which do not have an establishment in the Union but which offer services in the Union shall designate, in writing, a legal or natural person to act as their legal representative in one of the Member States where the provider offers its services.

2. Providers of intermediary services shall mandate their legal representatives for the purpose of being addressed in addition to or instead of such providers, by the Member States' competent authorities, the Commission and the Board, on all issues necessary for the receipt of, compliance with and enforcement of decisions issued in relation to this Regulation. Providers of intermediary services shall provide their legal representative with necessary powers and sufficient resources to guarantee their efficient and timely cooperation with the Member States' competent authorities, the Commission and the Board, and to comply with such decisions.
3. It shall be possible for the designated legal representative to 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 provider of intermediary services.
4. Providers of intermediary services shall notify the name, postal address, email address and telephone number of their legal representative to the Digital Services Coordinator in the Member State where that legal representative resides or is established. They shall ensure that that information is publicly available, easily accessible, accurate and kept up to date.
5. The designation of a legal representative within the Union pursuant to paragraph 1 shall not constitute an establishment in the Union.

#### Article 14

##### **Terms and conditions**

1. Providers of intermediary services shall include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions. That information shall include information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review, as well as the rules of procedure of their internal complaint handling system. It shall be set out in clear, plain, intelligible, user-friendly and unambiguous language, and shall be publicly available in an easily accessible and machine-readable format.
2. Providers of intermediary services shall inform the recipients of the service of any significant change to the terms and conditions.
3. Where an intermediary service is primarily directed at minors or is predominantly used by them, the provider of that intermediary service shall explain the conditions for, and any restrictions on, the use of the service in a way that minors can understand.
4. Providers of intermediary services shall act in a diligent, objective and proportionate manner in applying and enforcing the restrictions referred to in paragraph 1, with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service, such as the freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms as enshrined in the Charter.
5. Providers of very large online platforms and of very large online search engines shall provide recipients of services with a concise, easily-accessible and machine-readable summary of the terms and conditions, including the available remedies and redress mechanisms, in clear and unambiguous language.
6. Very large online platforms and very large online search engines within the meaning of Article 33 shall publish their terms and conditions in the official languages of all the Member States in which they offer their services.

#### Article 15

##### **Transparency reporting obligations for providers of intermediary services**

1. Providers of intermediary services shall make publicly available, in a machine-readable format and in an easily accessible manner, at least once a year, clear, easily comprehensible reports on any content moderation that they engaged in during the relevant period. Those reports shall include, in particular, information on the following, as applicable:

- (a) for providers of intermediary services, the number of orders received from Member States' authorities including orders issued in accordance with Articles 9 and 10, categorised by the type of illegal content concerned, the Member State issuing the order, and the median time needed to inform the authority issuing the order, or any other authority specified in the order, of its receipt, and to give effect to the order;
- (b) for providers of hosting services, the number of notices submitted in accordance with Article 16, categorised by the type of alleged illegal content concerned, the number of notices submitted by trusted flaggers, any action taken pursuant to the notices by differentiating whether the action was taken on the basis of the law or the terms and conditions of the provider, the number of notices processed by using automated means and the median time needed for taking the action;
- (c) for providers of intermediary services, meaningful and comprehensible information about the content moderation engaged in at the providers' own initiative, including the use of automated tools, the measures taken to provide training and assistance to persons in charge of content moderation, the number and type of measures taken that affect the availability, visibility and accessibility of information provided by the recipients of the service and the recipients' ability to provide information through the service, and other related restrictions of the service; the information reported shall be categorised by the type of illegal content or violation of the terms and conditions of the service provider, by the detection method and by the type of restriction applied;
- (d) for providers of intermediary services, the number of complaints received through the internal complaint-handling systems in accordance with the provider's terms and conditions and additionally, for providers of online platforms, in accordance with Article 20, the basis for those complaints, decisions taken in respect of those complaints, the median time needed for taking those decisions and the number of instances where those decisions were reversed;
- (e) any use made of automated means for the purpose of content moderation, including a qualitative description, a specification of the precise purposes, indicators of the accuracy and the possible rate of error of the automated means used in fulfilling those purposes, and any safeguards applied.

2. Paragraph 1 of this Article shall not apply to providers of intermediary services that qualify as micro or small enterprises as defined in Recommendation 2003/361/EC and which are not very large online platforms within the meaning of Article 33 of this Regulation.

3. The Commission may adopt implementing acts to lay down templates concerning the form, content and other details of reports pursuant to paragraph 1 of this Article, including harmonised reporting periods. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 88.

## SECTION 2

### *Additional provisions applicable to providers of hosting services, including online platforms*

#### Article 16

##### **Notice and action mechanisms**

1. Providers of hosting services shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content. Those mechanisms shall be easy to access and user-friendly, and shall allow for the submission of notices exclusively by electronic means.

2. The mechanisms referred to in paragraph 1 shall be such as to facilitate the submission of sufficiently precise and adequately substantiated notices. To that end, the providers of hosting services shall take the necessary measures to enable and to facilitate the submission of notices containing all of the following elements:

- (a) a sufficiently substantiated explanation of the reasons why the individual or entity alleges the information in question to be illegal content;
- (b) a clear indication of the exact electronic location of that information, such as the exact URL or URLs, and, where necessary, additional information enabling the identification of the illegal content adapted to the type of content and to the specific type of hosting service;
- (c) the name and email address of the individual or entity submitting the notice, except in the case of information considered to involve one of the offences referred to in Articles 3 to 7 of Directive 2011/93/EU;
- (d) a statement confirming the bona fide belief of the individual or entity submitting the notice that the information and allegations contained therein are accurate and complete.

3. Notices referred to in this Article shall be considered to give rise to actual knowledge or awareness for the purposes of Article 6 in respect of the specific item of information concerned where they allow a diligent provider of hosting services to identify the illegality of the relevant activity or information without a detailed legal examination.

4. Where the notice contains the electronic contact information of the individual or entity that submitted it, the provider of hosting services shall, without undue delay, send a confirmation of receipt of the notice to that individual or entity.

5. The provider shall also, without undue delay, notify that individual or entity of its decision in respect of the information to which the notice relates, providing information on the possibilities for redress in respect of that decision.

6. Providers of hosting services shall process any notices that they receive under the mechanisms referred to in paragraph 1 and take their decisions in respect of the information to which the notices relate, in a timely, diligent, non-arbitrary and objective manner. Where they use automated means for that processing or decision-making, they shall include information on such use in the notification referred to in paragraph 5.

#### *Article 17*

#### **Statement of reasons**

1. Providers of hosting services shall provide a clear and specific statement of reasons to any affected recipients of the service for any of the following restrictions imposed on the ground that the information provided by the recipient of the service is illegal content or incompatible with their terms and conditions:

- (a) any restrictions of the visibility of specific items of information provided by the recipient of the service, including removal of content, disabling access to content, or demoting content;
- (b) suspension, termination or other restriction of monetary payments;
- (c) suspension or termination of the provision of the service in whole or in part;
- (d) suspension or termination of the recipient of the service's account.

2. Paragraph 1 shall only apply where the relevant electronic contact details are known to the provider. It shall apply at the latest from the date that the restriction is imposed, regardless of why or how it was imposed.

Paragraph 1 shall not apply where the information is deceptive high-volume commercial content.

3. The statement of reasons referred to in paragraph 1 shall at least contain the following information:
  - (a) information on whether the decision entails either the removal of, the disabling of access to, the demotion of or the restriction of the visibility of the information, or the suspension or termination of monetary payments related to that information, or imposes other measures referred to in paragraph 1 with regard to the information, and, where relevant, the territorial scope of the decision and its duration;
  - (b) the facts and circumstances relied on in taking the decision, including, where relevant, information on whether the decision was taken pursuant to a notice submitted in accordance with Article 16 or based on voluntary own-initiative investigations and, where strictly necessary, the identity of the notifier;
  - (c) where applicable, information on the use made of automated means in taking the decision, including information on whether the decision was taken in respect of content detected or identified using automated means;
  - (d) where the decision concerns allegedly illegal content, a reference to the legal ground relied on and explanations as to why the information is considered to be illegal content on that ground;
  - (e) where the decision is based on the alleged incompatibility of the information with the terms and conditions of the provider of hosting services, a reference to the contractual ground relied on and explanations as to why the information is considered to be incompatible with that ground;
  - (f) clear and user-friendly information on the possibilities for redress available to the recipient of the service in respect of the decision, in particular, where applicable through internal complaint-handling mechanisms, out-of-court dispute settlement and judicial redress.
4. The information provided by the providers of hosting services in accordance with this Article shall be clear and easily comprehensible and as precise and specific as reasonably possible under the given circumstances. The information shall, in particular, be such as to reasonably allow the recipient of the service concerned to effectively exercise the possibilities for redress referred to in of paragraph 3, point (f).
5. This Article shall not apply to any orders referred to in Article 9.

#### Article 18

#### **Notification of suspicions of criminal offences**

1. Where a provider of hosting services becomes aware of any information giving rise to a suspicion that a criminal offence involving a threat to the life or safety of a person or persons has taken place, is taking place or is likely to take place, it shall promptly inform the law enforcement or judicial authorities of the Member State or Member States concerned of its suspicion and provide all relevant information available.
2. Where the provider of hosting services cannot identify with reasonable certainty the Member State concerned, it shall inform the law enforcement authorities of the Member State in which it is established or where its legal representative resides or is established or inform Europol, or both.

For the purpose of this Article, the Member State concerned shall be the Member State in which the offence is suspected to have taken place, to be taking place or to be likely to take place, or the Member State where the suspected offender resides or is located, or the Member State where the victim of the suspected offence resides or is located.

## SECTION 3

***Additional provisions applicable to providers of online platforms****Article 19***Exclusion for micro and small enterprises**

1. This Section, with the exception of Article 24(3) thereof, shall not apply to providers of online platforms that qualify as micro or small enterprises as defined in Recommendation 2003/361/EC.

This Section, with the exception of Article 24(3) thereof, shall not apply to providers of online platforms that previously qualified for the status of a micro or small enterprise as defined in Recommendation 2003/361/EC during the 12 months following their loss of that status pursuant to Article 4(2) thereof, except when they are very large online platforms in accordance with Article 33.

2. By derogation from paragraph 1 of this Article, this Section shall apply to providers of online platforms that have been designated as very large online platforms in accordance with Article 33, irrespective of whether they qualify as micro or small enterprises.

*Article 20***Internal complaint-handling system**

1. Providers of online platforms shall provide recipients of the service, including individuals or entities that have submitted a notice, for a period of at least six months following the decision referred to in this paragraph, with access to an effective internal complaint-handling system that enables them to lodge complaints, electronically and free of charge, against the decision taken by the provider of the online platform upon the receipt of a notice or against the following decisions taken by the provider of the online platform on the grounds that the information provided by the recipients constitutes illegal content or is incompatible with its terms and conditions:

- (a) decisions whether or not to remove or disable access to or restrict visibility of the information;
- (b) decisions whether or not to suspend or terminate the provision of the service, in whole or in part, to the recipients;
- (c) decisions whether or not to suspend or terminate the recipients' account;
- (d) decisions whether or not to suspend, terminate or otherwise restrict the ability to monetise information provided by the recipients.

2. The period of at least six months referred to in paragraph 1 of this Article shall start on the day on which the recipient of the service is informed about the decision in accordance with Article 16(5) or Article 17.

3. Providers of online platforms shall ensure that their internal complaint-handling systems are easy to access, user-friendly and enable and facilitate the submission of sufficiently precise and adequately substantiated complaints.

4. Providers of online platforms shall handle complaints submitted through their internal complaint-handling system in a timely, non-discriminatory, diligent and non-arbitrary manner. Where a complaint contains sufficient grounds for the provider of the online platform to consider that its decision not to act upon the notice is unfounded or that the information to which the complaint relates is not illegal and is not incompatible with its terms and conditions, or contains information indicating that the complainant's conduct does not warrant the measure taken, it shall reverse its decision referred to in paragraph 1 without undue delay.

5. Providers of online platforms shall inform complainants without undue delay of their reasoned decision in respect of the information to which the complaint relates and of the possibility of out-of-court dispute settlement provided for in Article 21 and other available possibilities for redress.

6. Providers of online platforms shall ensure that the decisions, referred to in paragraph 5, are taken under the supervision of appropriately qualified staff, and not solely on the basis of automated means.

#### Article 21

### Out-of-court dispute settlement

1. Recipients of the service, including individuals or entities that have submitted notices, addressed by the decisions referred to in Article 20(1) shall be entitled to select any out-of-court dispute settlement body that has been certified in accordance with paragraph 3 of this Article in order to resolve disputes relating to those decisions, including complaints that have not been resolved by means of the internal complaint-handling system referred to in that Article.

Providers of online platforms shall ensure that information about the possibility for recipients of the service to have access to an out-of-court dispute settlement, as referred to in the first subparagraph, is easily accessible on their online interface, clear and user-friendly.

The first subparagraph is without prejudice to the right of the recipient of the service concerned to initiate, at any stage, proceedings to contest those decisions by the providers of online platforms before a court in accordance with the applicable law.

2. Both parties shall engage, in good faith, with the selected certified out-of-court dispute settlement body with a view to resolving the dispute.

Providers of online platforms may refuse to engage with such out-of-court dispute settlement body if a dispute has already been resolved concerning the same information and the same grounds of alleged illegality or incompatibility of content.

The certified out-of-court dispute settlement body shall not have the power to impose a binding settlement of the dispute on the parties.

3. The Digital Services Coordinator of the Member State where the out-of-court dispute settlement body is established shall, for a maximum period of five years, which may be renewed, certify the body, at its request, where the body has demonstrated that it meets all of the following conditions:

- (a) it is impartial and independent, including financially independent, of providers of online platforms and of recipients of the service provided by providers of online platforms, including of individuals or entities that have submitted notices;
- (b) it has the necessary expertise in relation to the issues arising in one or more particular areas of illegal content, or in relation to the application and enforcement of terms and conditions of one or more types of online platform, allowing the body to contribute effectively to the settlement of a dispute;
- (c) its members are remunerated in a way that is not linked to the outcome of the procedure;
- (d) the out-of-court dispute settlement that it offers is easily accessible, through electronic communications technology and provides for the possibility to initiate the dispute settlement and to submit the requisite supporting documents online;
- (e) it is capable of settling disputes in a swift, efficient and cost-effective manner and in at least one of the official languages of the institutions of the Union;
- (f) the out-of-court dispute settlement that it offers takes place in accordance with clear and fair rules of procedure that are easily and publicly accessible, and that comply with applicable law, including this Article.

The Digital Services Coordinator shall, where applicable, specify in the certificate:

- (a) the particular issues to which the body's expertise relates, as referred to in point (b) of the first subparagraph; and
- (b) the official language or languages of the institutions of the Union in which the body is capable of settling disputes, as referred to in point (e) of the first subparagraph.

4. Certified out-of-court dispute settlement bodies shall report to the Digital Services Coordinator that certified them, on an annual basis, on their functioning, specifying at least the number of disputes they received, the information about the outcomes of those disputes, the average time taken to resolve them and any shortcomings or difficulties encountered. They shall provide additional information at the request of that Digital Services Coordinator.

Digital Services Coordinators shall, every two years, draw up a report on the functioning of the out-of-court dispute settlement bodies that they certified. That report shall in particular:

- (a) list the number of disputes that each certified out-of-court dispute settlement body has received annually;
- (b) indicate the outcomes of the procedures brought before those bodies and the average time taken to resolve the disputes;
- (c) identify and explain any systematic or sectoral shortcomings or difficulties encountered in relation to the functioning of those bodies;
- (d) identify best practices concerning that functioning;
- (e) make recommendations as to how to improve that functioning, where appropriate.

Certified out-of-court dispute settlement bodies shall make their decisions available to the parties within a reasonable period of time and no later than 90 calendar days after the receipt of the complaint. In the case of highly complex disputes, the certified out-of-court dispute settlement body may, at its own discretion, extend the 90 calendar day period for an additional period that shall not exceed 90 days, resulting in a maximum total duration of 180 days.

5. If the out-of-court dispute settlement body decides the dispute in favour of the recipient of the service, including the individual or entity that has submitted a notice, the provider of the online platform shall bear all the fees charged by the out-of-court dispute settlement body, and shall reimburse that recipient, including the individual or entity, for any other reasonable expenses that it has paid in relation to the dispute settlement. If the out-of-court dispute settlement body decides the dispute in favour of the provider of the online platform, the recipient of the service, including the individual or entity, shall not be required to reimburse any fees or other expenses that the provider of the online platform paid or is to pay in relation to the dispute settlement, unless the out-of-court dispute settlement body finds that that recipient manifestly acted in bad faith.

The fees charged by the out-of-court dispute settlement body to the providers of online platforms for the dispute settlement shall be reasonable and shall in any event not exceed the costs incurred by the body. For recipients of the service, the dispute settlement shall be available free of charge or at a nominal fee.

Certified out-of-court dispute settlement bodies shall make the fees, or the mechanisms used to determine the fees, known to the recipient of the service, including to the individuals or entities that have submitted a notice, and to the provider of the online platform concerned, before engaging in the dispute settlement.

6. Member States may establish out-of-court dispute settlement bodies for the purposes of paragraph 1 or support the activities of some or all out-of-court dispute settlement bodies that they have certified in accordance with paragraph 3.

Member States shall ensure that any of their activities undertaken under the first subparagraph do not affect the ability of their Digital Services Coordinators to certify the bodies concerned in accordance with paragraph 3.

7. A Digital Services Coordinator that has certified an out-of-court dispute settlement body shall revoke that certification if it determines, following an investigation either on its own initiative or on the basis of the information received by third parties, that the out-of-court dispute settlement body no longer meets the conditions set out in paragraph 3. Before revoking that certification, the Digital Services Coordinator shall afford that body an opportunity to react to the findings of its investigation and its intention to revoke the out-of-court dispute settlement body's certification.

8. Digital Services Coordinators shall notify to the Commission the out-of-court dispute settlement bodies that they have certified in accordance with paragraph 3, including where applicable the specifications referred to in the second subparagraph of that paragraph, as well as the out-of-court dispute settlement bodies the certification of which they have revoked. The Commission shall publish a list of those bodies, including those specifications, on a dedicated website that is easily accessible, and keep it up to date.

9. This Article is without prejudice to Directive 2013/11/EU and alternative dispute resolution procedures and entities for consumers established under that Directive.

## Article 22

### Trusted flaggers

1. Providers of online platforms shall take the necessary technical and organisational measures to ensure that notices submitted by trusted flaggers, acting within their designated area of expertise, through the mechanisms referred to in Article 16, are given priority and are processed and decided upon without undue delay.

2. The status of 'trusted flagger' under this Regulation shall be awarded, upon application by any entity, by the Digital Services Coordinator of the Member State in which the applicant is established, to an applicant that has demonstrated that it meets all of the following conditions:

- (a) it has particular expertise and competence for the purposes of detecting, identifying and notifying illegal content;
- (b) it is independent from any provider of online platforms;
- (c) it carries out its activities for the purposes of submitting notices diligently, accurately and objectively.

3. Trusted flaggers shall publish, at least once a year easily comprehensible and detailed reports on notices submitted in accordance with Article 16 during the relevant period. The report shall list at least the number of notices categorised by:

- (a) the identity of the provider of hosting services,
- (b) the type of allegedly illegal content notified,
- (c) the action taken by the provider.

Those reports shall include an explanation of the procedures in place to ensure that the trusted flagger retains its independence.

Trusted flaggers shall send those reports to the awarding Digital Services Coordinator, and shall make them publicly available. The information in those reports shall not contain personal data.

4. Digital Services Coordinators shall communicate to the Commission and the Board the names, addresses and email addresses of the entities to which they have awarded the status of the trusted flagger in accordance with paragraph 2 or whose trusted flagger status they have suspended in accordance with paragraph 6 or revoked in accordance with paragraph 7.

5. The Commission shall publish the information referred to in paragraph 4 in a publicly available database, in an easily accessible and machine-readable format, and shall keep the database up to date.

6. Where a provider of online platforms has information indicating that a trusted flagger has submitted a significant number of insufficiently precise, inaccurate or inadequately substantiated notices through the mechanisms referred to in Article 16, including information gathered in connection to the processing of complaints through the internal complaint-handling systems referred to in Article 20(4), it shall communicate that information to the Digital Services Coordinator that awarded the status of trusted flagger to the entity concerned, providing the necessary explanations and supporting documents. Upon receiving the information from the provider of online platforms, and if the Digital Services Coordinator considers that there are legitimate reasons to open an investigation, the status of trusted flagger shall be suspended during the period of the investigation. That investigation shall be carried out without undue delay.

7. The Digital Services Coordinator that awarded the status of trusted flagger to an entity shall revoke that status if it determines, following an investigation either on its own initiative or on the basis information received from third parties, including the information provided by a provider of online platforms pursuant to paragraph 6, that the entity no longer meets the conditions set out in paragraph 2. Before revoking that status, the Digital Services Coordinator shall afford the entity an opportunity to react to the findings of its investigation and its intention to revoke the entity's status as trusted flagger.

8. The Commission, after consulting the Board, shall, where necessary, issue guidelines to assist providers of online platforms and Digital Services Coordinators in the application of paragraphs 2, 6 and 7.

#### Article 23

### Measures and protection against misuse

1. Providers of online platforms shall suspend, for a reasonable period of time and after having issued a prior warning, the provision of their services to recipients of the service that frequently provide manifestly illegal content.

2. Providers of online platforms shall suspend, for a reasonable period of time and after having issued a prior warning, the processing of notices and complaints submitted through the notice and action mechanisms and internal complaints-handling systems referred to in Articles 16 and 20, respectively, by individuals or entities or by complainants that frequently submit notices or complaints that are manifestly unfounded.

3. When deciding on suspension, providers of online platforms shall assess, on a case-by-case basis and in a timely, diligent and objective manner, whether the recipient of the service, the individual, the entity or the complainant engages in the misuse referred to in paragraphs 1 and 2, taking into account all relevant facts and circumstances apparent from the information available to the provider of online platforms. Those circumstances shall include at least the following:

- (a) the absolute numbers of items of manifestly illegal content or manifestly unfounded notices or complaints, submitted within a given time frame;
- (b) the relative proportion thereof in relation to the total number of items of information provided or notices submitted within a given time frame;
- (c) the gravity of the misuses, including the nature of illegal content, and of its consequences;
- (d) where it is possible to identify it, the intention of the recipient of the service, the individual, the entity or the complainant.

4. Providers of online platforms shall set out, in a clear and detailed manner, in their terms and conditions their policy in respect of the misuse referred to in paragraphs 1 and 2, and shall give examples of the facts and circumstances that they take into account when assessing whether certain behaviour constitutes misuse and the duration of the suspension.

*Article 24***Transparency reporting obligations for providers of online platforms**

1. In addition to the information referred to in Article 15, providers of online platforms shall include in the reports referred to in that Article information on the following:
  - (a) the number of disputes submitted to the out-of-court dispute settlement bodies referred to in Article 21, the outcomes of the dispute settlement, and the median time needed for completing the dispute settlement procedures, as well as the share of disputes where the provider of the online platform implemented the decisions of the body;
  - (b) the number of suspensions imposed pursuant to Article 23, distinguishing between suspensions enacted for the provision of manifestly illegal content, the submission of manifestly unfounded notices and the submission of manifestly unfounded complaints.
2. By 17 February 2023 and at least once every six months thereafter, providers shall publish for each online platform or online search engine, in a publicly available section of their online interface, information on the average monthly active recipients of the service in the Union, calculated as an average over the period of the past six months and in accordance with the methodology laid down in the delegated acts referred to in Article 33(3), where those delegated acts have been adopted.
3. Providers of online platforms or of online search engines shall communicate to the Digital Services Coordinator of establishment and the Commission, upon their request and without undue delay, the information referred to in paragraph 2, updated to the moment of such request. That Digital Services Coordinator or the Commission may require the provider of the online platform or of the online search engine to provide additional information as regards the calculation referred to in that paragraph, including explanations and substantiation in respect of the data used. That information shall not include personal data.
4. When the Digital Services Coordinator of establishment has reasons to consider, based the information received pursuant to paragraphs 2 and 3 of this Article, that a provider of online platforms or of online search engines meets the threshold of average monthly active recipients of the service in the Union laid down in Article 33(1), it shall inform the Commission thereof.
5. Providers of online platforms shall, without undue delay, submit to the Commission the decisions and the statements of reasons referred to in Article 17(1) for the inclusion in a publicly accessible machine-readable database managed by the Commission. Providers of online platforms shall ensure that the information submitted does not contain personal data.
6. The Commission may adopt implementing acts to lay down templates concerning the form, content and other details of reports pursuant to paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 88.

*Article 25***Online interface design and organisation**

1. Providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions.
2. The prohibition in paragraph 1 shall not apply to practices covered by Directive 2005/29/EC or Regulation (EU) 2016/679.
3. The Commission may issue guidelines on how paragraph 1 applies to specific practices, notably:
  - (a) giving more prominence to certain choices when asking the recipient of the service for a decision;

- (b) repeatedly requesting that the recipient of the service make a choice where that choice has already been made, especially by presenting pop-ups that interfere with the user experience;
- (c) making the procedure for terminating a service more difficult than subscribing to it.

#### Article 26

### Advertising on online platforms

1. Providers of online platforms that present advertisements on their online interfaces shall ensure that, for each specific advertisement presented to each individual recipient, the recipients of the service are able to identify, in a clear, concise and unambiguous manner and in real time, the following:

- (a) that the information is an advertisement, including through prominent markings, which might follow standards pursuant to Article 44;
- (b) the natural or legal person on whose behalf the advertisement is presented;
- (c) the natural or legal person who paid for the advertisement if that person is different from the natural or legal person referred to in point (b);
- (d) meaningful information directly and easily accessible from the advertisement about the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, about how to change those parameters.

2. Providers of online platforms shall provide recipients of the service with a functionality to declare whether the content they provide is or contains commercial communications.

When the recipient of the service submits a declaration pursuant to this paragraph, the provider of online platforms shall ensure that other recipients of the service can identify in a clear and unambiguous manner and in real time, including through prominent markings, which might follow standards pursuant to Article 44, that the content provided by the recipient of the service is or contains commercial communications, as described in that declaration.

3. Providers of online platforms shall not present advertisements to recipients of the service based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679.

#### Article 27

### Recommender system transparency

1. Providers of online platforms that use recommender systems shall set out in their terms and conditions, in plain and intelligible language, the main parameters used in their recommender systems, as well as any options for the recipients of the service to modify or influence those main parameters.

2. The main parameters referred to in paragraph 1 shall explain why certain information is suggested to the recipient of the service. They shall include, at least:

- (a) the criteria which are most significant in determining the information suggested to the recipient of the service;
- (b) the reasons for the relative importance of those parameters.

3. Where several options are available pursuant to paragraph 1 for recommender systems that determine the relative order of information presented to recipients of the service, providers of online platforms shall also make available a functionality that allows the recipient of the service to select and to modify at any time their preferred option. That functionality shall be directly and easily accessible from the specific section of the online platform's online interface where the information is being prioritised.

*Article 28***Online protection of minors**

1. Providers of online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service.
2. Providers of online platform shall not present advertisements on their interface based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor.
3. Compliance with the obligations set out in this Article shall not oblige providers of online platforms to process additional personal data in order to assess whether the recipient of the service is a minor.
4. The Commission, after consulting the Board, may issue guidelines to assist providers of online platforms in the application of paragraph 1.

## SECTION 4

***Additional provisions applicable to providers of online platforms allowing consumers to conclude distance contracts with traders****Article 29***Exclusion for micro and small enterprises**

1. This Section shall not apply to providers of online platforms allowing consumers to conclude distance contracts with traders that qualify as micro or small enterprises as defined in Recommendation 2003/361/EC.

This Section shall not apply to providers of online platforms allowing consumers to conclude distance contracts with traders that previously qualified for the status of a micro or small enterprise as defined in Recommendation 2003/361/EC during the 12 months following their loss of that status pursuant to Article 4(2) thereof, except when they are very large online platforms in accordance with Article 33.

2. By derogation from paragraph 1 of this Article, this Section shall apply to providers of online platforms allowing consumers to conclude distance contracts with traders that have been designated as very large online platforms in accordance with Article 33, irrespective of whether they qualify as micro or small enterprises.

*Article 30***Traceability of traders**

1. Providers of online platforms allowing consumers to conclude distance contracts with traders shall ensure that traders can only use those online platforms to promote messages on or to offer products or services to consumers located in the Union if, prior to the use of their services for those purposes, they have obtained the following information, where applicable to the trader:

- (a) the name, address, telephone number and email address of the trader;
- (b) a copy of the identification document of the trader or any other electronic identification as defined by Article 3 of Regulation (EU) No 910/2014 of the European Parliament and of the Council <sup>(40)</sup>;

<sup>(40)</sup> Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

- (c) the payment account details of the trader;
- (d) where the trader is registered in a trade register or similar public register, the trade register in which the trader is registered and its registration number or equivalent means of identification in that register;
- (e) a self-certification by the trader committing to only offer products or services that comply with the applicable rules of Union law.

2. Upon receiving the information referred to in paragraph 1 and prior to allowing the trader concerned to use its services, the provider of the online platform allowing consumers to conclude distance contracts with traders shall, through the use of any freely accessible official online database or online interface made available by a Member State or the Union or through requests to the trader to provide supporting documents from reliable sources, make best efforts to assess whether the information referred to in paragraph 1, points (a) to (e), is reliable and complete. For the purpose of this Regulation, traders shall be liable for the accuracy of the information provided.

As regards traders that are already using the services of providers of online platforms allowing consumers to conclude distance contracts with traders for the purposes referred to in paragraph 1 on 17 February 2024, the providers shall make best efforts to obtain the information listed from the traders concerned within 12 months. Where the traders concerned fail to provide the information within that period, the providers shall suspend the provision of their services to those traders until they have provided all information.

3. Where the provider of the online platform allowing consumers to conclude distance contracts with traders obtains sufficient indications or has reason to believe that any item of information referred to in paragraph 1 obtained from the trader concerned is inaccurate, incomplete or not up-to-date, that provider shall request that the trader remedy that situation without delay or within the period set by Union and national law.

Where the trader fails to correct or complete that information, the provider of the online platform allowing consumers to conclude distance contracts with traders shall swiftly suspend the provision of its service to that trader in relation to the offering of products or services to consumers located in the Union until the request has been fully complied with.

4. Without prejudice to Article 4 of Regulation (EU) 2019/1150, if a provider of an online platform allowing consumers to conclude distance contracts with traders refuses to allow a trader to use its service pursuant to paragraph 1, or suspends the provision of its service pursuant to paragraph 3 of this Article, the trader concerned shall have the right to lodge a complaint as provided for in Articles 20 and 21 of this Regulation.

5. Providers of online platforms allowing consumers to conclude distance contracts with traders shall store the information obtained pursuant to paragraphs 1 and 2 in a secure manner for a period of six months after the end of the contractual relationship with the trader concerned. They shall subsequently delete the information.

6. Without prejudice to paragraph 2 of this Article, the provider of the online platform allowing consumers to conclude distance contracts with traders shall only disclose the information to third parties where so required in accordance with the applicable law, including the orders referred to in Article 10 and any orders issued by Member States' competent authorities or the Commission for the performance of their tasks under this Regulation.

7. The provider of the online platform allowing consumers to conclude distance contracts with traders shall make the information referred to in paragraph 1, points (a), (d) and (e) available on its online platform to the recipients of the service in a clear, easily accessible and comprehensible manner. That information shall be available at least on the online platform's online interface where the information on the product or service is presented.

*Article 31***Compliance by design**

1. Providers of online platforms allowing consumers to conclude distance contracts with traders shall ensure that its online interface is designed and organised in a way that enables traders to comply with their obligations regarding pre-contractual information, compliance and product safety information under applicable Union law.

In particular, the provider concerned shall ensure that its online interface enables traders to provide information on the name, address, telephone number and email address of the economic operator, as defined in Article 3, point (13), of Regulation (EU) 2019/1020 and other Union law.

2. Providers of online platforms allowing consumers to conclude distance contracts with traders shall ensure that its online interface is designed and organised in a way that it allows traders to provide at least the following:

- (a) the information necessary for the clear and unambiguous identification of the products or the services promoted or offered to consumers located in the Union through the services of the providers;
- (b) any sign identifying the trader such as the trademark, symbol or logo; and,
- (c) where applicable, the information concerning the labelling and marking in compliance with rules of applicable Union law on product safety and product compliance.

3. Providers of online platforms allowing consumers to conclude distance contracts with traders shall make best efforts to assess whether such traders have provided the information referred to in paragraphs 1 and 2 prior to allowing them to offer their products or services on those platforms. After allowing the trader to offer products or services on its online platform that allows consumers to conclude distance contracts with traders, the provider shall make reasonable efforts to randomly check in any official, freely accessible and machine-readable online database or online interface whether the products or services offered have been identified as illegal.

*Article 32***Right to information**

1. Where a provider of an online platform allowing consumers to conclude distance contracts with traders becomes aware, irrespective of the means used, that an illegal product or service has been offered by a trader to consumers located in the Union through its services, that provider shall inform, insofar as it has their contact details, consumers who purchased the illegal product or service through its services of the following:

- (a) the fact that the product or service is illegal;
- (b) the identity of the trader; and
- (c) any relevant means of redress.

The obligation laid down in the first subparagraph shall be limited to purchases of illegal products or services made within the six months preceding the moment that the provider became aware of the illegality.

2. Where, in the situation referred to in paragraph 1, the provider of the online platform allowing consumers to conclude distance contracts with traders does not have the contact details of all consumers concerned, that provider shall make publicly available and easily accessible on its online interface the information concerning the illegal product or service, the identity of the trader and any relevant means of redress.

## SECTION 5

***Additional obligations for providers of very large online platforms and of very large online search engines to manage systemic risks****Article 33***Very large online platforms and very large online search engines**

1. This Section shall apply to online platforms and online search engines which have a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, and which are designated as very large online platforms or very large online search engines pursuant to paragraph 4.
2. The Commission shall adopt delegated acts in accordance with Article 87 to adjust the number of average monthly active recipients of the service in the Union referred to in paragraph 1, where the Union's population increases or decreases at least by 5 % in relation to its population in 2020 or its population after adjustment by means of a delegated act in the year in which the latest delegated act was adopted. In such a case, it shall adjust the number so that it corresponds to 10 % of the Union's population in the year in which it adopts the delegated act, rounded up or down to allow the number to be expressed in millions.
3. The Commission may adopt delegated acts in accordance with Article 87, after consulting the Board, to supplement the provisions of this Regulation by laying down the methodology for calculating the number of average monthly active recipients of the service in the Union, for the purposes of paragraph 1 of this Article and Article 24(2), ensuring that the methodology takes account of market and technological developments.
4. The Commission shall, after having consulted the Member State of establishment or after taking into account the information provided by the Digital Services Coordinator of establishment pursuant to Article 24(4), adopt a decision designating as a very large online platform or a very large online search engine for the purposes of this Regulation the online platform or the online search engine which has a number of average monthly active recipients of the service equal to or higher than the number referred to in paragraph 1 of this Article. The Commission shall take its decision on the basis of data reported by the provider of the online platform or of the online search engine pursuant to Article 24(2), or information requested pursuant to Article 24(3) or any other information available to the Commission.

The failure by the provider of the online platform or of the online search engine to comply with Article 24(2) or to comply with the request by the Digital Services Coordinator of establishment or by the Commission pursuant to Article 24(3) shall not prevent the Commission from designating that provider as a provider of a very large online platform or of a very large online search engine pursuant to this paragraph.

Where the Commission bases its decision on other information available to the Commission pursuant to the first subparagraph of this paragraph or on the basis of additional information requested pursuant to Article 24(3), the Commission shall give the provider of the online platform or of the online search engine concerned 10 working days in which to submit its views on the Commission's preliminary findings and on its intention to designate the online platform or the online search engine as a very large online platform or as a very large online search engine, respectively. The Commission shall take due account of the views submitted by the provider concerned.

The failure of the provider of the online platform or of the online search engine concerned to submit its views pursuant to the third subparagraph shall not prevent the Commission from designating that online platform or that online search engine as a very large online platform or as a very large online search engine, respectively, based on other information available to it.

5. The Commission shall terminate the designation if, during an uninterrupted period of one year, the online platform or the online search engine does not have a number of average monthly active recipients of the service equal to or higher than the number referred to in paragraph 1.

6. The Commission shall notify its decisions pursuant to paragraphs 4 and 5, without undue delay, to the provider of the online platform or of the online search engine concerned, to the Board and to the Digital Services Coordinator of establishment.

The Commission shall ensure that the list of designated very large online platforms and very large online search engines is published in the *Official Journal of the European Union*, and shall keep that list up to date. The obligations set out in this Section shall apply, or cease to apply, to the very large online platforms and very large online search engines concerned from four months after the notification to the provider concerned referred to in the first subparagraph.

#### Article 34

### Risk assessment

1. Providers of very large online platforms and of very large online search engines shall diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services.

They shall carry out the risk assessments by the date of application referred to in Article 33(6), second subparagraph, and at least once every year thereafter, and in any event prior to deploying functionalities that are likely to have a critical impact on the risks identified pursuant to this Article. This risk assessment shall be specific to their services and proportionate to the systemic risks, taking into consideration their severity and probability, and shall include the following systemic risks:

- (a) the dissemination of illegal content through their services;
- (b) any actual or foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights to human dignity enshrined in Article 1 of the Charter, to respect for private and family life enshrined in Article 7 of the Charter, to the protection of personal data enshrined in Article 8 of the Charter, to freedom of expression and information, including the freedom and pluralism of the media, enshrined in Article 11 of the Charter, to non-discrimination enshrined in Article 21 of the Charter, to respect for the rights of the child enshrined in Article 24 of the Charter and to a high-level of consumer protection enshrined in Article 38 of the Charter;
- (c) any actual or foreseeable negative effects on civic discourse and electoral processes, and public security;
- (d) any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being.

2. When conducting risk assessments, providers of very large online platforms and of very large online search engines shall take into account, in particular, whether and how the following factors influence any of the systemic risks referred to in paragraph 1:

- (a) the design of their recommender systems and any other relevant algorithmic system;
- (b) their content moderation systems;
- (c) the applicable terms and conditions and their enforcement;
- (d) systems for selecting and presenting advertisements;
- (e) data related practices of the provider.

The assessments shall also analyse whether and how the risks pursuant to paragraph 1 are influenced by intentional manipulation of their service, including by inauthentic use or automated exploitation of the service, as well as the amplification and potentially rapid and wide dissemination of illegal content and of information that is incompatible with their terms and conditions.

The assessment shall take into account specific regional or linguistic aspects, including when specific to a Member State.

3. Providers of very large online platforms and of very large online search engines shall preserve the supporting documents of the risk assessments for at least three years after the performance of risk assessments, and shall, upon request, communicate them to the Commission and to the Digital Services Coordinator of establishment.

#### Article 35

### Mitigation of risks

1. Providers of very large online platforms and of very large online search engines shall put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified pursuant to Article 34, with particular consideration to the impacts of such measures on fundamental rights. Such measures may include, where applicable:

- (a) adapting the design, features or functioning of their services, including their online interfaces;
- (b) adapting their terms and conditions and their enforcement;
- (c) adapting content moderation processes, including the speed and quality of processing notices related to specific types of illegal content and, where appropriate, the expeditious removal of, or the disabling of access to, the content notified, in particular in respect of illegal hate speech or cyber violence, as well as adapting any relevant decision-making processes and dedicated resources for content moderation;
- (d) testing and adapting their algorithmic systems, including their recommender systems;
- (e) adapting their advertising systems and adopting targeted measures aimed at limiting or adjusting the presentation of advertisements in association with the service they provide;
- (f) reinforcing the internal processes, resources, testing, documentation, or supervision of any of their activities in particular as regards detection of systemic risk;
- (g) initiating or adjusting cooperation with trusted flaggers in accordance with Article 22 and the implementation of the decisions of out-of-court dispute settlement bodies pursuant to Article 21;
- (h) initiating or adjusting cooperation with other providers of online platforms or of online search engines through the codes of conduct and the crisis protocols referred to in Articles 45 and 48 respectively;
- (i) taking awareness-raising measures and adapting their online interface in order to give recipients of the service more information;
- (j) taking targeted measures to protect the rights of the child, including age verification and parental control tools, tools aimed at helping minors signal abuse or obtain support, as appropriate;
- (k) ensuring that an item of information, whether it constitutes a generated or manipulated image, audio or video that appreciably resembles existing persons, objects, places or other entities or events and falsely appears to a person to be authentic or truthful is distinguishable through prominent markings when presented on their online interfaces, and, in addition, providing an easy to use functionality which enables recipients of the service to indicate such information.

2. The Board, in cooperation with the Commission, shall publish comprehensive reports, once a year. The reports shall include the following:

- (a) identification and assessment of the most prominent and recurrent systemic risks reported by providers of very large online platforms and of very large online search engines or identified through other information sources, in particular those provided in compliance with Articles 39, 40 and 42;

- (b) best practices for providers of very large online platforms and of very large online search engines to mitigate the systemic risks identified.

Those reports shall present systemic risks broken down by the Member States in which they occurred and in the Union as a whole, as applicable.

3. The Commission, in cooperation with the Digital Services Coordinators, may issue guidelines on the application of paragraph 1 in relation to specific risks, in particular to present best practices and recommend possible measures, having due regard to the possible consequences of the measures on fundamental rights enshrined in the Charter of all parties involved. When preparing those guidelines the Commission shall organise public consultations.

### Article 36

#### **Crisis response mechanism**

1. Where a crisis occurs, the Commission, acting upon a recommendation of the Board may adopt a decision, requiring one or more providers of very large online platforms or of very large online search engines to take one or more of the following actions:

- (a) assess whether, and if so to what extent and how, the functioning and use of their services significantly contribute to a serious threat as referred to in paragraph 2, or are likely to do so;
- (b) identify and apply specific, effective and proportionate measures, such as any of those provided for in Article 35(1) or Article 48(2), to prevent, eliminate or limit any such contribution to the serious threat identified pursuant to point (a) of this paragraph;
- (c) report to the Commission by a certain date or at regular intervals specified in the decision, on the assessments referred to in point (a), on the precise content, implementation and qualitative and quantitative impact of the specific measures taken pursuant to point (b) and on any other issue related to those assessments or those measures, as specified in the decision.

When identifying and applying measures pursuant to point (b) of this paragraph, the service provider or providers shall take due account of the gravity of the serious threat referred to in paragraph 2, of the urgency of the measures and of the actual or potential implications for the rights and legitimate interests of all parties concerned, including the possible failure of the measures to respect the fundamental rights enshrined in the Charter.

2. For the purpose of this Article, a crisis shall be deemed to have occurred where extraordinary circumstances lead to a serious threat to public security or public health in the Union or in significant parts of it.

3. When taking the decision referred to in paragraph 1, the Commission shall ensure that all of the following requirements are met:

- (a) the actions required by the decision are strictly necessary, justified and proportionate, having regard in particular to the gravity of the serious threat referred to in paragraph 2, the urgency of the measures and the actual or potential implications for the rights and legitimate interests of all parties concerned, including the possible failure of the measures to respect the fundamental rights enshrined in the Charter;
- (b) the decision specifies a reasonable period within which specific measures referred to in paragraph 1, point (b), are to be taken, having regard, in particular, to the urgency of those measures and the time needed to prepare and implement them;
- (c) the actions required by the decision are limited to a period not exceeding three months.

4. After adopting the decision referred to in paragraph 1, the Commission shall, without undue delay, take the following steps:

- (a) notify the decision to the provider or providers to which the decision is addressed;

- (b) make the decision publicly available; and
- (c) inform the Board of the decision, invite it to submit its views thereon, and keep it informed of any subsequent developments relating to the decision.

5. The choice of specific measures to be taken pursuant to paragraph 1, point (b), and to paragraph 7, second subparagraph, shall remain with the provider or providers addressed by the Commission's decision.

6. The Commission may on its own initiative or at the request of the provider, engage in a dialogue with the provider to determine whether, in light of the provider's specific circumstances, the intended or implemented measures referred to in paragraph 1, point (b), are effective and proportionate in achieving the objectives pursued. In particular, the Commission shall ensure that the measures taken by the service provider under paragraph 1, point (b), meet the requirements referred to in paragraph 3, points (a) and (c).

7. The Commission shall monitor the application of the specific measures taken pursuant to the decision referred to in paragraph 1 of this Article on the basis of the reports referred to in point (c) of that paragraph and any other relevant information, including information it may request pursuant to Article 40 or 67, taking into account the evolution of the crisis. The Commission shall report regularly to the Board on that monitoring, at least on a monthly basis.

Where the Commission considers that the intended or implemented specific measures pursuant to paragraph 1, point (b), are not effective or proportionate it may, after consulting the Board, adopt a decision requiring the provider to review the identification or application of those specific measures.

8. Where appropriate in view of the evolution of the crisis, the Commission, acting on the Board's recommendation, may amend the decision referred to in paragraph 1 or in paragraph 7, second subparagraph, by:

- (a) revoking the decision and, where appropriate, requiring the very large online platform or very large online search engine to cease to apply the measures identified and implemented pursuant to paragraph 1, point (b), or paragraph 7, second subparagraph, in particular where the grounds for such measures do not exist anymore;
- (b) extending the period referred to paragraph 3, point (c), by a period of no more than three months;
- (c) taking account of experience gained in applying the measures, in particular the possible failure of the measures to respect the fundamental rights enshrined in the Charter.

9. The requirements of paragraphs 1 to 6 shall apply to the decision and to the amendment thereof referred to in this Article.

10. The Commission shall take utmost account of the recommendation of the Board issued pursuant to this Article.

11. The Commission shall report to the European Parliament and to the Council on a yearly basis following the adoption of decisions in accordance with this Article, and, in any event, three months after the end of the crisis, on the application of the specific measures taken pursuant to those decisions.

#### Article 37

#### **Independent audit**

1. Providers of very large online platforms and of very large online search engines shall be subject, at their own expense and at least once a year, to independent audits to assess compliance with the following:

- (a) the obligations set out in Chapter III;
- (b) any commitments undertaken pursuant to the codes of conduct referred to in Articles 45 and 46 and the crisis protocols referred to in Article 48.

2. Providers of very large online platforms and of very large online search engines shall afford the organisations carrying out the audits pursuant to this Article the cooperation and assistance necessary to enable them to conduct those audits in an effective, efficient and timely manner, including by giving them access to all relevant data and premises and by answering oral or written questions. They shall refrain from hampering, unduly influencing or undermining the performance of the audit.

Such audits shall ensure an adequate level of confidentiality and professional secrecy in respect of the information obtained from the providers of very large online platforms and of very large online search engines and third parties in the context of the audits, including after the termination of the audits. However, complying with that requirement shall not adversely affect the performance of the audits and other provisions of this Regulation, in particular those on transparency, supervision and enforcement. Where necessary for the purpose of the transparency reporting pursuant to Article 42(4), the audit report and the audit implementation report referred to in paragraphs 4 and 6 of this Article shall be accompanied with versions that do not contain any information that could reasonably be considered to be confidential.

3. Audits performed pursuant to paragraph 1 shall be performed by organisations which:

- (a) are independent from, and do not have any conflicts of interest with, the provider of very large online platforms or of very large online search engines concerned and any legal person connected to that provider; in particular:
  - (i) have not provided non-audit services related to the matters audited to the provider of very large online platform or of very large online search engine concerned and to any legal person connected to that provider in the 12 months' period before the beginning of the audit and have committed to not providing them with such services in the 12 months' period after the completion of the audit;
  - (ii) have not provided auditing services pursuant to this Article to the provider of very large online platform or of very large online search engine concerned and any legal person connected to that provider during a period longer than 10 consecutive years;
  - (iii) are not performing the audit in return for fees which are contingent on the result of the audit;
- (b) have proven expertise in the area of risk management, technical competence and capabilities;
- (c) have proven objectivity and professional ethics, based in particular on adherence to codes of practice or appropriate standards.

4. Providers of very large online platforms and of very large online search engines shall ensure that the organisations that perform the audits establish an audit report for each audit. That report shall be substantiated, in writing, and shall include at least the following:

- (a) the name, address and the point of contact of the provider of the very large online platform or of the very large online search engine subject to the audit and the period covered;
- (b) the name and address of the organisation or organisations performing the audit;
- (c) a declaration of interests;
- (d) a description of the specific elements audited, and the methodology applied;
- (e) a description and a summary of the main findings drawn from the audit;
- (f) a list of the third parties consulted as part of the audit;
- (g) an audit opinion on whether the provider of the very large online platform or of the very large online search engine subject to the audit complied with the obligations and with the commitments referred to in paragraph 1, namely 'positive', 'positive with comments' or 'negative';
- (h) where the audit opinion is not 'positive', operational recommendations on specific measures to achieve compliance and the recommended timeframe to achieve compliance.

5. Where the organisation performing the audit was unable to audit certain specific elements or to express an audit opinion based on its investigations, the audit report shall include an explanation of the circumstances and the reasons why those elements could not be audited.

6. Providers of very large online platforms or of very large online search engines receiving an audit report that is not 'positive' shall take due account of the operational recommendations addressed to them with a view to take the necessary measures to implement them. They shall, within one month from receiving those recommendations, adopt an audit implementation report setting out those measures. Where they do not implement the operational recommendations, they shall justify in the audit implementation report the reasons for not doing so and set out any alternative measures that they have taken to address any instances of non-compliance identified.

7. The Commission is empowered to adopt delegated acts in accordance with Article 87 to supplement this Regulation by laying down the necessary rules for the performance of the audits pursuant to this Article, in particular as regards the necessary rules on the procedural steps, auditing methodologies and reporting templates for the audits performed pursuant to this Article. Those delegated acts shall take into account any voluntary auditing standards referred to in Article 44(1), point (e).

#### Article 38

### Recommender systems

In addition to the requirements set out in Article 27, providers of very large online platforms and of very large online search engines that use recommender systems shall provide at least one option for each of their recommender systems which is not based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679.

#### Article 39

### Additional online advertising transparency

1. Providers of very large online platforms or of very large online search engines that present advertisements on their online interfaces shall compile and make publicly available in a specific section of their online interface, through a searchable and reliable tool that allows multicriteria queries and through application programming interfaces, a repository containing the information referred to in paragraph 2, for the entire period during which they present an advertisement and until one year after the advertisement was presented for the last time on their online interfaces. They shall ensure that the repository does not contain any personal data of the recipients of the service to whom the advertisement was or could have been presented, and shall make reasonable efforts to ensure that the information is accurate and complete.

2. The repository shall include at least all of the following information:

- (a) the content of the advertisement, including the name of the product, service or brand and the subject matter of the advertisement;
- (b) the natural or legal person on whose behalf the advertisement is presented;
- (c) the natural or legal person who paid for the advertisement, if that person is different from the person referred to in point (b);
- (d) the period during which the advertisement was presented;
- (e) whether the advertisement was intended to be presented specifically to one or more particular groups of recipients of the service and if so, the main parameters used for that purpose including where applicable the main parameters used to exclude one or more of such particular groups;
- (f) the commercial communications published on the very large online platforms and identified pursuant to Article 26(2);
- (g) the total number of recipients of the service reached and, where applicable, aggregate numbers broken down by Member State for the group or groups of recipients that the advertisement specifically targeted.

3. As regards paragraph 2, points (a), (b) and (c), where a provider of very large online platform or of very large online search engine has removed or disabled access to a specific advertisement based on alleged illegality or incompatibility with its terms and conditions, the repository shall not include the information referred to in those points. In such case, the repository shall include, for the specific advertisement concerned, the information referred to in Article 17(3), points (a) to (e), or Article 9(2), point (a)(i), as applicable.

The Commission may, after consultation of the Board, the relevant vetted researchers referred to in Article 40 and the public, issue guidelines on the structure, organisation and functionalities of the repositories referred to in this Article.

#### Article 40

##### **Data access and scrutiny**

1. Providers of very large online platforms or of very large online search engines shall provide the Digital Services Coordinator of establishment or the Commission, at their reasoned request and within a reasonable period specified in that request, access to data that are necessary to monitor and assess compliance with this Regulation.

2. Digital Services Coordinators and the Commission shall use the data accessed pursuant to paragraph 1 only for the purpose of monitoring and assessing compliance with this Regulation and shall take due account of the rights and interests of the providers of very large online platforms or of very large online search engines and the recipients of the service concerned, including the protection of personal data, the protection of confidential information, in particular trade secrets, and maintaining the security of their service.

3. For the purposes of paragraph 1, providers of very large online platforms or of very large online search engines shall, at the request of either the Digital Service Coordinator of establishment or of the Commission, explain the design, the logic, the functioning and the testing of their algorithmic systems, including their recommender systems.

4. Upon a reasoned request from the Digital Services Coordinator of establishment, providers of very large online platforms or of very large online search engines shall, within a reasonable period, as specified in the request, provide access to data to vetted researchers who meet the requirements in paragraph 8 of this Article, for the sole purpose of conducting research that contributes to the detection, identification and understanding of systemic risks in the Union, as set out pursuant to Article 34(1), and to the assessment of the adequacy, efficiency and impacts of the risk mitigation measures pursuant to Article 35.

5. Within 15 days following receipt of a request as referred to in paragraph 4, providers of very large online platforms or of very large online search engines may request the Digital Services Coordinator of establishment, to amend the request, where they consider that they are unable to give access to the data requested because one of following two reasons:

(a) they do not have access to the data;

(b) giving access to the data will lead to significant vulnerabilities in the security of their service or the protection of confidential information, in particular trade secrets.

6. Requests for amendment pursuant to paragraph 5 shall contain proposals for one or more alternative means through which access may be provided to the requested data or other data which are appropriate and sufficient for the purpose of the request.

The Digital Services Coordinator of establishment shall decide on the request for amendment within 15 days and communicate to the provider of the very large online platform or of the very large online search engine its decision and, where relevant, the amended request and the new period to comply with the request.

7. Providers of very large online platforms or of very large online search engines shall facilitate and provide access to data pursuant to paragraphs 1 and 4 through appropriate interfaces specified in the request, including online databases or application programming interfaces.

8. Upon a duly substantiated application from researchers, the Digital Services Coordinator of establishment shall grant such researchers the status of 'vetted researchers' for the specific research referred to in the application and issue a reasoned request for data access to a provider of very large online platform or of very large online search engine pursuant to paragraph 4, where the researchers demonstrate that they meet all of the following conditions:

- (a) they are affiliated to a research organisation as defined in Article 2, point (1), of Directive (EU) 2019/790;
- (b) they are independent from commercial interests;
- (c) their application discloses the funding of the research;
- (d) they are capable of fulfilling the specific data security and confidentiality requirements corresponding to each request and to protect personal data, and they describe in their request the appropriate technical and organisational measures that they have put in place to this end;
- (e) their application demonstrates that their access to the data and the time frames requested are necessary for, and proportionate to, the purposes of their research, and that the expected results of that research will contribute to the purposes laid down in paragraph 4;
- (f) the planned research activities will be carried out for the purposes laid down in paragraph 4;
- (g) they have committed themselves to making their research results publicly available free of charge, within a reasonable period after the completion of the research, subject to the rights and interests of the recipients of the service concerned, in accordance with Regulation (EU) 2016/679.

Upon receipt of the application pursuant to this paragraph, the Digital Services Coordinator of establishment shall inform the Commission and the Board.

9. Researchers may also submit their application to the Digital Services Coordinator of the Member State of the research organisation to which they are affiliated. Upon receipt of the application pursuant to this paragraph the Digital Services Coordinator shall conduct an initial assessment as to whether the respective researchers meet all of the conditions set out in paragraph 8. The respective Digital Services Coordinator shall subsequently send the application, together with the supporting documents submitted by the respective researchers and the initial assessment, to the Digital Services Coordinator of establishment. The Digital Services Coordinator of establishment shall take a decision whether to award a researcher the status of 'vetted researcher' without undue delay.

While taking due account of the initial assessment provided, the final decision to award a researcher the status of 'vetted researcher' lies within the competence of Digital Services Coordinator of establishment, pursuant to paragraph 8.

10. The Digital Services Coordinator that awarded the status of vetted researcher and issued the reasoned request for data access to the providers of very large online platforms or of very large online search engines in favour of a vetted researcher shall issue a decision terminating the access if it determines, following an investigation either on its own initiative or on the basis of information received from third parties, that the vetted researcher no longer meets the conditions set out in paragraph 8, and shall inform the provider of the very large online platform or of the very large online search engine concerned of the decision. Before terminating the access, the Digital Services Coordinator shall allow the vetted researcher to react to the findings of its investigation and to its intention to terminate the access.

11. Digital Services Coordinators of establishment shall communicate to the Board the names and contact information of the natural persons or entities to which they have awarded the status of 'vetted researcher' in accordance with paragraph 8, as well as the purpose of the research in respect of which the application was made or, where they have terminated the access to the data in accordance with paragraph 10, communicate that information to the Board.

12. Providers of very large online platforms or of very large online search engines shall give access without undue delay to data, including, where technically possible, to real-time data, provided that the data is publicly accessible in their online interface by researchers, including those affiliated to not for profit bodies, organisations and associations, who comply with the conditions set out in paragraph 8, points (b), (c), (d) and (e), and who use the data solely for performing research that contributes to the detection, identification and understanding of systemic risks in the Union pursuant to Article 34(1).

13. The Commission shall, after consulting the Board, adopt delegated acts supplementing this Regulation by laying down the technical conditions under which providers of very large online platforms or of very large online search engines are to share data pursuant to paragraphs 1 and 4 and the purposes for which the data may be used. Those delegated acts shall lay down the specific conditions under which such sharing of data with researchers can take place in compliance with Regulation (EU) 2016/679, as well as relevant objective indicators, procedures and, where necessary, independent advisory mechanisms in support of sharing of data, taking into account the rights and interests of the providers of very large online platforms or of very large online search engines and the recipients of the service concerned, including the protection of confidential information, in particular trade secrets, and maintaining the security of their service.

#### Article 41

### Compliance function

1. Providers of very large online platforms or of very large online search engines shall establish a compliance function, which is independent from their operational functions and composed of one or more compliance officers, including the head of the compliance function. That compliance function shall have sufficient authority, stature and resources, as well as access to the management body of the provider of the very large online platform or of the very large online search engine to monitor the compliance of that provider with this Regulation.

2. The management body of the provider of the very large online platform or of the very large online search engine shall ensure that compliance officers have the professional qualifications, knowledge, experience and ability necessary to fulfil the tasks referred to in paragraph 3.

The management body of the provider of the very large online platform or of the very large online search engine shall ensure that the head of the compliance function is an independent senior manager with distinct responsibility for the compliance function.

The head of the compliance function shall report directly to the management body of the provider of the very large online platform or of the very large online search engine, and may raise concerns and warn that body where risks referred to in Article 34 or non-compliance with this Regulation affect or may affect the provider of the very large online platform or of the very large online search engine concerned, without prejudice to the responsibilities of the management body in its supervisory and managerial functions.

The head of the compliance function shall not be removed without prior approval of the management body of the provider of the very large online platform or of the very large online search engine.

3. Compliance officers shall have the following tasks:

- (a) cooperating with the Digital Services Coordinator of establishment and the Commission for the purpose of this Regulation;
- (b) ensuring that all risks referred to in Article 34 are identified and properly reported on and that reasonable, proportionate and effective risk-mitigation measures are taken pursuant to Article 35;
- (c) organising and supervising the activities of the provider of the very large online platform or of the very large online search engine relating to the independent audit pursuant to Article 37;

- (d) informing and advising the management and employees of the provider of the very large online platform or of the very large online search engine about relevant obligations under this Regulation;
- (e) monitoring the compliance of the provider of the very large online platform or of the very large online search engine with its obligations under this Regulation;
- (f) where applicable, monitoring the compliance of the provider of the very large online platform or of the very large online search engine with commitments made under the codes of conduct pursuant to Articles 45 and 46 or the crisis protocols pursuant to Article 48.

4. Providers of very large online platforms or of very large online search engines shall communicate the name and contact details of the head of the compliance function to the Digital Services Coordinator of establishment and to the Commission.

5. The management body of the provider of the very large online platform or of the very large online search engine shall define, oversee and be accountable for the implementation of the provider's governance arrangements that ensure the independence of the compliance function, including the division of responsibilities within the organisation of the provider of very large online platform or of very large online search engine, the prevention of conflicts of interest, and sound management of systemic risks identified pursuant to Article 34.

6. The management body shall approve and review periodically, at least once a year, the strategies and policies for taking up, managing, monitoring and mitigating the risks identified pursuant to Article 34 to which the very large online platform or the very large online search engine is or might be exposed to.

7. The management body shall devote sufficient time to the consideration of the measures related to risk management. It shall be actively involved in the decisions related to risk management, and shall ensure that adequate resources are allocated to the management of the risks identified in accordance with Article 34.

#### Article 42

### Transparency reporting obligations

1. Providers of very large online platforms or of very large online search engines shall publish the reports referred to in Article 15 at the latest by two months from the date of application referred to in Article 33(6), second subparagraph, and thereafter at least every six months.

2. The reports referred to in paragraph 1 of this Article published by providers of very large online platforms shall, in addition to the information referred to in Article 15 and Article 24(1), specify:

- (a) the human resources that the provider of very large online platforms dedicates to content moderation in respect of the service offered in the Union, broken down by each applicable official language of the Member States, including for compliance with the obligations set out in Articles 16 and 22, as well as for compliance with the obligations set out in Article 20;
- (b) the qualifications and linguistic expertise of the persons carrying out the activities referred to in point (a), as well as the training and support given to such staff;
- (c) the indicators of accuracy and related information referred to in Article 15(1), point (e), broken down by each official language of the Member States.

The reports shall be published in at least one of the official languages of the Member States.

3. In addition to the information referred to in Articles 24(2), the providers of very large online platforms or of very large online search engines shall include in the reports referred to in paragraph 1 of this Article the information on the average monthly recipients of the service for each Member State.

4. Providers of very large online platforms or of very large online search engines shall transmit to the Digital Services Coordinator of establishment and the Commission, without undue delay upon completion, and make publicly available at the latest three months after the receipt of each audit report pursuant to Article 37(4):

- (a) a report setting out the results of the risk assessment pursuant to Article 34;
- (b) the specific mitigation measures put in place pursuant to Article 35(1);
- (c) the audit report provided for in Article 37(4);
- (d) the audit implementation report provided for in Article 37(6);
- (e) where applicable, information about the consultations conducted by the provider in support of the risk assessments and design of the risk mitigation measures.

5. Where a provider of very large online platform or of very large online search engine considers that the publication of information pursuant to paragraph 4 might result in the disclosure of confidential information of that provider or of the recipients of the service, cause significant vulnerabilities for the security of its service, undermine public security or harm recipients, the provider may remove such information from the publicly available reports. In that case, the provider shall transmit the complete reports to the Digital Services Coordinator of establishment and the Commission, accompanied by a statement of the reasons for removing the information from the publicly available reports.

#### Article 43

#### Supervisory fee

1. The Commission shall charge providers of very large online platforms and of very large online search engines an annual supervisory fee upon their designation pursuant to Article 33.
2. The overall amount of the annual supervisory fees shall cover the estimated costs that the Commission incurs in relation to its supervisory tasks under this Regulation, in particular costs related to the designation pursuant to Article 33, to the set-up, maintenance and operation of the database pursuant to Article 24(5) and to the information sharing system pursuant to Article 85, to referrals pursuant to Article 59, to supporting the Board pursuant to Article 62 and to the supervisory tasks pursuant to Article 56 and Section 4 of Chapter IV.
3. The providers of very large online platforms and of very large online search engines shall be charged annually a supervisory fee for each service for which they have been designated pursuant to Article 33.

The Commission shall adopt implementing acts establishing the amount of the annual supervisory fee in respect of each provider of very large online platform or of very large online search engine. When adopting those implementing acts, the Commission shall apply the methodology laid down in the delegated act referred to in paragraph 4 of this Article and shall respect the principles set out in paragraph 5 of this Article. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 88.

4. The Commission shall adopt delegated acts, in accordance with Article 87, laying down the detailed methodology and procedures for:
  - (a) the determination of the estimated costs referred to in paragraph 2;
  - (b) the determination of the individual annual supervisory fees referred to in paragraph 5, points (b) and (c);
  - (c) the determination of the maximum overall limit defined in paragraph 5, point (c); and
  - (d) the detailed arrangements necessary to make payments.

When adopting those delegated acts, the Commission shall respect the principles set out in paragraph 5 of this Article.

5. The implementing act referred to in paragraph 3 and the delegated act referred to in paragraph 4 shall respect the following principles:

- (a) the estimation of the overall amount of the annual supervisory fee takes into account the costs incurred in the previous year;
- (b) the annual supervisory fee is proportionate to the number of average monthly active recipients in the Union of each very large online platform or each very large online search engine designated pursuant to Article 33;
- (c) the overall amount of the annual supervisory fee charged on a given provider of very large online platform or very large search engine does not, in any case, exceed 0,05 % of its worldwide annual net income in the preceding financial year.

6. The individual annual supervisory fees charged pursuant to paragraph 1 of this Article shall constitute external assigned revenue in accordance with Article 21(5) of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council <sup>(41)</sup>.

7. The Commission shall report annually to the European Parliament and to the Council on the overall amount of the costs incurred for the fulfilment of the tasks under this Regulation and the total amount of the individual annual supervisory fees charged in the preceding year.

## SECTION 6

### ***Other provisions concerning due diligence obligations***

#### *Article 44*

#### **Standards**

1. The Commission shall consult the Board, and shall support and promote the development and implementation of voluntary standards set by relevant European and international standardisation bodies, at least in respect of the following:

- (a) electronic submission of notices under Article 16;
- (b) templates, design and process standards for communicating with the recipients of the service in a user-friendly manner on restrictions resulting from terms and conditions and changes thereto;
- (c) electronic submission of notices by trusted flaggers under Article 22, including through application programming interfaces;
- (d) specific interfaces, including application programming interfaces, to facilitate compliance with the obligations set out in Articles 39 and 40;
- (e) auditing of very large online platforms and of very large online search engines pursuant to Article 37;
- (f) interoperability of the advertisement repositories referred to in Article 39(2);
- (g) transmission of data between advertising intermediaries in support of transparency obligations pursuant to Article 26(1), points (b), (c) and (d);
- (h) technical measures to enable compliance with obligations relating to advertising contained in this Regulation, including the obligations regarding prominent markings for advertisements and commercial communications referred to in Article 26;

---

<sup>(41)</sup> Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (OJ L 193, 30.7.2018, p. 1).

- (i) choice interfaces and presentation of information on the main parameters of different types of recommender systems, in accordance with Articles 27 and 38;
- (j) standards for targeted measures to protect minors online.

2. The Commission shall support the update of the standards in the light of technological developments and the behaviour of the recipients of the services in question. The relevant information regarding the update of the standards shall be publicly available and easily accessible.

#### Article 45

### Codes of conduct

1. The Commission and the Board shall encourage and facilitate the drawing up of voluntary codes of conduct at Union level to contribute to the proper application of this Regulation, taking into account in particular the specific challenges of tackling different types of illegal content and systemic risks, in accordance with Union law in particular on competition and the protection of personal data.

2. Where significant systemic risk within the meaning of Article 34(1) emerge and concern several very large online platforms or very large online search engines, the Commission may invite the providers of very large online platforms concerned or the providers of very large online search engines concerned, and other providers of very large online platforms, of very large online search engines, of online platforms and of other intermediary services, as appropriate, as well as relevant competent authorities, civil society organisations and other relevant stakeholders, to participate in the drawing up of codes of conduct, including by setting out commitments to take specific risk mitigation measures, as well as a regular reporting framework on any measures taken and their outcomes.

3. When giving effect to paragraphs 1 and 2, the Commission and the Board, and where relevant other bodies, shall aim to ensure that the codes of conduct clearly set out their specific objectives, contain key performance indicators to measure the achievement of those objectives and take due account of the needs and interests of all interested parties, and in particular citizens, at Union level. The Commission and the Board shall also aim to ensure that participants report regularly to the Commission and their respective Digital Services Coordinators of establishment on any measures taken and their outcomes, as measured against the key performance indicators that they contain. Key performance indicators and reporting commitments shall take into account differences in size and capacity between different participants.

4. The Commission and the Board shall assess whether the codes of conduct meet the aims specified in paragraphs 1 and 3, and shall regularly monitor and evaluate the achievement of their objectives, having regard to the key performance indicators that they might contain. They shall publish their conclusions.

The Commission and the Board shall also encourage and facilitate regular review and adaptation of the codes of conduct.

In the case of systematic failure to comply with the codes of conduct, the Commission and the Board may invite the signatories to the codes of conduct to take the necessary action.

#### Article 46

### Codes of conduct for online advertising

1. The Commission shall encourage and facilitate the drawing up of voluntary codes of conduct at Union level by providers of online platforms and other relevant service providers, such as providers of online advertising intermediary services, other actors involved in the programmatic advertising value chain, or organisations representing recipients of the service and civil society organisations or relevant authorities to contribute to further transparency for actors in the online advertising value chain beyond the requirements of Articles 26 and 39.

2. The Commission shall aim to ensure that the codes of conduct pursue an effective transmission of information that fully respects the rights and interests of all parties involved, as well as a competitive, transparent and fair environment in online advertising, in accordance with Union and national law, in particular on competition and the protection of privacy and personal data. The Commission shall aim to ensure that the codes of conduct at least address the following:

- (a) the transmission of information held by providers of online advertising intermediaries to recipients of the service concerning the requirements set in Article 26(1), points (b), (c) and (d);
- (b) the transmission of information held by providers of online advertising intermediaries to the repositories pursuant to Article 39;
- (c) meaningful information on data monetisation.

3. The Commission shall encourage the development of the codes of conduct by 18 February 2025 and their application by 18 August 2025.

4. The Commission shall encourage all the actors in the online advertising value chain referred to in paragraph 1 to endorse the commitments stated in the codes of conduct, and to comply with them.

#### Article 47

### Codes of conduct for accessibility

1. The Commission shall encourage and facilitate the drawing up of codes of conduct at Union level with the involvement of providers of online platforms and other relevant service providers, organisations representing recipients of the service and civil society organisations or relevant authorities to promote full and effective, equal participation, by improving access to online services that, through their initial design or subsequent adaptation, address the particular needs of persons with disabilities.

2. The Commission shall aim to ensure that the codes of conduct pursue the objective of ensuring that those services are accessible in compliance with Union and national law, in order to maximise their foreseeable use by persons with disabilities. The Commission shall aim to ensure that the codes of conduct address at least the following objectives:

- (a) designing and adapting services to make them accessible to persons with disabilities by making them perceivable, operable, understandable and robust;
- (b) explaining how the services meet the applicable accessibility requirements and making this information available to the public in an accessible manner for persons with disabilities;
- (c) making information, forms and measures provided pursuant to this Regulation available in such a manner that they are easy to find, easy to understand, and accessible to persons with disabilities.

3. The Commission shall encourage the development of the codes of conduct by 18 February 2025 and their application by 18 August 2025.

#### Article 48

### Crisis protocols

1. The Board may recommend that the Commission initiate the drawing up, in accordance with paragraphs 2, 3 and 4, of voluntary crisis protocols for addressing crisis situations. Those situations shall be strictly limited to extraordinary circumstances affecting public security or public health.

2. The Commission shall encourage and facilitate the providers of very large online platforms, of very large online search engines and, where appropriate, the providers of other online platforms or of other online search engines, to participate in the drawing up, testing and application of those crisis protocols. The Commission shall aim to ensure that those crisis protocols include one or more of the following measures:

- (a) prominently displaying information on the crisis situation provided by Member States' authorities or at Union level, or, depending on the context of the crisis, by other relevant reliable bodies;
- (b) ensuring that the provider of intermediary services designates a specific point of contact for crisis management; where relevant, this may be the electronic point of contact referred to in Article 11 or, in the case of providers of very large online platforms or of very large online search engines, the compliance officer referred to in Article 41;
- (c) where applicable, adapt the resources dedicated to compliance with the obligations set out in Articles 16, 20, 22, 23 and 35 to the needs arising from the crisis situation.

3. The Commission shall, as appropriate, involve Member States' authorities, and may also involve Union bodies, offices and agencies in drawing up, testing and supervising the application of the crisis protocols. The Commission may, where necessary and appropriate, also involve civil society organisations or other relevant organisations in drawing up the crisis protocols.

4. The Commission shall aim to ensure that the crisis protocols set out clearly all of the following:

- (a) the specific parameters to determine what constitutes the specific extraordinary circumstance the crisis protocol seeks to address and the objectives it pursues;
- (b) the role of each participant and the measures they are to put in place in preparation and once the crisis protocol has been activated;
- (c) a clear procedure for determining when the crisis protocol is to be activated;
- (d) a clear procedure for determining the period during which the measures to be taken once the crisis protocol has been activated are to be taken, which is strictly limited to what is necessary for addressing the specific extraordinary circumstances concerned;
- (e) safeguards to address any negative effects on the exercise of the fundamental rights enshrined in the Charter, in particular the freedom of expression and information and the right to non-discrimination;
- (f) a process to publicly report on any measures taken, their duration and their outcomes, upon the termination of the crisis situation.

5. If the Commission considers that a crisis protocol fails to effectively address the crisis situation, or to safeguard the exercise of fundamental rights as referred to in paragraph 4, point (e), it shall request the participants to revise the crisis protocol, including by taking additional measures.

## CHAPTER IV

## IMPLEMENTATION, COOPERATION, PENALTIES AND ENFORCEMENT

## SECTION 1

***Competent authorities and national Digital Services Coordinators****Article 49***Competent authorities and Digital Services Coordinators**

1. Member States shall designate one or more competent authorities to be responsible for the supervision of providers of intermediary services and enforcement of this Regulation ('competent authorities').
2. Member States shall designate one of the competent authorities as their Digital Services Coordinator. The Digital Services Coordinator shall be responsible for all matters relating to supervision and enforcement of this Regulation in that Member State, unless the Member State concerned has assigned certain specific tasks or sectors to other competent authorities. The Digital Services Coordinator shall in any event be responsible for ensuring coordination at national level in respect of those matters and for contributing to the effective and consistent supervision and enforcement of this Regulation throughout the Union.

For that purpose, Digital Services Coordinators shall cooperate with each other, other national competent authorities, the Board and the Commission, without prejudice to the possibility for Member States to provide for cooperation mechanisms and regular exchanges of views between the Digital Services Coordinator and other national authorities where relevant for the performance of their respective tasks.

Where a Member State designates one or more competent authorities in addition to the Digital Services Coordinator, it shall ensure that the respective tasks of those authorities and of the Digital Services Coordinator are clearly defined and that they cooperate closely and effectively when performing their tasks.

3. Member States shall designate the Digital Services Coordinators by 17 February 2024.

Member States shall make publicly available, and communicate to the Commission and the Board, the name of their competent authority designated as Digital Services Coordinator and information on how it can be contacted. The Member State concerned shall communicate to the Commission and the Board the name of the other competent authorities referred to in paragraph 2, as well as their respective tasks.

4. The provisions applicable to Digital Services Coordinators set out in Articles 50, 51 and 56 shall also apply to any other competent authorities that the Member States designate pursuant to paragraph 1 of this Article.

*Article 50***Requirements for Digital Services Coordinators**

1. Member States shall ensure that their Digital Services Coordinators perform their tasks under this Regulation in an impartial, transparent and timely manner. Member States shall ensure that their Digital Services Coordinators have all necessary resources to carry out their tasks, including sufficient technical, financial and human resources to adequately supervise all providers of intermediary services falling within their competence. Each Member State shall ensure that its Digital Services Coordinator has sufficient autonomy in managing its budget within the budget's overall limits, in order not to adversely affect the independence of the Digital Services Coordinator.

2. When carrying out their tasks and exercising their powers in accordance with this Regulation, the Digital Services Coordinators shall act with complete independence. They shall remain free from any external influence, whether direct or indirect, and shall neither seek nor take instructions from any other public authority or any private party.

3. Paragraph 2 of this Article is without prejudice to the tasks of Digital Services Coordinators within the system of supervision and enforcement provided for in this Regulation and the cooperation with other competent authorities in accordance with Article 49(2). Paragraph 2 of this Article shall not prevent the exercise of judicial review and shall also be without prejudice to proportionate accountability requirements regarding the general activities of the Digital Services Coordinators, such as financial expenditure or reporting to national parliaments, provided that those requirements do not undermine the achievement of the objectives of this Regulation.

#### Article 51

### **Powers of Digital Services Coordinators**

1. Where needed in order to carry out their tasks under this Regulation, Digital Services Coordinators shall have the following powers of investigation, in respect of conduct by providers of intermediary services falling within the competence of their Member State:

- (a) the power to require those providers, as well as any other persons acting for purposes related to their trade, business, craft or profession that may reasonably be aware of information relating to a suspected infringement of this Regulation, including organisations performing the audits referred to in Article 37 and Article 75(2), to provide such information without undue delay;
- (b) the power to carry out, or to request a judicial authority in their Member State to order, inspections of any premises that those providers or those persons use for purposes related to their trade, business, craft or profession, or to request other public authorities to do so, in order to examine, seize, take or obtain copies of information relating to a suspected infringement in any form, irrespective of the storage medium;
- (c) the power to ask any member of staff or representative of those providers or those persons to give explanations in respect of any information relating to a suspected infringement and to record the answers with their consent by any technical means.

2. Where needed for carrying out their tasks under this Regulation, Digital Services Coordinators shall have the following enforcement powers, in respect of providers of intermediary services falling within the competence of their Member State:

- (a) the power to accept the commitments offered by those providers in relation to their compliance with this Regulation and to make those commitments binding;
- (b) the power to order the cessation of infringements and, where appropriate, to impose remedies proportionate to the infringement and necessary to bring the infringement effectively to an end, or to request a judicial authority in their Member State to do so;
- (c) the power to impose fines, or to request a judicial authority in their Member State to do so, in accordance with Article 52 for failure to comply with this Regulation, including with any of the investigative orders issued pursuant to paragraph 1 of this Article;
- (d) the power to impose a periodic penalty payment, or to request a judicial authority in their Member State to do so, in accordance with Article 52 to ensure that an infringement is terminated in compliance with an order issued pursuant to point (b) of this subparagraph or for failure to comply with any of the investigative orders issued pursuant to paragraph 1 of this Article;
- (e) the power to adopt interim measures or to request the competent national judicial authority in their Member State to do so, to avoid the risk of serious harm.

As regards the first subparagraph, points (c) and (d), Digital Services Coordinators shall also have the enforcement powers set out in those points in respect of the other persons referred to in paragraph 1 for failure to comply with any of the orders issued to them pursuant to that paragraph. They shall only exercise those enforcement powers after providing those other persons in good time with all relevant information relating to such orders, including the applicable period, the fines or periodic payments that may be imposed for failure to comply and the possibilities for redress.

3. Where needed for carrying out their tasks under this Regulation, Digital Services Coordinators shall, in respect of providers of intermediary services falling within the competence of their Member State, where all other powers pursuant to this Article to bring about the cessation of an infringement have been exhausted and the infringement has not been remedied or is continuing and is causing serious harm which cannot be avoided through the exercise of other powers available under Union or national law, also have the power to take the following measures:

- (a) to require the management body of those providers, without undue delay, to examine the situation, adopt and submit an action plan setting out the necessary measures to terminate the infringement, ensure that the provider takes those measures, and report on the measures taken;
- (b) where the Digital Services Coordinator considers that a provider of intermediary services has not sufficiently complied with the requirements referred to in point (a), that the infringement has not been remedied or is continuing and is causing serious harm, and that that infringement entails a criminal offence involving a threat to the life or safety of persons, to request that the competent judicial authority of its Member State order the temporary restriction of access of recipients to the service concerned by the infringement or, only where that is not technically feasible, to the online interface of the provider of intermediary services on which the infringement takes place.

The Digital Services Coordinator shall, except where it acts upon the Commission's request referred to in Article 82, prior to submitting the request referred to in the first subparagraph, point (b), of this paragraph invite interested parties to submit written observations within a period that shall not be less than two weeks, describing the measures that it intends to request and identifying the intended addressee or addressees thereof. The provider of intermediary services, the intended addressee or addressees and any other third party demonstrating a legitimate interest shall be entitled to participate in the proceedings before the competent judicial authority. Any measure ordered shall be proportionate to the nature, gravity, recurrence and duration of the infringement, without unduly restricting access to lawful information by recipients of the service concerned.

The restriction of access shall be for a period of four weeks, subject to the possibility for the competent judicial authority, in its order, to allow the Digital Services Coordinator to extend that period for further periods of the same lengths, subject to a maximum number of extensions set by that judicial authority. The Digital Services Coordinator shall only extend the period where, having regard to the rights and interests of all parties affected by that restriction and all relevant circumstances, including any information that the provider of intermediary services, the addressee or addressees and any other third party that demonstrated a legitimate interest may provide to it, it considers that both of the following conditions have been met:

- (a) the provider of intermediary services has failed to take the necessary measures to terminate the infringement;
- (b) the temporary restriction does not unduly restrict access to lawful information by recipients of the service, having regard to the number of recipients affected and whether any adequate and readily accessible alternatives exist.

Where the Digital Services Coordinator considers that the conditions set out in the third subparagraph, points (a) and (b), have been met but it cannot further extend the period pursuant to the third subparagraph, it shall submit a new request to the competent judicial authority, as referred to in the first subparagraph, point (b).

4. The powers listed in paragraphs 1, 2 and 3 shall be without prejudice to Section 3.
5. The measures taken by the Digital Services Coordinators in the exercise of their powers listed in paragraphs 1, 2 and 3 shall be effective, dissuasive and proportionate, having regard, in particular, to the nature, gravity, recurrence and duration of the infringement or suspected infringement to which those measures relate, as well as the economic, technical and operational capacity of the provider of the intermediary services concerned where relevant.
6. Member States shall lay down specific rules and procedures for the exercise of the powers pursuant to paragraphs 1, 2 and 3 and shall ensure that any exercise of those powers is subject to adequate safeguards laid down in the applicable national law in compliance with the Charter and with the general principles of Union law. In particular, those measures shall only be taken in accordance with the right to respect for private life and the rights of defence, including the rights to be heard and of access to the file, and subject to the right to an effective judicial remedy of all affected parties.

#### Article 52

#### **Penalties**

1. Member States shall lay down the rules on penalties applicable to infringements of this Regulation by providers of intermediary services within their competence and shall take all the necessary measures to ensure that they are implemented in accordance with Article 51.
2. Penalties shall be effective, proportionate and dissuasive. Member States shall notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendments affecting them.
3. Member States shall ensure that the maximum amount of fines that may be imposed for a failure to comply with an obligation laid down in this Regulation shall be 6 % of the annual worldwide turnover of the provider of intermediary services concerned in the preceding financial year. Member States shall ensure that the maximum amount of the fine that may be imposed for the supply of incorrect, incomplete or misleading information, failure to reply or rectify incorrect, incomplete or misleading information and failure to submit to an inspection shall be 1 % of the annual income or worldwide turnover of the provider of intermediary services or person concerned in the preceding financial year.
4. Member States shall ensure that the maximum amount of a periodic penalty payment shall be 5 % of the average daily worldwide turnover or income of the provider of intermediary services concerned in the preceding financial year per day, calculated from the date specified in the decision concerned.

#### Article 53

#### **Right to lodge a complaint**

Recipients of the service and any body, organisation or association mandated to exercise the rights conferred by this Regulation on their behalf shall have the right to lodge a complaint against providers of intermediary services alleging an infringement of this Regulation with the Digital Services Coordinator of the Member State where the recipient of the service is located or established. The Digital Services Coordinator shall assess the complaint and, where appropriate, transmit it to the Digital Services Coordinator of establishment, accompanied, where considered appropriate, by an opinion. Where the complaint falls under the responsibility of another competent authority in its Member State, the Digital Services Coordinator receiving the complaint shall transmit it to that authority. During these proceedings, both parties shall have the right to be heard and receive appropriate information about the status of the complaint, in accordance with national law.

*Article 54***Compensation**

Recipients of the service shall have the right to seek, in accordance with Union and national law, compensation from providers of intermediary services, in respect of any damage or loss suffered due to an infringement by those providers of their obligations under this Regulation.

*Article 55***Activity reports**

1. Digital Services Coordinators shall draw up annual reports on their activities under this Regulation, including the number of complaints received pursuant to Article 53 and an overview of their follow-up. The Digital Services Coordinators shall make the annual reports available to the public in a machine-readable format, subject to the applicable rules on the confidentiality of information pursuant to Article 84, and shall communicate them to the Commission and to the Board.
2. The annual report shall also include the following information:
  - (a) the number and subject matter of orders to act against illegal content and orders to provide information issued in accordance with Articles 9 and 10 by any national judicial or administrative authority of the Member State of the Digital Services Coordinator concerned;
  - (b) the effects given to those orders, as communicated to the Digital Services Coordinator pursuant to Articles 9 and 10.
3. Where a Member State has designated several competent authorities pursuant to Article 49, it shall ensure that the Digital Services Coordinator draws up a single report covering the activities of all competent authorities and that the Digital Services Coordinator receives all relevant information and support needed to that effect from the other competent authorities concerned.

*SECTION 2****Competences, coordinated investigation and consistency mechanisms****Article 56***Competences**

1. The Member State in which the main establishment of the provider of intermediary services is located shall have exclusive powers to supervise and enforce this Regulation, except for the powers provided for in paragraphs 2, 3 and 4.
2. The Commission shall have exclusive powers to supervise and enforce Section 5 of Chapter III.
3. The Commission shall have powers to supervise and enforce this Regulation, other than those laid down in Section 5 of Chapter III thereof, against providers of very large online platforms and of very large online search engines.
4. Where the Commission has not initiated proceedings for the same infringement, the Member State in which the main establishment of the provider of very large online platform or of very large online search engine is located shall have powers to supervise and enforce the obligations under this Regulation, other than those laid down in Section 5 of Chapter III, with respect to those providers.
5. Member States and the Commission shall supervise and enforce the provisions of this Regulation in close cooperation.

6. Where a provider of intermediary services does not have an establishment in the Union, the Member State where its legal representative resides or is established or the Commission shall have powers, as applicable, in accordance with paragraphs 1 and 4 of this Article, to supervise and enforce the relevant obligations under this Regulation.

7. Where a provider of intermediary services fails to appoint a legal representative in accordance with Article 13, all Member States and, in case of a provider of a very large online platform or very large online search engine, the Commission shall have powers to supervise and enforce in accordance with this Article.

Where a Digital Services Coordinator intends to exercise its powers under this paragraph, it shall notify all other Digital Services Coordinators and the Commission, and ensure that the applicable safeguards afforded by the Charter are respected, in particular to avoid that the same conduct is sanctioned more than once for the infringement of the obligations laid down in this Regulation. Where the Commission intends to exercise its powers under this paragraph, it shall notify all other Digital Services Coordinators of that intention. Following the notification pursuant to this paragraph, other Member States shall not initiate proceedings for the same infringement as that referred to in the notification.

#### Article 57

### Mutual assistance

1. Digital Services Coordinators and the Commission shall cooperate closely and provide each other with mutual assistance in order to apply this Regulation in a consistent and efficient manner. Mutual assistance shall include, in particular, exchange of information in accordance with this Article and the duty of the Digital Services Coordinator of establishment to inform all Digital Services Coordinators of destination, the Board and the Commission about the opening of an investigation and the intention to take a final decision, including its assessment, in respect of a specific provider of intermediary services.

2. For the purpose of an investigation, the Digital Services Coordinator of establishment may request other Digital Services Coordinators to provide specific information in their possession as regards a specific provider of intermediary services or to exercise their investigative powers referred to in Article 51(1) with regard to specific information located in their Member State. Where appropriate, the Digital Services Coordinator receiving the request may involve other competent authorities or other public authorities of the Member State in question.

3. The Digital Services Coordinator receiving the request pursuant to paragraph 2 shall comply with such request and inform the Digital Services Coordinator of establishment about the action taken, without undue delay and no later than two months after its receipt, unless:

- (a) the scope or the subject matter of the request is not sufficiently specified, justified or proportionate in view of the investigative purposes; or
- (b) neither the requested Digital Service Coordinator nor other competent authority or other public authority of that Member State is in possession of the requested information nor can have access to it; or
- (c) the request cannot be complied with without infringing Union or national law.

The Digital Services Coordinator receiving the request shall justify its refusal by submitting a reasoned reply, within the period set out in the first subparagraph.

#### Article 58

### Cross-border cooperation among Digital Services Coordinators

1. Unless the Commission has initiated an investigation for the same alleged infringement, where a Digital Services Coordinator of destination has reason to suspect that a provider of an intermediary service has infringed this Regulation in a manner negatively affecting the recipients of the service in the Member State of that Digital Services Coordinator, it may request the Digital Services Coordinator of establishment to assess the matter and to take the necessary investigatory and enforcement measures to ensure compliance with this Regulation.

2. Unless the Commission has initiated an investigation for the same alleged infringement, and at the request of at least three Digital Services Coordinators of destination that have reason to suspect that a specific provider of intermediary services infringed this Regulation in a manner negatively affecting recipients of the service in their Member States, the Board may request the Digital Services Coordinator of establishment to assess the matter and take the necessary investigatory and enforcement measures to ensure compliance with this Regulation.
3. A request pursuant to paragraph 1 or 2 shall be duly reasoned, and shall at least indicate:
  - (a) the point of contact of the provider of the intermediary services concerned as provided for in Article 11;
  - (b) a description of the relevant facts, the provisions of this Regulation concerned and the reasons why the Digital Services Coordinator that sent the request, or the Board, suspects that the provider infringed this Regulation, including the description of the negative effects of the alleged infringement;
  - (c) any other information that the Digital Services Coordinator that sent the request, or the Board, considers relevant, including, where appropriate, information gathered on its own initiative or suggestions for specific investigatory or enforcement measures to be taken, including interim measures.
4. The Digital Services Coordinator of establishment shall take utmost account of the request pursuant to paragraphs 1 or 2 of this Article. Where it considers that it has insufficient information to act upon the request and has reasons to consider that the Digital Services Coordinator that sent the request, or the Board, could provide additional information, the Digital Services Coordinator of establishment may either request such information in accordance with Article 57 or, alternatively, may launch a joint investigation pursuant to Article 60(1) involving at least the requesting Digital Services Coordinator. The period laid down in paragraph 5 of this Article shall be suspended until that additional information is provided or until the invitation to participate in the joint investigation is refused.
5. The Digital Services Coordinator of establishment shall, without undue delay and in any event not later than two months following receipt of the request pursuant to paragraph 1 or 2, communicate to the Digital Services Coordinator that sent the request, and the Board, the assessment of the suspected infringement and an explanation of any investigatory or enforcement measures taken or envisaged in relation thereto to ensure compliance with this Regulation.

#### Article 59

#### **Referral to the Commission**

1. In the absence of a communication within the period laid down in Article 58(5), in the case of a disagreement of the Board with the assessment or the measures taken or envisaged pursuant to Article 58(5) or in the cases referred to in Article 60(3), the Board may refer the matter to the Commission, providing all relevant information. That information shall include at least the request or recommendation sent to the Digital Services Coordinator of establishment, the assessment by that Digital Services Coordinator, the reasons for the disagreement and any additional information supporting the referral.
2. The Commission shall assess the matter within two months following the referral of the matter pursuant to paragraph 1, after having consulted the Digital Services Coordinator of establishment.
3. Where, pursuant to paragraph 2 of this Article, the Commission considers that the assessment or the investigatory or enforcement measures taken or envisaged pursuant to Article 58(5) are insufficient to ensure effective enforcement or otherwise incompatible with this Regulation, it shall communicate its views to the Digital Services Coordinator of establishment and the Board and request the Digital Services Coordinator of establishment to review the matter.

The Digital Services Coordinator of establishment shall take the necessary investigatory or enforcement measures to ensure compliance with this Regulation, taking utmost account of the views and request for review by the Commission. The Digital Services Coordinator of establishment shall inform the Commission, as well as the requesting Digital Services Coordinator or the Board that took action pursuant to Article 58(1) or (2), about the measures taken within two months from that request for review.

#### Article 60

### Joint investigations

1. The Digital Services Coordinator of establishment may launch and lead joint investigations with the participation of one or more other Digital Services Coordinators concerned:

- (a) at its own initiative, to investigate an alleged infringement of this Regulation by a given provider of intermediary services in several Member States; or
- (b) upon recommendation of the Board, acting on the request of at least three Digital Services Coordinators alleging, based on a reasonable suspicion, an infringement by a given provider of intermediary services affecting recipients of the service in their Member States.

2. Any Digital Services Coordinator that proves that it has a legitimate interest in participating in a joint investigation pursuant to paragraph 1 may request to do so. The joint investigation shall be concluded within three months from its launch, unless otherwise agreed amongst the participants.

The Digital Services Coordinator of establishment shall communicate its preliminary position on the alleged infringement no later than one month after the end of the deadline referred to in the first subparagraph to all Digital Services Coordinators, the Commission and the Board. The preliminary position shall take into account the views of all other Digital Services Coordinators participating in the joint investigation. Where applicable, this preliminary position shall also set out the enforcement measures envisaged.

3. The Board may refer the matter to the Commission pursuant to Article 59, where:

- (a) the Digital Services Coordinator of establishment failed to communicate its preliminary position within the deadline set out in paragraph 2;
- (b) the Board substantially disagrees with the preliminary position communicated by the Digital Services Coordinator of establishment; or
- (c) the Digital Services Coordinator of establishment failed to initiate the joint investigation promptly following the recommendation by the Board pursuant to paragraph 1, point (b).

4. In carrying out the joint investigation, the participating Digital Services Coordinators shall cooperate in good faith, taking into account, where applicable, the indications of the Digital Services Coordinator of establishment and the Board's recommendation. The Digital Services Coordinators of destination participating in the joint investigation shall be entitled, at the request of or after having consulted the Digital Services Coordinator of establishment, to exercise their investigative powers referred to in Article 51(1) in respect of the providers of intermediary services concerned by the alleged infringement, with regard to information and premises located within their territory.

## SECTION 3

**European Board for Digital Services**

## Article 61

**European Board for Digital Services**

1. An independent advisory group of Digital Services Coordinators on the supervision of providers of intermediary services named 'European Board for Digital Services' (the 'Board') is established.
2. The Board shall advise the Digital Services Coordinators and the Commission in accordance with this Regulation to achieve the following objectives:
  - (a) contributing to the consistent application of this Regulation and effective cooperation of the Digital Services Coordinators and the Commission with regard to matters covered by this Regulation;
  - (b) coordinating and contributing to guidelines and analysis of the Commission and Digital Services Coordinators and other competent authorities on emerging issues across the internal market with regard to matters covered by this Regulation;
  - (c) assisting the Digital Services Coordinators and the Commission in the supervision of very large online platforms.

## Article 62

**Structure of the Board**

1. The Board shall be composed of Digital Services Coordinators who shall be represented by high-level officials. The failure by one or more Member States to designate a Digital Services Coordinator shall not prevent the Board from performing its tasks under this Regulation. Where provided for by national law, other competent authorities entrusted with specific operational responsibilities for the application and enforcement of this Regulation alongside the Digital Services Coordinator may participate in the Board. Other national authorities may be invited to the meetings, where the issues discussed are of relevance for them.
2. The Board shall be chaired by the Commission. The Commission shall convene the meetings and prepare the agenda in accordance with the tasks of the Board pursuant to this Regulation and in line with its rules of procedure. When the Board is requested to adopt a recommendation pursuant to this Regulation, it shall immediately make the request available to other Digital Services Coordinators through the information sharing system set out in Article 85.
3. Each Member State shall have one vote. The Commission shall not have voting rights.

The Board shall adopt its acts by simple majority. When adopting a recommendation to the Commission referred to in Article 36(1), first subparagraph, the Board shall vote within 48 hours after the request of the Chair of the Board.

4. The Commission shall provide administrative and analytical support for the activities of the Board pursuant to this Regulation.
5. The Board may invite experts and observers to attend its meetings, and may cooperate with other Union bodies, offices, agencies and advisory groups, as well as external experts as appropriate. The Board shall make the results of this cooperation publicly available.
6. The Board may consult interested parties, and shall make the results of such consultation publicly available.
7. The Board shall adopt its rules of procedure, following the consent of the Commission.

*Article 63***Tasks of the Board**

1. Where necessary to meet the objectives set out in Article 61(2), the Board shall in particular:
  - (a) support the coordination of joint investigations;
  - (b) support the competent authorities in the analysis of reports and results of audits of very large online platforms or of very large online search engines to be transmitted pursuant to this Regulation;
  - (c) issue opinions, recommendations or advice to Digital Services Coordinators in accordance with this Regulation, taking into account, in particular, the freedom to provide services of the providers of intermediary service;
  - (d) advise the Commission on the measures referred to in Article 66 and, adopt opinions concerning very large online platforms or very large online search engines in accordance with this Regulation;
  - (e) support and promote the development and implementation of European standards, guidelines, reports, templates and code of conducts in cooperation with relevant stakeholders as provided for in this Regulation, including by issuing opinions or recommendations on matters related to Article 44, as well as the identification of emerging issues, with regard to matters covered by this Regulation.
2. Digital Services Coordinators and, where applicable, other competent authorities that do not follow the opinions, requests or recommendations addressed to them adopted by the Board shall provide the reasons for this choice, including an explanation on the investigations, actions and the measures that they have implemented, when reporting pursuant to this Regulation or when adopting their relevant decisions, as appropriate.

## SECTION 4

***Supervision, investigation, enforcement and monitoring in respect of providers of very large online platforms and of very large online search engines****Article 64***Development of expertise and capabilities**

1. The Commission, in cooperation with the Digital Services Coordinators and the Board, shall develop Union expertise and capabilities, including, where appropriate, through the secondment of Member States' personnel.
2. In addition, the Commission, in cooperation with the Digital Services Coordinators and the Board, shall coordinate the assessment of systemic and emerging issues across the Union in relation to very large online platforms or very large online search engines with regard to matters covered by this Regulation.
3. The Commission may ask the Digital Services Coordinators, the Board and other Union bodies, offices and agencies with relevant expertise to support the assessment of systemic and emerging issues across the Union under this Regulation.
4. Member States shall cooperate with the Commission, in particular through their respective Digital Services Coordinators and other competent authorities, where applicable, including by making available their expertise and capabilities.

*Article 65***Enforcement of obligations of providers of very large online platforms and of very large online search engines**

1. For the purposes of investigating compliance of providers of very large online platforms and of very large online search engines with the obligations laid down in this Regulation, the Commission may exercise the investigatory powers laid down in this Section even before initiating proceedings pursuant to Article 66(2). It may exercise those powers on its own initiative or following a request pursuant to paragraph 2 of this Article.
2. Where a Digital Services Coordinator has reason to suspect that a provider of a very large online platform or of a very large online search engine has infringed the provisions of Section 5 of Chapter III or has systemically infringed any of the provisions of this Regulation in a manner that seriously affects recipients of the service in its Member State, it may send, through the information sharing system referred to in Article 85, a request to the Commission to assess the matter.
3. A request pursuant to paragraph 2 shall be duly reasoned and at least indicate:
  - (a) the point of contact of the provider of the very large online platform or of the very large online search engine concerned as provided for in Article 11;
  - (b) a description of the relevant facts, the provisions of this Regulation concerned and the reasons why the Digital Services Coordinator that sent the request suspects that the provider of the very large online platforms or of the very large online search engine concerned infringed this Regulation, including a description of the facts that show that the suspected infringement is of a systemic nature;
  - (c) any other information that the Digital Services Coordinator that sent the request considers relevant, including, where appropriate, information gathered on its own initiative.

*Article 66***Initiation of proceedings by the Commission and cooperation in investigation**

1. The Commission may initiate proceedings in view of the possible adoption of decisions pursuant to Articles 73 and 74 in respect of the relevant conduct by the provider of the very large online platform or of the very large online search engine that the Commission suspect of having infringed any of the provisions of this Regulation.
2. Where the Commission decides to initiate proceedings pursuant to paragraph 1 of this Article, it shall notify all Digital Services Coordinators and the Board through the information sharing system referred to in Article 85, as well as the provider of the very large online platform or of the very large online search engine concerned.

The Digital Services Coordinators shall, without undue delay after being informed of initiation of the proceedings, transmit to the Commission any information they hold about the infringement at stake.

The initiation of proceedings pursuant to paragraph 1 of this Article by the Commission shall relieve the Digital Services Coordinator, or any competent authority where applicable, of its powers to supervise and enforce provided for in this Regulation pursuant to Article 56(4).

3. In the exercise of its powers of investigation under this Regulation the Commission may request the individual or joint support of any Digital Services Coordinators concerned by the suspected infringement, including the Digital Services Coordinator of establishment. The Digital Services Coordinators that have received such a request, and, where involved by the Digital Services Coordinator, any other competent authority, shall cooperate sincerely and in a timely manner with the Commission and shall be entitled to exercise their investigative powers referred to in Article 51(1) in respect of the provider of the very large online platform or of the very large online search engine at stake, with regard to information, persons and premises located within the territory of their Member State and in accordance with the request.

4. The Commission shall provide the Digital Services Coordinator of establishment and the Board with all relevant information about the exercise of the powers referred to in Articles 67 to 72 and its preliminary findings referred to in Article 79(1). The Board shall submit its views on those preliminary findings to the Commission within the period set pursuant to Article 79(2). The Commission shall take utmost account of any views of the Board in its decision.

#### Article 67

##### **Requests for information**

1. In order to carry out the tasks assigned to it under this Section, the Commission may, by simple request or by decision, require the provider of the very large online platform or of the very large online search engine concerned, as well as any other natural or legal person acting for purposes related to their trade, business, craft or profession that may be reasonably aware of information relating to the suspected infringement, including organisations performing the audits referred to in Article 37 and Article 75(2), to provide such information within a reasonable period.

2. When sending a simple request for information to the provider of the very large online platform or of the very large online search engine concerned or other person referred to in paragraph 1 of this Article, the Commission shall state the legal basis and the purpose of the request, specify what information is required and set the period within which the information is to be provided, and the fines provided for in Article 74 for supplying incorrect, incomplete or misleading information.

3. Where the Commission requires the provider of the very large online platform or of the very large online search engine concerned or other person referred to in paragraph 1 of this Article to supply information by decision, it shall state the legal basis and the purpose of the request, specify what information is required and set the period within which it is to be provided. It shall also indicate the fines provided for in Article 74 and indicate or impose the periodic penalty payments provided for in Article 76. It shall further indicate the right to have the decision reviewed by the Court of Justice of the European Union.

4. The providers of the very large online platform or of the very large online search engine concerned or other person referred to in paragraph 1 or their representatives and, in the case of legal persons, companies or firms, or where they have no legal personality, the persons authorised to represent them by law or by their constitution shall supply the information requested on behalf of the provider of the very large online platform or of the very large online search engine concerned or other person referred to in paragraph 1. Lawyers duly authorised to act may supply the information on behalf of their clients. The latter shall remain fully responsible if the information supplied is incomplete, incorrect or misleading.

5. At the request of the Commission, the Digital Services Coordinators and other competent authorities shall provide the Commission with all necessary information to carry out the tasks assigned to it under this Section.

6. The Commission shall, without undue delay after sending the simple request or the decision referred to in paragraph 1 of this Article, send a copy thereof to the Digital Services Coordinators, through the information sharing system referred to in Article 85.

#### Article 68

##### **Power to take interviews and statements**

1. In order to carry out the tasks assigned to it under this Section, the Commission may interview any natural or legal person who consents to being interviewed for the purpose of collecting information, relating to the subject-matter of an investigation, in relation to the suspected infringement. The Commission shall be entitled to record such interview by appropriate technical means.

2. If the interview referred to in paragraph 1 is conducted on other premises than those of the Commission, the Commission shall inform the Digital Services Coordinator of the Member State in the territory of which the interview takes place. If so requested by that Digital Services Coordinator, its officials may assist the officials and other accompanying persons authorised by the Commission to conduct the interview.

#### Article 69

### Power to conduct inspections

1. In order to carry out the tasks assigned to it under this Section, the Commission may conduct all necessary inspections at the premises of the provider of the very large online platform or of the very large online search engine concerned or of another person referred to in Article 67(1).

2. The officials and other accompanying persons authorised by the Commission to conduct an inspection shall be empowered to:

- (a) enter any premises, land and means of transport of the provider of the very large online platform or of the very large online search engine concerned or of the other person concerned;
- (b) examine the books and other records related to the provision of the service concerned, irrespective of the medium on which they are stored;
- (c) take or obtain in any form copies of or extracts from such books or other records;
- (d) require the provider of the very large online platform or of the very large online search engine or the other person concerned to provide access to and explanations on its organisation, functioning, IT system, algorithms, data-handling and business practices and to record or document the explanations given;
- (e) seal any premises used for purposes related to the trade, business, craft or profession of the provider of the very large online platform or of the very large online search engine or of the other person concerned, as well as books or other records, for the period and to the extent necessary for the inspection;
- (f) ask any representative or member of staff of the provider of the very large online platform or of the very large online search engine or the other person concerned for explanations on facts or documents relating to the subject-matter and purpose of the inspection and to record the answers;
- (g) address questions to any such representative or member of staff relating to the subject-matter and purpose of the inspection and to record the answers.

3. Inspections may be carried out with the assistance of auditors or experts appointed by the Commission pursuant to Article 72(2), and of Digital Services Coordinator or other competent national authorities of the Member State in the territory of which the inspection is conducted.

4. Where the production of required books or other records related to the provision of the service concerned is incomplete or where the answers to questions asked under paragraph 2 of this Article are incorrect, incomplete or misleading, the officials and other accompanying persons authorised by the Commission to conduct an inspection shall exercise their powers upon production of a written authorisation specifying the subject matter and purpose of the inspection and the penalties provided for in Articles 74 and 76. In good time before the inspection, the Commission shall inform the Digital Services Coordinator of the Member State in the territory in which the inspection is to be conducted thereof.

5. During inspections, the officials and other accompanying persons authorised by the Commission, the auditors and experts appointed by the Commission, the Digital Services Coordinator or the other competent authorities of the Member State in the territory of which the inspection is conducted may require the provider of the very large online platform or of the very large online search engine or other person concerned to provide explanations on its organisation, functioning, IT system, algorithms, data-handling and business conducts, and may address questions to its key personnel.

6. The provider of the very large online platform or of the very large online search engine or other natural or legal person concerned shall be required to submit to an inspection ordered by decision of the Commission. The decision shall specify the subject matter and purpose of the inspection, set the date on which it is to begin and indicate the penalties provided for in Articles 74 and 76 and the right to have the decision reviewed by the Court of Justice of the European Union. The Commission shall consult the Digital Services Coordinator of the Member State on territory of which the inspection is to be conducted prior to taking that decision.

7. Officials of, and other persons authorised or appointed by, the Digital Services Coordinator of the Member State on the territory of which the inspection is to be conducted shall, at the request of that Digital Services Coordinator or of the Commission, actively assist the officials and other accompanying persons authorised by the Commission in relation to the inspection. To this end, they shall have the powers listed in paragraph 2.

8. Where the officials and other accompanying persons authorised by the Commission find that the provider of the very large online platform or of the very large online search engine or the other person concerned opposes an inspection ordered pursuant to this Article, the Member State in the territory of which the inspection is to be conducted shall, at the request of those officials or other accompanying persons and in accordance with the national law of the Member State, afford them necessary assistance, including, where appropriate under that national law, in the form of coercive measures taken by a competent law enforcement authority, so as to enable them to conduct the inspection.

9. If the assistance provided for in paragraph 8 requires authorisation from a national judicial authority in accordance with the national law of the Member State concerned, such authorisation shall be applied for by the Digital Services Coordinator of that Member State at the request of the officials and other accompanying persons authorised by the Commission. Such authorisation may also be applied for as a precautionary measure.

10. Where the authorisation referred to in paragraph 9 is applied for, the national judicial authority before which a case has been brought shall verify that the Commission decision ordering the inspection is authentic and that the coercive measures envisaged are neither arbitrary nor excessive having regard to the subject matter of the inspection. When conducting such verification, the national judicial authority may ask the Commission, directly or through the Digital Services Coordinators of the Member State concerned, for detailed explanations, in particular those concerning the grounds on which the Commission suspects an infringement of this Regulation, concerning the seriousness of the suspected infringement and concerning the nature of the involvement of the provider of the very large online platform or of the very large online search engine or of the other person concerned. However, the national judicial authority shall not call into question the necessity for the inspection nor demand information from the case file of the Commission. The lawfulness of the Commission decision shall be subject to review only by the Court of Justice of the European Union.

#### Article 70

#### **Interim measures**

1. In the context of proceedings which may lead to the adoption of a decision of non-compliance pursuant to Article 73(1), where there is an urgency due to the risk of serious damage for the recipients of the service, the Commission may, by decision, order interim measures against the provider of the very large online platform or of the very large online search engine concerned on the basis of a *prima facie* finding of an infringement.

2. A decision under paragraph 1 shall apply for a specified period of time and may be renewed in so far this is necessary and appropriate.

*Article 71***Commitments**

1. If, during proceedings under this Section, the provider of the very large online platform or of the very large online search engine concerned offers commitments to ensure compliance with the relevant provisions of this Regulation, the Commission may by decision make those commitments binding on the provider of the very large online platform or of the very large online search engine concerned and declare that there are no further grounds for action.
2. The Commission may, upon request or on its own initiative, reopen the proceedings:
  - (a) where there has been a material change in any of the facts on which the decision was based;
  - (b) where the provider of the very large online platform or of the very large online search engine concerned acts contrary to its commitments; or
  - (c) where the decision was based on incomplete, incorrect or misleading information provided by the provider of the very large online platform or of the very large online search engine concerned or other person referred to in Article 67(1).
3. Where the Commission considers that the commitments offered by the provider of the very large online platform or of the very large online search engine concerned are unable to ensure effective compliance with the relevant provisions of this Regulation, it shall reject those commitments in a reasoned decision when concluding the proceedings.

*Article 72***Monitoring actions**

1. For the purposes of carrying out the tasks assigned to it under this Section, the Commission may take the necessary actions to monitor the effective implementation and compliance with this Regulation by providers of the very large online platform and of the very large online search engines. The Commission may order them to provide access to, and explanations relating to, its databases and algorithms. Such actions may include, imposing an obligation on the provider of the very large online platform or of the very large online search engine to retain all documents deemed to be necessary to assess the implementation of and compliance with the obligations under this Regulation.
2. The actions pursuant to paragraph 1 may include the appointment of independent external experts and auditors, as well as experts and auditors from competent national authorities with the agreement of the authority concerned, to assist the Commission in monitoring the effective implementation and compliance with the relevant provisions of this Regulation and to provide specific expertise or knowledge to the Commission.

*Article 73***Non-compliance**

1. The Commission shall adopt a non-compliance decision where it finds that the provider of the very large online platform or of the very large online search engine concerned does not comply with one or more of the following:
  - (a) the relevant provisions of this Regulation;
  - (b) interim measures ordered pursuant to Article 70;
  - (c) commitments made binding pursuant to Article 71.

2. Before adopting the decision pursuant to paragraph 1, the Commission shall communicate its preliminary findings to the provider of the very large online platform or of the very large online search engine concerned. In the preliminary findings, the Commission shall explain the measures that it considers taking, or that it considers that the provider of the very large online platform or of the very large online search engine concerned should take, in order to effectively address the preliminary findings.

3. In the decision adopted pursuant to paragraph 1 the Commission shall order the provider of the very large online platform or of the very large online search engine concerned to take the necessary measures to ensure compliance with the decision pursuant to paragraph 1 within a reasonable period specified therein and to provide information on the measures that that provider intends to take to comply with the decision.

4. The provider of the very large online platform or of the very large online search engine concerned shall provide the Commission with a description of the measures it has taken to ensure compliance with the decision pursuant to paragraph 1 upon their implementation.

5. Where the Commission finds that the conditions of paragraph 1 are not met, it shall close the investigation by a decision. The decision shall apply with immediate effect.

#### Article 74

##### Fines

1. In the decision referred to in Article 73, the Commission may impose on the provider of the very large online platform or of the very large online search engine concerned fines not exceeding 6 % of its total worldwide annual turnover in the preceding financial year where it finds that the provider, intentionally or negligently:

- (a) infringes the relevant provisions of this Regulation;
- (b) fails to comply with a decision ordering interim measures under Article 70; or
- (c) fails to comply with a commitment made binding by a decision pursuant to Article 71.

2. The Commission may adopt a decision imposing on the provider of the very large online platform or of the very large online search engine concerned or on another natural or legal person referred to in Article 67(1) fines not exceeding 1 % of the total annual income or worldwide turnover in the preceding financial year, where they intentionally or negligently:

- (a) supply incorrect, incomplete or misleading information in response to a simple request or request by a decision pursuant to Article 67;
- (b) fail to reply to the request for information by decision within the set period;
- (c) fail to rectify within the period set by the Commission, incorrect, incomplete or misleading information given by a member of staff, or fail or refuse to provide complete information;
- (d) refuse to submit to an inspection pursuant to Article 69;
- (e) fail to comply with the measures adopted by the Commission pursuant to Article 72; or
- (f) fail to comply with the conditions for access to the Commission's file pursuant to Article 79(4).

3. Before adopting the decision pursuant to paragraph 2 of this Article, the Commission shall communicate its preliminary findings to the provider of the very large online platform or of the very large online search engine concerned or to another person referred to in Article 67(1).

4. In fixing the amount of the fine, the Commission shall have regard to the nature, gravity, duration and recurrence of the infringement and, for fines imposed pursuant to paragraph 2, the delay caused to the proceedings.

*Article 75***Enhanced supervision of remedies to address infringements of obligations laid down in Section 5 of Chapter III**

1. When adopting a decision pursuant to Article 73 in relation to an infringement by a provider of a very large online platform or of a very large online search engine of any of the provisions of Section 5 of Chapter III, the Commission shall make use of the enhanced supervision system laid down in this Article. When doing so, it shall take utmost account of any opinion of the Board pursuant to this Article.

2. In the decision referred to in Article 73, the Commission shall require the provider of a very large online platform or of a very large online search engine concerned to draw up and communicate, within a reasonable period specified in the decision, to the Digital Services Coordinators, the Commission and the Board an action plan setting out the necessary measures which are sufficient to terminate or remedy the infringement. Those measures shall include a commitment to perform an independent audit in accordance with Article 37(3) and (4) on the implementation of the other measures, and shall specify the identity of the auditors, as well as the methodology, timing and follow-up of the audit. The measures may also include, where appropriate, a commitment to participate in a relevant code of conduct, as provided for in Article 45.

3. Within one month following receipt of the action plan, the Board shall communicate its opinion on the action plan to the Commission. Within one month following receipt of that opinion, the Commission shall decide whether the measures set out in the action plan are sufficient to terminate or remedy the infringement, and shall set a reasonable period for its implementation. The possible commitment to adhere to relevant codes of conduct shall be taken into account in that decision. The Commission shall subsequently monitor the implementation of the action plan. To that end, the provider of a very large online platform or of a very large online search engine concerned shall communicate the audit report to the Commission without undue delay after it becomes available, and shall keep the Commission up to date on steps taken to implement the action plan. The Commission may, where necessary for such monitoring, require the provider of a very large online platform or of a very large online search engine concerned to provide additional information within a reasonable period set by the Commission.

The Commission shall keep the Board and the Digital Services Coordinators informed about the implementation of the action plan, and about its monitoring thereof.

4. The Commission may take necessary measures in accordance with this Regulation, in particular Article 76(1), point (e), and Article 82(1), where:

- (a) the provider of the very large online platform or of the very large online search engine concerned fails to provide any action plan, the audit report, the necessary updates or any additional information required, within the applicable period;
- (b) the Commission rejects the proposed action plan because it considers that the measures set out therein are insufficient to terminate or remedy the infringement; or
- (c) the Commission considers, on the basis of the audit report, any updates or additional information provided or any other relevant information available to it, that the implementation of the action plan is insufficient to terminate or remedy the infringement.

*Article 76***Periodic penalty payments**

1. The Commission may adopt a decision, imposing on the provider of the very large online platform or of the very large online search engine concerned or other person referred to in Article 67(1), as applicable, periodic penalty payments not exceeding 5 % of the average daily income or worldwide annual turnover in the preceding financial year per day, calculated from the date appointed by the decision, in order to compel them to:

- (a) supply correct and complete information in response to a decision requiring information pursuant to Article 67;
- (b) submit to an inspection which it has ordered by decision pursuant to Article 69;

- (c) comply with a decision ordering interim measures pursuant to Article 70(1);
- (d) comply with commitments made legally binding by a decision pursuant to Article 71(1);
- (e) comply with a decision pursuant to Article 73(1), including where applicable the requirements it contains relating to the action plan referred to in Article 75.

2. Where the provider of the very large online platform or of the very large online search engine concerned or other person referred to in Article 67(1) has satisfied the obligation which the periodic penalty payment was intended to enforce, the Commission may fix the definitive amount of the periodic penalty payment at a figure lower than that under the original decision.

#### Article 77

##### **Limitation period for the imposition of penalties**

1. The powers conferred on the Commission by Articles 74 and 76 shall be subject to a limitation period of five years.
2. Time shall begin to run on the day on which the infringement is committed. However, in the case of continuing or repeated infringements, time shall begin to run on the day on which the infringement ceases.
3. Any action taken by the Commission or by the Digital Services Coordinator for the purpose of the investigation or proceedings in respect of an infringement shall interrupt the limitation period for the imposition of fines or periodic penalty payments. Actions which interrupt the limitation period shall include, in particular, the following:
  - (a) requests for information by the Commission or by a Digital Services Coordinator;
  - (b) inspection;
  - (c) the opening of a proceeding by the Commission pursuant to Article 66(1).
4. Each interruption shall start time running afresh. However, the limitation period for the imposition of fines or periodic penalty payments shall expire at the latest on the day on which a period equal to twice the limitation period has elapsed without the Commission having imposed a fine or a periodic penalty payment. That period shall be extended by the time during which the limitation period has been suspended pursuant to paragraph 5.
5. The limitation period for the imposition of fines or periodic penalty payments shall be suspended for as long as the decision of the Commission is the subject of proceedings pending before the Court of Justice of the European Union.

#### Article 78

##### **Limitation period for the enforcement of penalties**

1. The power of the Commission to enforce decisions taken pursuant to Articles 74 and 76 shall be subject to a limitation period of five years.
2. Time shall begin to run on the day on which the decision becomes final.
3. The limitation period for the enforcement of penalties shall be interrupted:
  - (a) by notification of a decision varying the original amount of the fine or periodic penalty payment or refusing an application for variation;
  - (b) by any action of the Commission, or of a Member State acting at the request of the Commission, designed to enforce payment of the fine or periodic penalty payment.
4. Each interruption shall start time running afresh.

5. The limitation period for the enforcement of penalties shall be suspended for so long as:
- (a) time to pay is allowed;
  - (b) enforcement of payment is suspended pursuant to a decision of the Court of Justice of the European Union or to a decision of a national court.

#### Article 79

##### **Right to be heard and access to the file**

1. Before adopting a decision pursuant to Article 73(1), Article 74 or 76, the Commission shall give the provider of the very large online platform or of the very large online search engine concerned or other person referred to in Article 67(1) the opportunity of being heard on:
  - (a) preliminary findings of the Commission, including any matter to which the Commission has taken objections; and
  - (b) measures that the Commission may intend to take in view of the preliminary findings referred to point (a).
2. The provider of the very large online platform or of the very large online search engine concerned or other person referred to in Article 67(1) may submit its observations on the Commission's preliminary findings within a reasonable period set by the Commission in its preliminary findings, which may not be less than 14 days.
3. The Commission shall base its decisions only on objections on which the parties concerned have been able to comment.
4. The rights of defence of the parties concerned shall be fully respected in the proceedings. They shall be entitled to have access to the Commission's file under the terms of a negotiated disclosure, subject to the legitimate interest of the provider of the very large online platform or of the very large online search engine or other person concerned in the protection of their business secrets. The Commission shall have the power to adopt decisions setting out such terms of disclosure in case of disagreement between the parties. The right of access to the file of the Commission shall not extend to confidential information and internal documents of the Commission, the Board, Digital Service Coordinators, other competent authorities or other public authorities of the Member States. In particular, the right of access shall not extend to correspondence between the Commission and those authorities. Nothing in this paragraph shall prevent the Commission from disclosing and using information necessary to prove an infringement.
5. The information collected pursuant to Articles 67, 68 and 69 shall be used only for the purpose of this Regulation.

#### Article 80

##### **Publication of decisions**

1. The Commission shall publish the decisions it adopts pursuant to Article 70(1), Article 71(1) and Articles 73 to 76. Such publication shall state the names of the parties and the main content of the decision, including any penalties imposed.
2. The publication shall have regard to the rights and legitimate interests of the provider of the very large online platform or of the very large online search engine concerned, any other person referred to in Article 67(1) and any third parties in the protection of their confidential information.

#### Article 81

##### **Review by the Court of Justice of the European Union**

In accordance with Article 261 TFEU, the Court of Justice of the European Union has unlimited jurisdiction to review decisions by which the Commission has imposed fines or periodic penalty payments. It may cancel, reduce or increase the fine or periodic penalty payment imposed.

*Article 82***Requests for access restrictions and cooperation with national courts**

1. Where all powers pursuant to this Section to bring about the cessation of an infringement of this Regulation have been exhausted, the infringement persists and causes serious harm which cannot be avoided through the exercise of other powers available under Union or national law, the Commission may request the Digital Services Coordinator of establishment of the provider of the very large online platform or of the very large online search engine concerned to act pursuant to Article 51(3).

Prior to making such request to the Digital Services Coordinator, the Commission shall invite interested parties to submit written observations within a period that shall not be less than 14 working days, describing the measures it intends to request and identifying the intended addressee or addressees thereof.

2. Where the coherent application of this Regulation so requires, the Commission, acting on its own initiative, may submit written observations to the competent judicial authority referred to Article 51(3). With the permission of the judicial authority in question, it may also make oral observations.

For the purpose of the preparation of its observations only, the Commission may request that judicial authority to transmit or ensure the transmission to it of any documents necessary for the assessment of the case.

3. When a national court rules on a matter which is already the subject matter of a decision adopted by the Commission under this Regulation, that national court shall not take any decision which runs counter to that Commission decision. National courts shall also avoid taking decisions which could conflict with a decision contemplated by the Commission in proceedings it has initiated under this Regulation. To that effect, a national court may assess whether it is necessary to stay its proceedings. This is without prejudice to Article 267 TFEU.

*Article 83***Implementing acts relating to Commission intervention**

In relation to the Commission intervention covered by this Section, the Commission may adopt implementing acts concerning the practical arrangements for:

- (a) the proceedings pursuant to Articles 69 and 72;
- (b) the hearings provided for in Article 79;
- (c) the negotiated disclosure of information provided for in Article 79.

Before the adoption of any measures pursuant to the first paragraph of this Article, the Commission shall publish a draft thereof and invite all interested parties to submit their comments within the period set out therein, which shall not be less than one month. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 88.

*SECTION 5****Common provisions on enforcement****Article 84***Professional secrecy**

Without prejudice to the exchange and to the use of information referred to in this Chapter, the Commission, the Board, Member States' competent authorities and their respective officials, servants and other persons working under their supervision, and any other natural or legal person involved, including auditors and experts appointed pursuant to Article 72(2), shall not disclose information acquired or exchanged by them pursuant to this Regulation and of the kind covered by the obligation of professional secrecy.

*Article 85***Information sharing system**

1. The Commission shall establish and maintain a reliable and secure information sharing system supporting communications between Digital Services Coordinators, the Commission and the Board. Other competent authorities may be granted access to this system where necessary for them to carry out the tasks conferred to them in accordance with this Regulation.
2. The Digital Services Coordinators, the Commission and the Board shall use the information sharing system for all communications pursuant to this Regulation.
3. The Commission shall adopt implementing acts laying down the practical and operational arrangements for the functioning of the information sharing system and its interoperability with other relevant systems. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 88.

*Article 86***Representation**

1. Without prejudice to Directive (EU) 2020/1828 or to any other type of representation under national law, recipients of intermediary services shall at least have the right to mandate a body, organisation or association to exercise the rights conferred by this Regulation on their behalf, provided the body, organisation or association meets all of the following conditions:
  - (a) it operates on a not-for-profit basis;
  - (b) it has been properly constituted in accordance with the law of a Member State;
  - (c) its statutory objectives include a legitimate interest in ensuring that this Regulation is complied with.
2. Providers of online platforms shall take the necessary technical and organisational measures to ensure that complaints submitted by bodies, organisations or associations referred to in paragraph 1 of this Article on behalf of recipients of the service through the mechanisms referred to in Article 20(1) are processed and decided upon with priority and without undue delay.

*SECTION 6****Delegated and implementing acts****Article 87***Exercise of the delegation**

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The delegation of power referred to in Articles 24, 33, 37, 40 and 43 shall be conferred on the Commission for five years starting from 16 November 2022. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

3. The delegation of power referred to in Articles 24, 33, 37, 40 and 43 may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.
5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
6. A delegated act adopted pursuant to Articles 24, 33, 37, 40 and 43 shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

#### Article 88

##### **Committee procedure**

1. The Commission shall be assisted by a committee ('the Digital Services Committee'). That Committee shall be a Committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 4 of Regulation (EU) No 182/2011 shall apply.

#### CHAPTER V

##### **FINAL PROVISIONS**

#### Article 89

##### **Amendments to Directive 2000/31/EC**

1. Articles 12 to 15 of Directive 2000/31/EC are deleted.
2. References to Articles 12 to 15 of Directive 2000/31/EC shall be construed as references to Articles 4, 5, 6 and 8 of this Regulation, respectively.

#### Article 90

##### **Amendment to Directive (EU) 2020/1828**

In Annex I to Directive (EU) 2020/1828, the following point is added:

'(68) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1).'

#### Article 91

##### **Review**

1. By 18 February 2027, the Commission shall evaluate and report to the European Parliament, the Council and the European Economic and Social Committee on the potential effect of this Regulation on the development and economic growth of small and medium-sized enterprises.

By 17 November 2025, the Commission shall evaluate and report to the European Parliament, the Council and the European Economic and Social Committee on:

- (a) the application of Article 33, including the scope of providers of intermediary services covered by the obligations set out in Section 5 of Chapter III of this Regulation;
- (b) the way that this Regulation interacts with other legal acts, in particular the acts referred to in Article 2(3) and (4).

2. By 17 November 2027, and every five years thereafter, the Commission shall evaluate this Regulation, and report to the European Parliament, the Council and the European Economic and Social Committee.

This report shall address in particular:

- (a) the application of paragraph 1, second subparagraph, points (a) and (b);
- (b) the contribution of this Regulation to the deepening and efficient functioning of the internal market for intermediary services, in particular as regards the cross-border provision of digital services;
- (c) the application of Articles 13, 16, 20, 21, 45 and 46;
- (d) the scope of the obligations on small and micro enterprises;
- (e) the effectiveness of the supervision and enforcement mechanisms;
- (f) the impact on the respect for the right to freedom of expression and information.

3. Where appropriate, the report referred to in paragraphs 1 and 2 shall be accompanied by a proposal for amendment of this Regulation.

4. The Commission shall, in the report referred to in paragraph 2 of this Article, also evaluate and report on the annual reports on their activities by the Digital Services Coordinators provided to the Commission and the Board pursuant to Article 55(1).

5. For the purpose of paragraph 2, Member States and the Board shall send information on the request of the Commission.

6. In carrying out the evaluations referred to in paragraph 2, the Commission shall take into account the positions and findings of the European Parliament, the Council, and other relevant bodies or sources, and shall pay specific attention to small and medium-sized enterprises and the position of new competitors.

7. By 18 February 2027, the Commission, after consulting the Board, shall carry out an assessment of the functioning of the Board and of the application of Article 43, and shall report it to the European Parliament, the Council and the European Economic and Social Committee, taking into account the first years of application of the Regulation. On the basis of the findings and taking utmost account of the opinion of the Board, that report shall, where appropriate, be accompanied by a proposal for amendment of this Regulation with regard to the structure of the Board.

#### *Article 92*

#### **Anticipated application to providers of very large online platforms and of very large online search engines**

This Regulation shall apply to providers of very large online platforms and of very large online search engines designated pursuant to Article 33(4) from four months after the notification to the provider concerned referred to in Article 33(6) where that date is earlier than 17 February 2024.

*Article 93***Entry into force and application**

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.
2. This Regulation shall apply from 17 February 2024.

However, Article 24(2), (3) and (6), Article 33(3) to (6), Article 37(7), Article 40(13), Article 43 and Sections 4, 5 and 6 of Chapter IV shall apply from 16 November 2022.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Strasbourg, 19 October 2022.

*For the European Parliament*  
*The President*  
R. METSOLA

*For the Council*  
*The President*  
M. BEK

---