



EUROPEAN  
COMMISSION

Brussels, **XXX**  
COM(2020) 825

2020/0361 (COD)  
**SENSITIVE\***: *Cabinets*  
*UNTIL ADOPTION*

Proposal for a

**REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**on a Single Market For Digital Services (Digital Services Act) and amending Directive  
2000/31/EC**

(Text with EEA relevance)

---

\* Distribution only on a 'Need to know' basis - Do not read or carry openly in public places. Must be stored securely and encrypted in storage and transmission. Destroy copies by shredding or secure deletion. Full handling instructions <https://europa.eu/db43PX>

## **EXPLANATORY MEMORANDUM**

### **1. CONTEXT OF THE PROPOSAL**

#### **Reasons for and objectives of the proposal**

Since the adoption of Directive 2000/31/EC<sup>1</sup> (the “e-Commerce Directive”), new and innovative information society (digital) services have emerged, changing the daily lives of Union citizens and shaping and transforming how they communicate, connect, consume and do business. Those services have contributed deeply to societal and economic transformations in the Union and across the world. At the same time, the use of those services has also become the source of new risks and challenges, both for society as a whole and individuals using such services. The coronavirus crisis has shown the importance of digital technologies in all aspects of modern life. It has clearly shown the dependency of our economy and society on digital services and highlighted both the benefits and the risks stemming from the current framework for the functioning of digital services.

In the Communication ‘Shaping Europe’s Digital Future’<sup>2</sup>, the Commission committed to update the horizontal rules that define the responsibilities and obligations of providers of digital services, and online platforms in particular.

In doing so, the Commission has taken account of the issues identified in the European Parliament’s own initiative reports and analysed the proposals therein. The European Parliament adopted two resolutions on the basis of Article 225 of the Treaty on the Functioning of the European Union (TFEU) on the ‘Digital Services Act – Improving the functioning of the Single Market’<sup>3</sup> and on the ‘Digital Services Act: adapting commercial and civil law rules for commercial entities operating online’<sup>4</sup>. The European Parliament also adopted a resolution under the non-legislative procedure on the ‘Digital Services Act and fundamental rights issues posed’<sup>5</sup>. In substance, the resolutions are complementary in many aspects. They include a strong call for maintaining the core principles of the e-Commerce Directive and for protecting fundamental rights in the online environment, as well as online anonymity wherever technically possible. They call for transparency, information obligations and accountability for digital services providers and advocate for effective obligations to tackle illegal content online. They also advocate for public oversight at EU and national level, and cooperation between competent authorities across jurisdictions in enforcing the law, especially when addressing cross-border matters.

The resolution on ‘Digital Services Act – Improving the functioning of the Single Market’ calls for an ambitious reform of the existing EU e-commerce legal framework while maintaining the core principles of its liability regime, the prohibition of general monitoring and the internal market clause, which it considers to be still valid today. Confirming the objectives of the e-Commerce Directive, the resolution calls for measures which have

<sup>1</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*).

<sup>2</sup> [https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020\\_en\\_4.pdf](https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf)

<sup>3</sup> European Parliament, Resolution on improving the functioning of the Single Market (2020/2018(INL)).

<sup>4</sup> European Parliament, Resolution on adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL)).

<sup>5</sup> European Parliament, Resolution on the Digital Services Act and fundamental rights issues posed (2020/2022(INI))

consumer protection at their core, by including a detailed section on online marketplaces, and which ensure consumer trust in the digital economy, while respecting users' fundamental rights. The resolution also advocates for rules to underpin a competitive digital environment in Europe, and envisages the Digital Services Act as a standard-setter at global level.

The resolution on 'Digital Services Act: adapting commercial and civil law rules for commercial entities operating online' calls for more fairness, transparency and accountability for digital services' content moderation processes, ensuring that fundamental rights are respected, and guaranteeing independent recourse to judicial redress. The resolution also includes the request for a detailed 'notice-and-action' mechanism addressing illegal content, comprehensive rules about online advertising, including targeted advertising, and enabling the development and use of smart contracts.

The non-legislative resolution on the 'Digital Services Act and fundamental rights issues posed' highlights the need for legal clarity for platforms and users, and respect for fundamental rights given the rapid development of technology. It calls for harmonised rules for addressing illegal content online and for liability exemptions and content moderation. The resolution also includes clear reporting and transparency responsibilities for platforms and authorities. The Council's Conclusions<sup>6</sup> also welcomed the Commission's announcement of a Digital Services Act, emphasising 'the need for clear and harmonised evidence-based rules on responsibilities and accountability for digital services that would guarantee internet intermediaries an appropriate level of legal certainty', and stressing 'the need to enhance European capabilities and the cooperation of national authorities, preserving and reinforcing the fundamental principles of the Single Market and the need to enhance citizens' safety and to protect their rights in the digital sphere across the Single Market'. This call for action was reiterated in the Council's Conclusions of 2 October 2020<sup>7</sup>.

Building on the key principles set out in the e-Commerce Directive, which remain valid today, this proposal seeks to ensure the best conditions for the provision of innovative digital services in the internal market, to contribute to online safety and the protection of fundamental rights, and to set a robust and durable governance structure for the effective supervision of providers of intermediary services.

The proposal defines clear responsibilities and accountability for providers of intermediary services, and in particular online platforms, such as social media and marketplaces. By setting out clear due-diligence obligations for certain intermediary services, including notice-and-action procedures for illegal content and the possibility to challenge the platforms' content moderation decisions, the proposal seeks to improve users' safety online across the entire Union and improve the protection of their fundamental rights. Furthermore, an obligation for certain online platforms to receive, store and partially verify and publish information on traders using their services will ensure a safer and more transparent online environment for consumers. Recognising the particular impact of very large online platforms on our economy and society, the proposal sets a higher standard of transparency and accountability on how the providers of such platforms moderate content, on advertising and on algorithmic processes. It sets obligations to assess the risks their systems pose to develop appropriate risk management tools to protect the integrity of their services against the use of manipulative techniques. The operational threshold for service providers in scope of these obligations includes those online

<sup>6</sup> Council Conclusions on Shaping Europe's Digital Future, 8711/20 of 9 June 2020, <https://www.consilium.europa.eu/media/44389/st08711-en20.pdf>

<sup>7</sup> <https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf>

platforms with a significant reach in the Union, currently estimated to be amounting to more than 45 million recipients of the service. This threshold is proportionate to the risks brought by the reach of the platforms in the Union; where the Union's population changes by a certain percentage, the Commission will adjust the number of recipients considered for the threshold, so that it consistently corresponds to 10 % of the Union's population. Additionally, the Digital Services Act will set out a co-regulatory backstop, including building on existing voluntary initiatives.

The proposal maintains the liability rules for providers of intermediary services set out in the e-Commerce Directive – by now established as a foundation of the digital economy and instrumental to the protection of fundamental rights online. Those rules have been interpreted by the Court of Justice of the European Union, thus providing valuable clarifications and guidance. Nevertheless, to ensure an effective harmonisation across the Union and avoid legal fragmentation, it is necessary to include those rules in a Regulation. It is also appropriate to clarify some aspects of those rules to eliminate existing disincentives towards voluntary own-investigations undertaken by providers of intermediary services to ensure their users' safety and to clarify their role from the perspective of consumers in certain circumstances. Those clarifications should help smaller, innovative providers scale up and grow by benefitting from greater legal certainty.

A deeper, borderless single market for digital services requires enhanced cooperation among Member States to guarantee effective oversight and enforcement of the new rules set out in the proposed Regulation. The proposal sets clear responsibilities for the Member State supervising the compliance of service providers established in its territory with the obligations set by the proposed Regulation. This ensures the swiftest and most effective enforcement of rules and protects all EU citizens. It aims at providing the simple and clear processes for both citizens and service providers to find relief in their interactions with supervising authorities. Where systemic risks emerge across the Union, the proposed Regulation provides for supervision and enforcement at Union level.

- **Consistency with existing policy provisions in the policy area**

The current EU legal framework regulating digital services is underpinned, first and foremost, by the e-Commerce Directive. This proposed Regulation is without prejudice to the e-Commerce Directive, and builds on the provisions laid down therein, notably on the internal market principle set out in Article 3. The proposed Regulation provides for a cooperation and coordination mechanism for the supervision of the obligations it imposes. With regard to the horizontal framework of the liability exemption for providers of intermediary services, this Regulation deletes Articles 12-15 in the e-Commerce Directive and reproduces them in the Regulation, maintaining the liability exemptions of such providers, as interpreted by the Court of Justice of the European Union.

- **Consistency with other Union policies**

The proposed Regulation introduces a horizontal framework for all categories of content, products, services and activities on intermediary services. The illegal nature of such content, products or services is not defined in this Regulation but results from Union law or from national law in accordance with Union law.

Sector-specific instruments do not cover all the regulatory gaps evidenced in the impact assessment report: they do not provide fully-fledged rules on the procedural obligations related to illegal content and they only include basic rules on transparency and accountability

of service providers and limited oversight mechanisms. In addition, sector-specific laws cover situations where adapted approaches are necessary. In terms of scope, they are limited from two perspectives. First, the sector-specific interventions address a small subset of issues (e.g. copyright infringements, terrorist content, child sexual abuse material or illegal hate speech, some illegal products). Second, they only cover the dissemination of such content on certain types of services (e.g. sub-set of online platforms for copyright infringements, only video-sharing platforms and only as regards audiovisual terrorist content or hate speech). However, it is important that the relationship between the new proposed Regulation and the sector-specific instruments is clarified.

The proposed Regulation complements existing sector-specific legislation and does not affect the application of existing EU laws regulating certain aspects of the provision of information society services, which apply as *lex specialis*. By way of example, the obligations set out in Directive 2010/13/EC, as amended by Directive (EU) 2018/1808, on video-sharing platform providers (“AVSMD”) as regards audiovisual content and audiovisual commercial communications will continue to apply. However, this Regulation applies to those providers to the extent that the AVSMD or other Union legal acts, such as the proposal for a Regulation on addressing the dissemination on terrorist content online, do not contain more specific provisions applicable to them.

The framework established in the Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services to ensure that business users of such services and corporate website users in relation to online search engines are granted appropriate transparency, fairness and effective redress possibilities, will apply as *lex specialis*.

Furthermore, the rules set out in the present proposal will be complementary to the consumer protection acquis and specifically with regard to Directive (EU) 2019/2161 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU which establish specific rules to increase transparency as to certain features offered by certain information society services.

This proposal is without prejudice to the Regulation (EU) 2016/679 (the General Data Protection Regulation) and other Union rules on protection of personal data and privacy of communications. For example, the measures concerning advertising on online platforms complement but do not amend existing rules on consent and the right to object to processing of personal data. They impose transparency obligations towards users of online platforms, and this information will also enable them to make use of their rights as data subjects. They also enable scrutiny by authorities and vetted researchers on how advertisements are displayed and how they are targeted.

The proposal is also fully consistent and further supports equality strategies adopted by the Commission in the context of the Union of Equality. The proposal is without prejudice to the Commission’s initiative aimed at improving the labour conditions of people working through digital platforms.

Finally, the proposed regulation builds on the Recommendation on illegal content of 2018.<sup>8</sup> It takes account of experiences gained with self-regulatory efforts supported by the

---

<sup>8</sup> Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online (C(2018) 1177 final)

Commission, such as the Product Safety Pledge<sup>9</sup>, the Memorandum of Understanding against counterfeit goods<sup>10</sup>, the Code of Conduct against illegal hate speech<sup>11</sup>, and the EU Internet Forum with regard to terrorist content.

## **2 LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY**

### **• Legal basis**

The legal basis for the proposal is Article 114 of the Treaty on the Functioning of the European Union, which provides for the establishment of measures to ensure the functioning of the Internal Market.

The primary objective of this proposal is to ensure the proper functioning of the internal market, in particular in relation to the provision of cross-border digital services (more specifically, intermediary services). In line with this objective, the proposal aims to ensure harmonised conditions for innovative cross-border services to develop in the Union, by addressing and preventing the emergence of obstacles to such economic activity resulting from differences in the way national laws develop, taking into account that several Member States have legislated or intend to legislate on issues such as the removal of illegal content online, diligence, notice and action procedures and transparency. At the same time, the proposal provides for the appropriate supervision of digital services and cooperation between authorities at Union level, therefore supporting trust, innovation and growth in the internal market.

### **• Subsidiarity**

Taking into account that the Internet is by its nature cross-border, the legislative efforts at national level referred to above hamper the provision and reception of services throughout the Union and are ineffective in ensuring the safety and uniform protection of the rights of Union citizens and businesses online. Harmonising the conditions for innovative cross-border digital services to develop in the Union, while maintaining a safe online environment, can only be served at Union level.

Union level action provides predictability and legal certainty, and reduces compliance costs across the Union. At the same time, it fosters the equal protection of all Union citizens, by ensuring that action against illegal content online by providers of intermediary services is consistent, regardless of their place of establishment. A well coordinated supervisory system, reinforced at Union level, also ensures a coherent approach applicable to providers of intermediary services operating in all Member States.

To effectively protect users online, and to avoid that Union-based digital service providers are subject to a competitive disadvantage, it is necessary to also cover to relevant service providers established outside of the Union whose operate on the internal market.

### **• Proportionality**

The proposal seeks to foster responsible and diligent behaviour by providers of intermediary services to ensure a safe online environment, which allows Union citizens and other parties to

<sup>9</sup> [https://ec.europa.eu/info/business-economy-euro/product-safety-and-requirements/product-safety/product-safety-pledge\\_en](https://ec.europa.eu/info/business-economy-euro/product-safety-and-requirements/product-safety/product-safety-pledge_en)

<sup>10</sup> [https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet\\_en](https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en)

<sup>11</sup> [https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online\\_en](https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en)

freely exercise their fundamental rights, in particular the freedom of expression and information. Key features of the proposal limit the Regulation to what is strictly necessary to achieve those objectives.

In particular, the proposal sets asymmetric due diligence obligations on different types of digital service providers depending on the nature of their services and their size, to ensure their services are not misused for illegal activities and providers operate responsibly. This approach addresses certain identified problems only there where they materialise, while not overburdening providers unconcerned by those problems. Certain substantive obligations are limited only to very large online platforms, which due to their reach have acquired a central, systemic role in facilitating the public debate and economic transactions. Very small providers are exempt from the obligations altogether.

As regards digital service providers established outside of the Union offering services in the Union, the Regulation requires the appointment of a legal representative in the Union to ensure effective oversight and, where necessary, enforcement.

Proportionate to the obligations, and taking into account the cross-border nature of digital services, the proposal will introduce a cooperation mechanism across Member States with enhanced Union level oversight of very large online platforms. Additionally, the proposal does not amend sector-specific legislation or the enforcement and governance mechanisms set thereunder, but provides for a horizontal framework to rely on, for aspects beyond specific content or subcategories of services regulated in sector-specific acts.

By establishing a clear framework, accompanied by cooperation between and with Member States, as well as by self-regulation, this proposal aims to enhance legal certainty and increase trust levels, while staying relevant and effective in the long term because of the flexibility of the cooperation framework.

- **Choice of the instrument**

Article 114 of the Treaty on the Functioning of the European Union gives the legislator the possibility to adopt regulations and directives.

The Commission has decided to put forward a proposal for a Regulation to ensure a consistent level of protection throughout the Union and to prevent divergences hampering the free provision of the relevant services within the internal market, as well as guarantee the uniform protection of rights and uniform obligations for business and consumers across the internal market. This is necessary to provide legal certainty and transparency for economic operators and consumers alike. The proposed Regulation also ensures consistent monitoring of the rights and obligations, and equivalent sanctions in all Member States, as well as effective cooperation between the supervisory authorities of different Member States and at Union level.

### **3 RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACTASSESSMENTS**

- **Ex-post evaluations/fitness checks of existing legislation**

This proposal builds on the evaluation of the e-Commerce Directive, conducted as a ‘back to back’ evaluation with the Impact Assessment accompanying the proposal. The specific objectives of the e-Commerce Directive were to ensure (i) a well-functioning internal market for digital services, (ii) the effective removal of illegal content online in full respect of fundamental rights, and (iii) an adequate level of information and transparency for consumers.

As regards the **effectiveness** of the e-Commerce Directive, the evaluation shows that while the e-Commerce Directive has provided an important incentive for the growth of the internal market for digital services, and enabled entry and scaling up of new providers of such services, the initial objectives have not been fully achieved.

In particular, the dynamic growth of the digital economy and the appearance of new types of service providers raises certain new challenges, dealt with differently by Member States, where the initial set of objectives need to be clarified. In addition, these developments put an additional strain on achieving already existing objectives as the increased legal fragmentation shows.

The evaluation also showed that while several new regulatory instruments make valuable contributions to the attainment of some of the policy objectives set out in the e-Commerce Directive, they provide only sector-specific solutions for some of the underlying problems (e.g. in addressing the proliferation of specific types of illegal activity). They therefore do not address such issues consistently for the entire digital ecosystem, as they are limited to certain types of services or certain types of illegal content. Furthermore, while self-regulatory initiatives have generally shown positive results, they cannot be legally enforced, nor do they cover all participants in the digital economy. As regards the **efficiency** of the e-Commerce Directive, the Directive imposed only limited additional costs for Member States' administrations and providers of information society services. The evaluation has not revealed particularly high or disproportionate costs and no substantial concerns have been raised regarding impacts on small and medium-sized enterprises. The main concern in this regard is related to the lack of clarity in the cooperation mechanism across Member States, creating burdens and duplication of costs, despite the opposite objective of the Directive, in particular where the supervision of online platforms is concerned. This has essentially reduced its efficiency in maintaining the functioning of the internal market.

In relation to questions about the continued **relevance** of the objectives pursued by the e-Commerce Directive, the evaluation shows that the objectives of the e-Commerce Directive continue to remain valid, while at the same time there are several new developments that are not well reflected in the existing public policy objectives.

First, the open public consultation, targeted submissions by stakeholders, reports issued by the European Parliament<sup>12</sup> as well as Council conclusions<sup>13</sup> confirm that the existing principles and objectives of the e-Commerce Directive remain valid today. However, new information asymmetries and risks have arisen since the entry into force of the Directive, notably related to the emergence of online platforms, in particular very large ones, and the scale of the digital transformation. This is for example the case in the areas of algorithmic decision making (with an impact on how information flows are intermediated online), or in online advertising systems.

The evaluation showed that the e-Commerce Directive is **coherent** with other EU interventions that took place since its adoption. The evaluation also did not identify any internal in-coherence of the e-Commerce Directive.

Finally, at least parts of the actual benefits of the e-Commerce Directive that the evaluation identified could be considered as **EU added value**. It is likely that Member States would have

---

<sup>12</sup>European Parliament, *ibidem*

<sup>13</sup>Shaping Europe's digital future, available at: <https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/en/pdf>.



continued applying their own regulatory systems without any common set of principles and that some Member States would have continued to have no horizontal rules in place at all. In the absence of robust evidence, it is however not possible to draw firm conclusions on the extent of this EU added value.

- **Stakeholder consultations**

Over the past five years, the Commission has consulted a wide range of different stakeholders, including providers of digital services such as online platforms and other intermediary services, businesses trading online, media publishers, brand owners and other businesses, users of digital services, civil society organisations, national authorities, academia, the technical community, international organisations and the general public. An array of targeted consultation steps have captured thoroughly stakeholder views on issues related to digital services and platforms over the last years.

The open public consultation on the Digital Services Act was open for 14 weeks, between 2<sup>nd</sup> of June and 8<sup>th</sup> of September and received 2,863 responses and around 300 position papers from a diverse group of stakeholders. Most feedback was submitted by the general public (66% from Union citizens, 8% from non-EU citizens), companies/ businesses organizations (7.4%), business associations (6%), and NGOs (5.6%). This was followed by public authorities (2.2%), academic/research institutions (1.2%), trade unions (0.9%), and consumer and environmental organisations (0.4%).

Overall, there is a general agreement amongst stakeholders for a need for action, both in addressing online safety and in furthering the internal market for digital services.

Stakeholders converge on the continued relevance of the main principles of the e-Commerce Directive and agree that they should be maintained, including the internal market principle for the supervision of digital services, the liability regime, and the prohibition of general monitoring obligations.

Stakeholders also broadly agree on the need to upgrade the framework in light of today's challenges by establishing clear obligations for service providers, harmonised across the EU. A majority of respondents, all categories included, indicated that they have encountered both harmful and illegal content, goods or services online, and specifically noted an alarming spike during the Covid-19 pandemic. A large share of respondents who say they have notified illegal content or goods to digital service providers expressed their dissatisfaction with the response and the ineffectiveness of reporting mechanisms after the exposure took place. Moreover, users perceive there to be a mismatch between providers' policies as stated and their concrete actions.

There is broad consensus, including among service providers responding to the consultation, on the need for simple, standardised, transparent notice and action obligations, harmonised across the internal market. This is considered as essential to enable rapid responses to illegal content and enhance legal clarity for users of platforms and for small platforms seeking to scale in the internal market. Respondents also agree on the importance of a redress mechanisms.

Concerning online marketplaces, several stakeholders flagged the need for more targeted measures such as the identification of sellers.

Respondents also generally agree that the territorial scope for these obligations should include all players offering goods, information or services in the Union, regardless of their place of establishment. A large share of respondents also emphasized the importance of these issues in particular where large platforms are concerned.

There is a general agreement among stakeholders that ‘harmful’ (yet not, or at least not necessarily, illegal) content should not be defined in the Digital Services Act and should not be subject to removal obligations, as this is a delicate area with severe implications for the protection of freedom of expression.

However, the way algorithmic systems shape information flows online is an area of concern among a wide category of stakeholders. Several stakeholders, in particular civil society and academics, pointed out the need for algorithmic accountability and transparency audits, especially with regard to how information is prioritized and targeted. Similarly, regarding online advertising, stakeholder views echoed the broad concerns around the lack of user empowerment and lack of meaningful oversight and enforcement.

When it comes to enforcement, there is a general understanding among stakeholders that cooperation between authorities should be improved both cross-border and within each Member State. EU oversight is considered crucial and the majority of respondents seems to favour a unified oversight entity.

- **Collection and use of expertise**

The preparatory steps for the proposal rest on an array of studies and expert advice, including a number of legal studies commissioned focusing on the implementation of the E-Commerce Directive and the state of legal fragmentation<sup>14</sup>, studies on algorithmic transparency and accountability<sup>15</sup>, as well as internal studies on costs of content moderation, liability regimes for intermediaries, and cost of non-Europe, with the support of the Joint Research Centre of the European Commission. For gathering the views and perceptions of the general public, the Commission ran a Eurobarometer survey in 2018 with a representative sample of over 33,000 respondents from all Member States<sup>16</sup>.

The legal analysis also rests on a rich collection of case law, in particular by the Court of Justice of the European Union, of several provisions of the e-Commerce Directive and related acts, such as provisions concerning the interpretation of the notion of “information society services”<sup>17</sup> or provisions concerning the liability of intermediary services providers<sup>18</sup>. The Commission also gathered expertise and views through targeted consultations and engagement activities, including a series of workshops, conferences, interviews with experts and judges, consultations of the Expert Group on e-commerce, as well as numerous bilateral meetings and analysis of ad hoc position and research papers from organizations, industry representatives, civil society and academia.

<sup>14</sup>Van Hoboken J. et al (2018), *Hosting Intermediary Services and Illegal Content Online*, and Schwemer, S., Mahler, T. & Styri, H. (2020). *Legal analysis of the intermediary service providers of non-hosting nature*, ICF, Grimaldi, *The Liability Regime and Notice-and-Action Procedures*, SMART 2016/0039

<sup>15</sup>Optimity Advisors, SMART 2017/ 0055 *Algorithmic Awareness building – State of the art report* and LNE, *Governance and Accountability Mechanisms for Algorithmic Systems* (forthcoming). SMART 2018/37

<sup>16</sup>Eurobarometer TNS. (2018, July). *Flash Eurobarometer 469: Illegal content online*

<sup>17</sup>For example, Case C-108/09, *Ker-Optika*, ECLI:EU:C:2010:725, Case C-291/13, *Papasavvas*, ECLI:EU:C:2014:2209, Case C-484/14, *Tobias McFadden v. Sony Music*, ECLI:EU:C:2016:689; Case C-434/15 *Asociación Profesional Élite Taxi*, ECLI:EU:C:2017:981 or Case C-390/18 *Airbnb Ireland UC*, ECLI:EU:C:2019:1112.

<sup>18</sup>Cases C-236/08 to C-238/08, *Google France and Google v. Vuitton*, ECLI:EU:C:2010:159; Case C-324/09, *eBay*, ECLI:EU:C:2011:474; Case C-70/10, *Scarlet*, ECLI:EU:C:2011:771; Case C-360/10, *Netlog*, ECLI:EU:C:2012:85; Case C-314/12, *UPC Telekabel Wien*, EU:C:2014:192; Case C-484/14, *Tobias McFadden v. Sony Music*, ECLI:EU:C:2016:689 or Case C-18/18, *Glawischnig*. ECLI:EU:C:2019:821.

Finally, the analysis rests on additional literature review, studies and research papers submitted by academics in the open public consultation and other independent studies, including the collection of studies carried out for the European Parliament<sup>19</sup>.

- **Impact assessment**

The Regulatory Scrutiny Board issued a positive opinion with reservations on the impact assessment, including suggestions for improvement<sup>20</sup>. The Impact Assessment report was further revised along these lines, notably in clarifying the interlinks between the Digital Services Act and the broader regulatory framework, providing more detailed descriptions of the policy options, and a more detailed analysis of the underlying evidence addressed in the revised impact assessment report.

The importance in our economy and society, but also the growing risks brought by digital services will continue to scale. In the baseline scenario, the Commission will continue to enforce existing rules, including on sector-specific issues, and will support the self-regulatory efforts in place. However, faced with the evolving problems, Member States will continue to legislate independently. The legal fragmentation with the resulting patchwork of national measures will not just fail to effectively tackle illegal activities and protect citizens' fundamental rights throughout the EU, it will also hinder new, innovative services from scaling up in the internal market, cementing the position of the few players which can afford the additional compliance costs. This leaves the rule setting and enforcement mostly to very large private companies, with ever-growing information asymmetry between online services, their users and public authorities.

Three main policy options were assessed, in addition to the baseline. Option 1 would codify the Recommendation of 2018: it would lay down a range of procedural obligations for online platforms to tackle illegal activities conducted by their users. The obligations would also include the necessary safeguards in order to protect users' fundamental rights and ensure transparency. It would also enhance the administrative cooperation mechanisms for authorities to resolve cross-border issues through a digital clearing house, facilitating information flows. Option 2 would in addition to measures in option 1, remove disincentives for service providers to take voluntary measures against illegal content, and introduce measures to enhance transparency around recommender systems and advertising. The enforcement and cooperation mechanism would be enhanced with the appointment of a central coordinator in each Member State. Option 3, building on the measures outlined in the previous options, includes targeted, asymmetric measures with stronger obligations for very large online platforms which are prone to the highest levels of risks for the EU society and economy, as well as certain limited clarifications of the liability regime for providers of intermediary services and an EU governance system with reinforced oversight and enforcement powers.

The assessment of the economic and social impacts identified, and the comparison of its effectiveness, efficiency, coherence and proportionality showed that Option 3 would most effectively meet the objectives of the intervention by establishing the proportionate

---

<sup>19</sup>Digital Services Act: Improving the functioning of the Single Market, available at: [https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272_EN.html). Digital Services Act: adapting commercial and civil law rules for commercial entities operating online, available at: [https://www.europarl.europa.eu/doceo/document/TA-9-2020-0273\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-9-2020-0273_EN.html). Digital Services Act and fundamental rights issues posed, available at: [https://www.europarl.europa.eu/doceo/document/TA-9-2020-0274\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-9-2020-0274_EN.html).

<sup>20</sup>Links to the summary sheet and the positive opinion of the RSB will be included after their publication.

framework fit for adapting to emerging challenges in the dynamic digital world. The components included in Option 3 are also broadly supported by stakeholders, including positions from the European Parliament and Member States.

The preferred option would support the access to the internal market for European Union intermediary service providers and their ability to scale-up by reducing costs related to the legal fragmentation. While costs for compliance with due diligence obligations are expected, it is estimated this is offset by reducing the current fragmentation through harmonisation. It is expected to have a positive impact on competitiveness, innovation and investment in digital services, in particular European Union start-ups and scale-ups offering platform business models but also, to varying extents, on sectors underpinned and amplified by digital commerce.

The preferred option intends to define the appropriate division of responsibilities between intermediary services, their recipients and authorities when fighting against illegal content online. To do so, it introduces an asymmetric approach to the due diligence obligations imposed on very large online platforms: this is a supervised risk management approach, with an important role of the governance system for enforcement. The asymmetric obligations are only imposed on very large online platforms, which have, based on the current data, not only the broadest reach, but are also the large companies with important turnover. Consequently, while the targeted measures are more restrictive than for other companies, they are proportionate to the ability of the companies to comply.

For public authorities, the proposed option would cut the costs brought by the inefficiencies and duplications in the existing set-up for the cooperation of authorities. While Member States would bear the costs of appointing a competent authority, new or already established, the efficiency gains are expected to outweigh them: for the individual authorities through mutualisation of resources, better information flows, and straight-forward processes for interacting with their counterparts across the internal market, as well as with service providers.

- **Regulatory fitness and simplification**

The Impact Assessment accompanying this proposal identifies the sole added value of Union intervention addressing the risk of legal fragmentation triggered by divergent regulatory and supervisory approaches (hence without accounting for the increased safety and trust on digital services) in a possible increase of cross-border digital trade of 1 to 1.8%, i.e. the equivalent of an increase in turnover generated cross-border of EUR 8.6 billion and up to EUR 15.5 billion.

With regard to added value in the enforcement of measures, the initiative creates important efficiency gains in the cooperation across Member States and mutualising some resources for technical assistance at EU level, for inspecting and auditing content moderation systems, recommender systems and online advertising on very large online platforms. This, in turn, leads to an increased effectiveness of enforcement and supervision measures, whereas the current system relies to a large extent on the limited capability for supervision in a small number of Member States.

- **Fundamental rights**

Union citizens and others are exposed to ever-increasing risks and harms online – from the spread of illegal content and activities, to limitations to express themselves and other societal harms. The envisaged policy measures in this legislative proposal will substantially improve this situation by providing a modern, future-proof governance framework, effectively safeguarding the rights and legitimate interests of all parties involved, most of all Union citizens. The proposal introduces important safeguards to allow citizens to freely express

themselves, while enhancing user agency in the online environment, as well as the exercise of other fundamental rights such as the right to an effective remedy, non-discrimination, rights of the child as well as the protection of personal data and privacy online.

The proposed Regulation will mitigate risks of erroneous or unjustified blocking speech, address the chilling effects on speech, stimulate the freedom to receive information and hold opinions, as well as reinforce users' redress possibilities. Vulnerable or disadvantaged groups or persons can be disproportionately affected by restrictions and removal measures following from (unconscious or conscious) biases potentially embedded in the notification systems by users and third parties, as well as replicated in automated content moderation tools used by platforms. The proposal will mitigate discriminatory risks, particularly for those groups or persons, including women and minority groups, and will contribute to the protection of the rights of the child and the right to human dignity online. The proposal will only require removal of illegal content and will impose mandatory safeguards when users' information is removed, including the provision of explanatory information to the user, complaint mechanisms supported by the service providers as well as external out-of-court dispute resolution mechanism. Furthermore, it will ensure EU citizens are also protected when using services provided by providers not established in the Union but active on the internal market, since those providers are covered too.

With regard to service providers' freedom to conduct a business, the costs incurred on businesses are offset by reducing fragmentation across the internal market. The proposal introduces safeguards to alleviate the burden on service providers, including measures against repeated unjustified notices and prior vetting of trusted flaggers by public authorities. Furthermore, certain obligations are targeted to very large online platforms, where the most serious risks often occur and which have the capacity absorb the additional burden.

The proposed legislation will preserve the prohibition of general monitoring obligations of the e-Commerce Directive, which in itself is crucial to the required fair balance of fundamental rights in the online world. The new Regulation prohibits general monitoring obligations, as they could disproportionately limit users' freedom of expression and freedom to receive information, and could burden service providers excessively and thus unduly interfere with their freedom to conduct a business. The prohibition also limits incentives for online surveillance and has positive implications for the protection of personal data and privacy.

All measures in the proposal are fully compliant and aligned with the high standard of personal data protection and protection of privacy of communications and private life, set in EU legislation.

#### **4 BUDGETARY IMPLICATIONS**

The budgetary impact of the proposal will be covered by the allocations foreseen in the MFF 2021-27 under the financial envelopes of the Digital Europe Programme and Single Market Programme as detailed in the legislative financial statement accompanying this proposal for a regulation. These implications require also reprogramming of Heading 7 of the Financial Perspective.

The legislative financial statement accompanying this proposal for a Regulation covers the budgetary impacts for the Regulation itself.

## 5 OTHER ELEMENTS

### • **Implementation plans and monitoring, evaluation and reporting arrangements**

The Commission will establish a comprehensive framework for continuously monitoring the output, results and impact of this legislative instrument upon the date of its application. Based on the established monitoring programme, an evaluation of the instrument is envisaged within five years from its entry into force.

### • **Detailed explanation of the specific provisions of the proposal**

Chapter I sets out general provisions, including the subject matter and scope of the Regulation (Article 1) and the definitions of key terms used in the Regulation (Article 2).

Chapter II contains provisions on the exemption of liability of providers of intermediary services. More specifically, it includes the conditions under which providers of mere conduit (Article 3), caching (Article 4) and hosting services (Article 5) are exempt from liability for the third-party information they transmit and store. It also provides that the liability exemptions should not be disapplied when providers of intermediary services carry out voluntary own-initiative investigations or comply with the law (Article 6) and it lays down a prohibition of general monitoring or active fact-finding obligations for those providers (Article 7). Finally, it imposes an obligation on providers of intermediary services in respect of orders from national judicial or administrative authorities to act against illegal content (Article 8) and to provide information (Article 9).

Chapter III sets out the due diligence obligations for a transparent and safe online environment, in five different sections.

**Section 1** lays down obligations applicable to all providers of intermediary services, in particular: the obligation to establish a single point of contact to facilitate direct communication with Member States' authorities, the Commission and the Board (Article 10); the obligation to designate a legal representative in the Union for providers not established in any Member State, but offering their services in the Union (Article 11); the obligation to set out in their terms and conditions any restrictions that they may impose on the use of their services and to act responsibly in applying and enforcing those restrictions (Article 12); and transparency reporting obligations in relation to the removal and the disabling of information considered to be illegal content or contrary to the providers' terms and conditions (Article 13).

**Section 2** lays down obligations, additional to those under Section 1, applicable to providers of hosting services. In particular, that section obliges those providers to put in place mechanisms to allow third parties to notify the presence of alleged illegal content (Article 14). Furthermore, if such a provider decides to remove or disable access to specific information provided by a recipient of the service, it imposes the obligation to provide that recipient with a statement of reasons (Article 15).

**Section 3** lays down obligations applicable to all online platforms, additional to those under Sections 1 and 2. The Section specifies that it does not apply to online platforms that are micro or small enterprises within the meaning of the Annex to Recommendation 2003/361/EC (Article 16). The Section lays down the obligation for online platforms to provide an internal complaint-handling system in respect of decisions taken in relation to alleged illegal content or information incompatible with their terms and conditions (Article 17). It also obliges online platforms to engage with certified out-of-court dispute settlement bodies to resolve any dispute with users of their services (Article 18). It further obliges online platforms to ensure

that notices submitted by entities granted the status of trusted flaggers are treated with priority (Article 19) and sets out the measures online platforms are to adopt against misuse (Article 20). Furthermore, this Section includes a requirement for online platforms to inform competent enforcement authorities in the event they become aware of any information giving rise to a suspicion of serious criminal offences involving a threat to the life or safety of persons (Article 21). The Section also obliges online platforms to receive, store, make reasonable efforts to assess the reliability of and publish specific information on the traders using their services where those online platforms allow consumers to conclude distance contracts with those traders (Article 22). Those online platforms are also obliged to organise their interface in a way that enables traders to respect Union consumer and product safety law (Article 22a). Online platforms are also obliged to publish reports on their activities relating to the removal and the disabling of information considered to be illegal content or contrary to their terms and conditions (Article 23). The Section also includes transparency obligations for online platforms in respect of online advertising (Article 24).

**Section 4** lays down obligations, additional to the obligations laid down in Sections 1 to 3, for very large online platforms (as defined by Article 25) to manage systemic risks. Very large online platforms are obliged to conduct risk assessments on the systemic risks brought about by or relating to the functioning and use of their services (Article 26) and to take reasonable and effective measures aimed at mitigating those risks (Article 27). They are also to submit themselves to external and independent audits (Article 28). The Section includes also a specific obligation in case very large online platforms use recommender systems (Article 29) or display online advertising on their online interface (Article 30). Furthermore, the Section sets out the conditions under which very large online platforms provide access to data to the Digital Services Coordinator of establishment or the Commission and vetted researchers (Article 31), the obligation to appoint one or more compliance officers to ensure compliance with the obligations laid down in the Regulation (Article 32) and specific, additional transparency reporting obligations (Article 33).

**Section 5** contains transversal provisions concerning due diligence obligations, namely the processes for which the Commission will support and promote the development and implementation of harmonised European standards (Article 34); the framework for the development of codes of conduct (Article 35); and the framework for the development of specific codes of conduct for online advertising (Article 36). There is also a provision on crisis protocols to address extraordinary circumstances affecting public security or public health (Article 37).

**Chapter IV** contains the provisions concerning the implementation and enforcement of this Regulation.

**Section 1** lays down provisions concerning national competent authorities, including Digital Services Coordinators, which are the primary national authorities designated by the Member States for the consistent application of this Regulation (Article 38). The Digital Services Coordinators, like other designated competent authorities, are independent and perform their tasks impartially, transparently and in a timely manner (Article 39). Member States where the main establishment of the provider is located have jurisdiction to enforce this Regulation (Article 40). The Digital Services Coordinators are granted specific powers (Article 41). Member States are to lay down rules on penalties applicable to breaches of the obligations by providers of intermediary services under this Regulation (Article 42). Digital Services Coordinators can receive complaints against providers of intermediary services for breaches of the obligations laid down in this Regulation (Article 43). Digital Services Coordinators are

required to publish annual reports on their activities (Article 44) and to cooperate with Digital Services Coordinators of other Member States (Article 45). Digital Services Coordinators can also participate in joint investigations with regard to matters covered by the Regulation (Article 46).

**Section 2** lays down provisions regarding the European Board for Digital Services, an independent advisory group of Digital Services Coordinators (Article 47). It also sets out the structure of that Board (Article 48) and its tasks (Article 49).

**Section 3** concerns the supervision, investigation, enforcement and monitoring of very large online platforms. It provides for enhanced supervision in the event such platforms infringe the provisions of Chapter III, Section 4 (Article 50). It also provides the possibility for the Commission to intervene vis à vis very large online platforms in case the infringements persist (Article 51). In these cases the Commission can carry out investigations, including through requests for information (Article 52), interviews (Article 53) and on-site inspections (Article 54), can adopt interim measures (Article 55) and make binding commitments by very large online platforms (Article 56), as well as monitor their compliance with the Regulation (Article 57). In case of non-compliance, the Commission can adopt non-compliance decisions (Article 58), as well as fines (Article 59) and periodic penalty payments (Article 60) for breaches of the Regulation by very large online platforms as well as for supply of incorrect, incomplete or misleading information in the context of the investigation. The Regulation sets also a limitation period for the imposition of penalties (Article 61) and for their enforcement (Article 62). Finally, the Regulation sets the procedural guarantees in front of the Commission, in particular the right to be heard and of access to the file (Article 63) and the publication of decisions (Article 64). The Section also provides for the cooperation of the Commission with national courts (Article 65) and for the adoption of implementing acts on practical arrangement on the proceedings (Article 66).

**Section 4** includes the common provisions on enforcement. It first lays down rules on an information-sharing system supporting communications between Digital Services Coordinators, the Commission and the Board (Article 67). It also includes the right of recipients of intermediary services to mandate a body, organisation and association to exercise their rights on their behalf (article 68).

**Section 5** relates to the adoption of delegated and implementing acts in accordance with Articles 290 and 291 of the Treaty on the Functioning of the European Union, respectively (Articles 69 and 70).

Finally, **Chapter V** contains the final provisions of this Regulation, which concern the deletion of Articles 12 to 15 of the e-Commerce Directive given that they have been incorporated in the Regulation (Article 71), amendments to Directive 2020/XX/EC (Article 72), evaluation of the Regulation (Article 73), and its entry into force and application (Article 74).



Proposal for a

**REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC**

(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>21</sup>,

Having regard to the opinion of the Committee of the Regions<sup>22</sup>,

Having regard to the opinion of the European Data Protection Supervisor<sup>23</sup>,

Acting in accordance with the ordinary legislative procedure,

Whereas:

- (1) Information society services and especially intermediary services have become an important part of the Union's economy and 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>24</sup>, new and innovative business models and services, such as online social networks and marketplaces, 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, both for individual users and for 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. Those diverging national laws negatively affect the internal market, which, pursuant to Article 26 of the Treaty, 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

---

<sup>21</sup>OJ C , , p. .

<sup>22</sup>OJ C , , p. .

<sup>23</sup>OJ C, p.

<sup>24</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).

cross-border nature of the internet, which is generally used to provide those services. The conditions for the provision of intermediary services 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.

- (3) Responsible and diligent behaviour by providers of intermediary services is essential for a safe, predictable and trusted 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 ('Charter'), in particular the freedom of expression and information and the freedom to conduct a business, and the right to non-discrimination.
- (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 in order 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>25</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 specified 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 residence, in so far as they provide services in the Union, as evidenced by a substantial connection to the Union.

---

<sup>25</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).

Obtenu par CONTEXTE

Regulation [...] on temporary derogation from certain provisions of Directive 2002/58/EC<sup>32</sup> as well as Union law on consumer protection, in particular Directive 2005/29/EC of the European Parliament and of the Council<sup>33</sup>, Directive 2011/83/EU and Directive 93/13/EEC, as amended by Directive (EU) 2019/2161 of the European Parliament and of the Council<sup>34</sup>, and on the protection of personal data, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council.<sup>35</sup> The protection of individuals with regard to the processing of personal data is solely governed by the rules of Union law on that subject, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC.

- (11) It should be clarified that this Regulation is without prejudice to the rules of Union law on copyright and related rights, which establish specific rules and procedures that should remain unaffected.
- (12) In order to achieve the objective of ensuring a safe, predictable and trusted online environment, for the purpose of this Regulation the concept of “illegal content” should be defined broadly and also covers 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 relates to activities that are illegal, such as the sharing of images depicting child sexual abuse, unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit products, the non-authorised use of copyright protected material or activities involving infringements of consumer protection 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 consistent 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 marketplaces, 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, again at their request. 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 of another service and that feature cannot, for objective technical reasons, be used without that

<sup>32</sup>Regulation [...] on temporary derogation from certain provisions of Directive 2002/58/EC.

<sup>33</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’)

<sup>34</sup>Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules

<sup>35</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).

other, principal service, and the integration of that feature 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.

- (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, that is, making the information easily accessible to users 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. The mere possibility to create groups of users of a given service should not, in itself, be understood to mean that the information disseminated in that manner is not disseminated to the public. However, the concept should exclude dissemination of information within closed groups consisting of a finite number of pre-determined persons. Interpersonal communication services, as defined in Directive (EU) 2018/1972 of the European Parliament and of the Council,<sup>36</sup> such as emails or private messaging services, fall outside the scope of this Regulation. Information should be considered disseminated to the public within the meaning of this Regulation only where that occurs upon the direct request by the recipient of the service that provided the information.
- (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 case law of the Court of Justice of the European Union.
- (17) The relevant rules of Chapter II 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

---

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

not be available in respect of liability relating to information provided not by the recipient of the service but by the provider of 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) A provider of intermediary services that deliberately collaborates with a recipient of the services in order to undertake illegal activities does not provide its service neutrally and should therefore not be able to benefit from the exemptions from liability provided for in this Regulation.
- (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. This requires, among other things, that the provider does not modify the information that it transmits. However, this requirement should not be understood to cover manipulations of a technical nature which take place in the course of the transmission, as such manipulations do not alter the integrity of the information transmitted.
- (22) In order to benefit from the exemption from liability for hosting services, the provider should, upon obtaining actual knowledge or awareness of 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 principle of freedom of expression. The provider can obtain such actual knowledge or awareness through, in particular, its own-initiative investigations or notices submitted to it by individuals or entities in accordance with this Regulation in so far as those 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.
- (23) 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 that it leads consumers to believe that the information was provided by those online platforms themselves or by recipients of the service 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. In that regard, it should be determined objectively, on the basis of all relevant circumstances, whether the presentation could lead to such a belief on the side of an average and reasonably well-informed consumer.
- (24) 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 requiring the termination or prevention of any infringement, including the removal of illegal content or the disabling of access to it.

- (25) In order to create legal certainty and not to discourage activities aimed at detecting, identifying and acting against illegal content that providers of intermediary services may undertake on a voluntary basis, it should be clarified that the mere fact that providers undertake such activities does not lead to the unavailability of the exemptions from liability set out in this Regulation, provided those activities are carried out in good faith and in a diligent manner. In addition, it is appropriate to clarify that the mere fact that those 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 lead to the unavailability of those exemptions from liability. Therefore, any such activities and measures that a given 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.
- (26) Whilst the rules in Chapter III of this Regulation concentrate on the liability of providers of intermediary services, it is important to recall that, despite the generally important role played by those 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 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 actor 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 for the availability and accessibility of information that is not illegal content.
- (27) Since 2000, new technologies have emerged that improve the availability, efficiency, speed, reliability, capacity and security of systems for the transmission 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 conduits’, ‘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, certificate authorities that issue digital certificates, or content delivery networks, that enable 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 e-mail 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 service.

- (28) Providers of intermediary services should not be 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 accordance with the conditions established in this Regulation. Nothing in this Regulation should be construed as an imposition of a general monitoring obligation or active fact-finding obligation, or as a general obligation for providers to take proactive measures to relation to illegal content.
- (29) Depending on the legal system of each Member State and the field of law at issue, national judicial or administrative authorities may order providers of intermediary services to act against certain specific items of illegal content or to provide certain specific items of 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, 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.
- (30) Orders to act against illegal content or to provide information should be issued in compliance with Union law, in particular 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) .../.... [proposed Regulation addressing the dissemination of terrorist content online], or Regulation (EU) 2017/2394 that confers specific powers to order the provision of information on 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 conformity with Union law and confidentiality requests by law enforcement authorities related to the non-disclosure of information.
- (31) 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 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 addition, where the order referring to the specific information may have effects beyond the territory of the Member State of the authority concerned, the authority should assess whether the information at issue is likely to constitute illegal content in



other Member States concerned and, where relevant, take account of the relevant rules of Union law or international law and the interests of international comity.

- (32) 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 services with applicable Union or national rules. Therefore, orders about 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, should remain unaffected by the rules of this Regulation on the provision of information.
- (33) Orders to act against illegal content and to provide information are subject to the rules safeguarding the competence of the Member State where the service provider addressed is established and 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 where the service provider is established on certain specified grounds and regarding the notification of such measures, do not apply in respect of those orders.
- (34) 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 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 minors, women and users with minority background, protect the relevant fundamental rights enshrined in the Charter, to ensure meaningful accountability of those providers and to empower recipients and other affected parties, whilst facilitating the necessary oversight by competent authorities.
- (35) In that regard, it is important that the due diligence obligations are adapted to the type 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, online platforms and very large online platforms. To the extent that providers of intermediary services may fall within those different categories in view of the nature of their services and their size, they should comply with all of the corresponding obligations of this Regulation. Those harmonised due diligence obligations, which should be reasonable and non-arbitrary, are needed to achieve the identified public policy concerns, such as safeguarding the legitimate interests of the recipients of the service, addressing illegal practices and protecting fundamental rights online.
- (36) In order to facilitate smooth and efficient communications relating to matters covered by this Regulation, providers of intermediary services should be required to establish a single point of contact and to publish relevant information relating to their point of contact, including the languages to be used in such communications. The 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 point of contact should serve operational purposes and should not necessarily have to have a physical location .

- (37) Providers of intermediary services that are established in a third country that offer services in the Union should designate a sufficiently mandated legal representative in the Union and provide information relating to their legal representatives, so as to allow for the effective oversight and, where necessary, enforcement of this Regulation in relation to those providers. It should be possible for the legal representative to also function as point of contact, provided the relevant requirements of this Regulation are complied with.
- (38) 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.
- (39) To ensure an adequate level of transparency and accountability, providers of intermediary services should annually report, in accordance with the harmonised requirements contained in this Regulation, on the content moderation they engage in, including the measures taken as a result of the application and enforcement of their terms and conditions. However, so as 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>37</sup>
- (40) 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 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'). 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. 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 as far as they qualify as providers of hosting services covered by this Regulation.
- (41) The rules on such notice and action mechanisms should be harmonised at Union level, so as to provide for the timely, diligent and objective 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. The fundamental rights include, as the case may be, the right to freedom of expression and 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 of the recipients of the service; the freedom to conduct a business, including the freedom

<sup>37</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).

of contract, of service providers; as well as 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 of parties affected by illegal content.

- (42) Where a hosting service provider decides to remove or disable information provided by a recipient of the service, for instance following receipt of a notice or acting on its own initiative, including through the use of automated means, that provider should inform the recipient of its decision, the reasons for its decision and the available redress possibilities 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. Available recourses to challenge the decision of the hosting service provider should always include judicial redress.
- (43) To avoid disproportionate burdens, the additional obligations imposed on online platforms under this Regulation should not apply to micro or small enterprises as defined in Recommendation 2003/361/EC of the Commission,<sup>38</sup> unless their reach and impact is such that they meet the criteria to qualify as very large online platforms under this Regulation. The consolidation rules laid down in that Recommendation help ensure that any circumvention of those additional obligations is prevented. The exemption of micro- and small enterprises from those additional obligations should not be understood as affecting their ability to set up, on a voluntary basis, a system that complies with one or more of those obligations.
- (44) Recipients of the service should be able to easily and effectively contest certain decisions of online platforms that negatively affect them. Therefore, online platforms should be required to provide for internal complaint-handling systems, which meet certain conditions aimed at ensuring that the systems are easily accessible and lead to swift and fair outcomes. In addition, provision should be made for the possibility of out-of-court dispute settlement of disputes, including those that could not be resolved in 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 possibilities to contest decisions of online platforms thus created should complement, yet leave unaffected in all respects, the possibility to seek judicial redress in accordance with the laws of the Member State concerned.
- (45) For contractual consumer-to-business disputes over the purchase of goods or services, Directive 2013/11/EU of the European Parliament and of the Council<sup>39</sup> 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.

<sup>38</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).

<sup>39</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).

- (46) Action against illegal content can be taken more quickly and reliably where online platforms take the necessary measures to ensure that notices submitted by trusted flaggers 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 objective manner. 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, that they represent collective interests and that they work in a diligent 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 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. For intellectual property rights, organisations of industry and of right-holders could be awarded trusted flagger status, where they have demonstrated that they meet the applicable conditions. The rules of this Regulation on trusted flaggers should not be understood to prevent 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>40</sup>
- (47) The misuse of services 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 and proportionate safeguards against such misuse. 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 respectively that the notices or complaints are unfounded. Under certain conditions, online platforms should temporarily suspend their relevant activities in respect of the person engaged in abusive behaviour. For reasons of transparency, this possibility should be set out, clearly and in sufficiently detail, in the terms and conditions of the online platforms. Redress should always be open to the decisions taken in this regard by online platforms and they should be subject to oversight by the competent Digital Services Coordinator. The rules of this Regulation on misuse should not prevent online platforms from taking other measures to address the provision of illegal content by recipients of their service or other misuse of their services, 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.
- (48) An online platform 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

---

<sup>40</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

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 online platform is aware, the suspicion that the recipient may have committed, may be committing or is likely to commit a serious criminal offence involving a threat to the life or safety of person, such as offences specified in Directive 2011/93/EU of the European Parliament and of the Council<sup>41</sup>. In such instances, the online platform should inform without delay the competent law enforcement authorities of such suspicion, providing all relevant information available to it, including where relevant the content in question and an explanation of its suspicion. 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 online platforms. Online platforms 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.

- (49) 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 online platform, 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 online platforms should store all information in a secure manner for a reasonable period of time that does not exceed what is necessary, so that it 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.
- (50) To ensure an efficient and adequate application of that obligation, without imposing any disproportionate burdens, the online platforms covered should make reasonable efforts to verify 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<sup>42</sup>, or by requesting the traders concerned to provide trustworthy supporting documents, such as copies of identity documents, certified bank 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 online platforms covered should not be required to engage in excessive or costly online fact-finding exercises or to carry out verifications on the spot. Nor should such online platforms, which have made the reasonable efforts required by this Regulation, be understood as guaranteeing the reliability of the information towards consumer or other interested parties.
- (51) In view of the particular responsibilities and obligations of online platforms, they should be made subject to transparency reporting obligations, which apply in addition

<sup>41</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>42</sup>[https://ec.europa.eu/taxation\\_customs/vies/vieshome.do?selectedLanguage=en](https://ec.europa.eu/taxation_customs/vies/vieshome.do?selectedLanguage=en)

to the transparency reporting obligations applicable to all providers of intermediary services under this Regulation. For the purposes of determining whether online platforms may be very large online platforms that are subject to certain additional obligations under this Regulation, the transparency reporting obligations for online platforms should include certain obligations relating to the publication and communication of information on the average monthly active recipients of the service in the Union.

- (52) Online advertisement plays an important role in the online environment, including in relation to the provision of the services of online platforms. However, online advertisement can contribute to significant risks, ranging from advertisement that is itself illegal content, to contributing to financial incentives for the publication or amplification of illegal or otherwise harmful content and activities online, or the discriminatory display of advertising 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, 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 displayed. In addition, recipients of the service should have information on the main parameters used for determining that specific advertising is to be displayed to them, providing meaningful explanations of the logic used to that end, including when this is based on profiling. The requirements of this Regulation on the provision of information relating to advertisement 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 (Regulation on Privacy and Electronic Communications) in particular those regarding the storage of information in terminal equipment and the access to information stored therein.
- (53) Given the importance of very large online platforms, due to their reach, in particular as expressed in number of recipients of the service, in facilitating public debate, economic transactions and the dissemination of information, opinions and ideas and in influencing how recipients obtain and communicate information online, it is necessary to impose specific obligations on those platforms, in addition to the obligations applicable to all online platforms. Those additional obligations on very large online platforms are necessary to address those public policy concerns, there being no alternative and less restrictive measures that would effectively achieve the same result.
- (54) Very large online platforms may cause societal risks, different in scope and impact from those caused by smaller platforms. Once the user base of a platform reaches a significant share of the Union population, the systemic risks the platform poses have a disproportionately negative impact in the Union. As an operational estimate of such significant reach, very large online platforms are considered platforms with a number of recipients exceeding 45 million users, a number equivalent to 10% of the Union population. The operational threshold should be maintained up to date through delegated acts. Such very large online platforms should therefore bear the highest standard of due diligence obligations, proportionate to their societal impact and means.
- (55) In view of the network effects characterising the platform economy, the user base of an online platform may quickly expand and reach the dimension of a very large online platform, 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 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 should be able to request more frequent reporting from the platform on the user base to be able to timely identify the moment at which that platform should be designated as a very large online platform for the purposes of this Regulation.

- (56) Very large online platforms are used in a way that strongly influences safety online, the shaping of public opinion and discourse, as well as on online trade. The way they design their services is generally optimised to benefit their often advertising-driven business models and can cause societal concerns. In the absence of effective regulation and enforcement, they can set the rules of the game, without effectively identifying and mitigating the risks and the societal and economic harm they can cause. Under this Regulation, very large online platforms should therefore assess the systemic risks stemming from the functioning and use of their service, as well as by potential misuses by the recipients of the service, and take appropriate mitigating measures.
- (57) Three categories of systemic risks should be assessed in-depth. A first category concerns the risks associated with the misuse of their service through the dissemination of illegal content, such as the dissemination of child sexual abuse material or illegal hate speech, and the conduct of illegal activities, such as the sale of products or services prohibited by Union or national law, including counterfeit products. For example, and without prejudice to the personal responsibility of the recipient of the service of very large online platforms for possible illegality of his or her activity under the applicable law, such dissemination or activities may constitute a significant systematic risk where access to such content may be amplified through accounts with a particularly wide reach. A second category concerns the impact of the service on the exercise of fundamental rights, as protected by the Charter of Fundamental Rights, including the freedom of expression and information, the right to private life, the right to non-discrimination and the rights of the child. Such risks may arise, for example, in relation to the design of the algorithmic systems used by the very large online platform or the misuse of their service through the submission of abusive notices or other methods for silencing speech or hampering competition. A third category of risks concerns the intentional and, oftentimes, coordinated manipulation of the platform's service, with a foreseeable impact on public health, civic discourse, electoral processes, public security and protection of minors. Such risks may arise, for example, through the creation of fake accounts, the use of bots, and other automated or partially automated behaviours, which may lead to the rapid and widespread dissemination of information that is illegal content or incompatible with an online platform's terms and conditions.
- (58) Very large online platforms should deploy the necessary means to diligently mitigate the systemic risks identified in the risk assessment. Very large online platforms should under such mitigating measures consider, for example, enhancing or otherwise adapting the design and functioning of their content moderation, algorithmic recommender systems and online interfaces, so that they discourage and limit the dissemination of illegal content, adapting their decision-making processes, or adapting their terms and conditions. They may also include corrective measures, such as discontinuing advertising revenue for specific content, or other actions, such as improving the visibility of authoritative information sources. Very large online

platforms may reinforce their internal processes or supervision of any of their activities, in particular as regards the detection of systemic risks. They may also initiate or increase cooperation with trusted flaggers, organise training sessions and exchanges with trusted flagger organisations, and cooperate with other service providers, including by initiating or joining existing codes of conduct or other self-regulatory measures. Any measures adopted should respect the due diligence requirements of this Regulation and be effective and appropriate for mitigating the specific risks identified and should be proportionate in light of the very large online platform's economic capacity and the need to avoid unnecessary restrictions on the use of their service, taking due account of potential negative effects on the fundamental rights of the recipients of the service.

- (59) Very large online platforms 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.
- (60) Given the need to ensure verification by independent experts, very large online platforms 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. They should give the auditor access to all relevant data necessary to perform the audit properly. Auditors should also be able to make use of other sources of objective information, including studies by vetted researchers. Auditors should guarantee the confidentiality, security and integrity of the information, such as trade secrets, that they obtain when performing their tasks and have the necessary expertise in the area of risk management and technical competence to audit algorithms. Auditors should be independent, so as to be able to perform their tasks in an adequate and trustworthy manner. If their independence is not beyond doubt, they should resign or abstain from the audit engagement.
- (61) The audit report should be substantiated, so as 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 very large online platform to comply with their obligations under this Regulation. The report should be transmitted to the Digital Services Coordinator of establishment and the Board without delay, together with the risk assessment and the mitigation measures, as well as the platform's plans for addressing the audit's recommendations. The 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 very large online platform 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 very large online platform does not comply with this Regulation or the commitments undertaken.
- (62) A core part of a very large 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. They also play an important role in the amplification of certain messages, the viral dissemination of information and the stimulation of online behaviour. Consequently, very large online platforms should ensure that recipients are appropriately informed, and can influence the information presented to them. They should clearly present the main parameters for such recommender systems in an easily comprehensible manner to ensure that the recipients understand how information is prioritised for them. They should also ensure that the recipients enjoy alternative options for the main parameters, including options that are not based on profiling of the recipient.

- (63) Advertising systems used by very large online platforms 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 online interface. Very large online platforms should ensure public access to repositories of advertisements displayed 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 and related data on the advertiser and the delivery of the advertisement, in particular where targeted advertising is concerned.
- (64) In order to appropriately supervise the compliance of very large online platforms 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. Such a requirement may include, for example, the data necessary to assess the risks and possible harms brought about by the platform's systems, data on the accuracy, functioning and testing of algorithmic systems for content moderation, recommender systems or advertising systems, or data on processes and outputs of content moderation or of internal complaint-handling systems within the meaning of this Regulation. 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 online platforms, Digital Services Coordinators, other competent authorities, the Commission and the public. This Regulation therefore provides a framework for compelling access to data from very large online platforms to vetted researchers. All requirements for access to data under that framework should be proportionate and appropriately protect the rights and legitimate interests, including trade secrets and other confidential information, of the platform and any other parties concerned, including the recipients of the service.
- (65) Given the complexity of the functioning of the systems deployed and the systemic risks they present to society, very large online platforms should appoint compliance officers, which should have the necessary qualifications to operationalise measures and monitor the compliance with this Regulation within the platform's organisation. Very large online platforms should ensure that the compliance officer is involved, properly and in a timely manner, in all issues which relate to this Regulation. In view of the additional risks relating to their activities and their additional obligations under this Regulation, the other transparency requirements set out in this Regulation, should be complemented by additional transparency requirements applicable specifically to

very large online platforms, notably to report on the risk assessments performed and subsequent measures adopted as provided by this Regulation.

- (66) 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 industry standards covering certain technical procedures, where the industry can help develop standardised means to comply with this Regulation, such as allowing the submission of notices, including through application programming interfaces, or about the interoperability of advertisement repositories. 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.
- (67) The Commission and the Board should encourage the drawing-up of codes of conduct to contribute to the application of this Regulation. 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 guidance provided by the Commission and the Board, by participating in the same codes of conduct.
- (68) It is appropriate that this Regulation identify certain areas of consideration for such codes of conducts. 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 on systemic societal risks, such as disinformation or manipulative and abusive activities. This includes coordinated operations aimed at amplifying information, such as the use of bots or fake accounts for the creation of fake or misleading information, sometimes with a purpose of obtaining economic gain, which are particularly harmful for vulnerable recipients of the service, such as children. In relation to such areas, adherence to and compliance with a given code of conduct by a very large online platform may be considered as an appropriate risk mitigating measure. The refusal without proper explanations by an online platform of the Commission's invitation to participate in the drawing up and application of such a code of conduct could be taken into account, where relevant, when determining whether the online platform has infringed the obligations laid down by this Regulation.
- (69) The provision of online advertising generally involves several actors, including intermediary services that connect publishers of advertising with advertisers. Codes of conducts should support and complement the transparency obligations relating to advertisement for online platforms and very large online platforms 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. 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.
- (70) In case of extraordinary circumstances affecting public security or public health, the Commission may initiate the drawing up of crisis protocols to coordinate a rapid,

collective and cross-border response in the online environment. Extraordinary circumstances may entail any unforeseeable event, such as earthquakes, hurricanes, pandemics, war and acts of terrorism, where, for example, online platforms may be 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, 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 very large online platforms to monitor the information which they transmit or store, nor actively to seek facts or circumstances indicating illegal content.

- (71) The task of ensuring adequate oversight and enforcement of the obligations laid down in this Regulation should in principle be attributed to the Member States. To this end, they should appoint at least one authority with the task to apply and enforce this Regulation. 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, such as electronic communications' regulators, media regulators or consumer protection authorities, reflecting their domestic constitutional, organisational and administrative structure.
- (72) Given the cross-border nature of the services at stake and the horizontal range of obligations introduced by this Regulation, the 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 apply and enforce this Regulation, only one authority in that Member State should be identified 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 should ensure effective involvement of all relevant authorities in the supervision and enforcement at Union level.
- (73) 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 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 these 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 national control or monitoring mechanisms regarding their financial expenditure or to judicial review, or that they should not have the possibility to consult

other national authorities, including law enforcement authorities or crisis management authorities, where appropriate.

- (74) Member States can designate an existing national authority with the function of the Digital Services Coordinator, or with specific tasks to apply 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.
- (75) In the absence of a general requirement for providers of intermediary services to ensure a physical presence within the territory of one of the Member States, there is a need to ensure clarity under which Member State's jurisdiction those providers fall for the purposes of enforcing the rules laid down in this Regulation by the national competent authorities. A provider should be under the jurisdiction of the Member State where its main establishment 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 do not have an establishment 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 jurisdiction, considering the function of legal representatives under this Regulation. In the interest of the effective application of this Regulation, all Member States should, however, have jurisdiction in respect of providers that failed to designate a legal representative, provided that the principle of *ne bis in idem* is respected. To that aim, each Member State that exercises jurisdiction in respect of such providers should, without undue delay, inform all other Member States of the measures they have taken in the exercise of that jurisdiction.
- (76) 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. 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 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.
- (77) 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.
- (78) 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 in principle take all relevant facts and circumstances of the case into account, including information gathered by competent authorities in other Member States.

- (79) 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, whether the provider is active in several Member States.
- (80) In order to ensure effective enforcement of this Regulation, individuals or representative organisations should be able to lodge any complaint related to compliance with this Regulation with the Digital Services Coordinator in the territory where they received the service, without prejudice to this Regulation's rules on jurisdiction. Complaints should 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.
- (81) Member States should ensure that, where all other powers to bring about the cessation of an infringement of this Regulation have been exhausted without success and it is necessary to avoid serious harm in particular to Union citizens, Digital Services Coordinators can request the management body of the provider to identify and overcome any problems identified and draw up an action plan to overcome those problems and a timetable for its implementation and, where this does not bring the expected results and the recurrent infringements relate to serious criminal offences involving a threat to the life or safety of persons, to request a competent judicial authority to order the temporary restriction of access of recipients of the service to the online interface of the provider of intermediary services infringing this Regulation. Such requests such only be made when existing powers to order the disabling of access to online interfaces as provided by national or Union laws, 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 are being used by a third party to infringe an intellectual property right, are unavailable.

- (82) Such an order should not go beyond what is necessary to achieve its objective. For that purpose, it should 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.
- (83) The Digital Services Coordinator should regularly publish a report on the activities carried out under this Regulation. 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 common information sharing system, the Digital Services Coordinator should include in its annual report the number and categories of these orders addressed to providers of intermediary services issued by judicial and administrative authorities in its Member State.
- (84) Where a Digital Services Coordinator requests another Digital Services Coordinator to take action, the requesting Digital Services Coordinator, or the Board in case it issued a recommendation to assess issues involving more than three Member States, 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 a failure to adopt any measures. The Commission, on the basis of the information made available by the concerned authorities, should accordingly be able to request the competent Digital Services Coordinator to re-assess the matter and take the necessary measures to ensure compliance within a defined time 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. A failure by the Digital Services Coordinator of establishment to take any measures pursuant to such a request may also lead to the Commission's intervention under Section 3 of Chapter IV of this Regulation, where the suspected infringer is a very large online platform
- (85) In order to facilitate cross-border supervision and investigations involving several Member States, the Digital Services Coordinators should be able to participate, on a permanent or temporary basis, in joint oversight and investigation activities concerning matters covered by this Regulation. Those activities may include other competent authorities and may cover a variety of issues, ranging from coordinated data gathering exercises to requests for information or inspections of premises, within the limits and scope of powers available to each participating authority. The Board may be requested to provide advice in relation to those activities, for example by proposing roadmaps and timelines for activities or proposing ad-hoc task-forces with participation of the authorities involved.
- (86) In view of the particular challenges that may emerge in relation to assessing and ensuring a very large online platform's compliance, for instance relating to the scale or complexity of a suspected infringement or the need for particular expertise or capabilities at Union level, Digital Services Coordinators should have the possibility to request the Commission to intervene and exercise its investigatory and enforcement powers under this Regulation. Such intervention upon request should require the consent of both the requesting Digital Services Coordinator and the Commission. However, once the Commission initiated the proceedings, the Digital Services Coordinator should be precluded from exercising its powers in respect of the conduct of the platform at issue, so as to avoid duplication, inconsistencies and risks from the viewpoint of the principle of *ne bis in idem*.

- (87) In order to ensure a consistent application of this Regulation, it is necessary to set up an independent advisory group at Union level, which should support the Commission and help coordinate the actions of Digital Services Coordinators. That European Board for Digital Services should consist of the Digital Services Coordinators, 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.
- (88) The Board should contribute to achieving a common Union perspective on the consistent application of this Regulation and to 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 very large online platforms. The Board should also contribute to the drafting of relevant templates and codes of conduct and analyse emerging general trends in the development of digital services in the Union.
- (89) For that purpose, the Board should be able to adopt opinions, requests and recommendations addressed to Digital Service 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.
- (90) 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 equality between women and men, and non-discrimination, data protection, electronic communications, audiovisual services, detection and investigation of frauds against the EU budget as regards custom duties, or consumer protection, as necessary for the performance of its tasks.
- (91) 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.
- (92) 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.
- (93) Given the importance of very large online platforms, 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.

- (94) In order to address those public policy concerns it is therefore necessary to provide for a common system of enhanced supervision and enforcement at Union level. Once an infringement has been identified, for instance pursuant to individual or joint investigations, auditing or complaints, the Digital Services Coordinator of establishment, upon its own initiative or upon the Board's advice, should monitor any subsequent measure taken by the very large online platform concerned as set out in its action plan, and inform the Board and the Commission. The Digital Services Coordinator should be able to ask for an additional, specific audit to be carried out, on a voluntary basis, where it considers that the measures outlined in the plan may not be sufficient to address the infringement. The Digital Services Coordinator should perform its role under this common system in a timely manner and taking utmost account of any opinions and other advice of the Board.
- (95) Where the infringement by the very large online platform is not effectively addressed pursuant to the action plan, the Commission may, on its own initiative or upon advice of the Board, decide to further investigate the infringement concerned and the measures that the platform has subsequently taken. After having conducted the necessary investigations, the Commission should be able to issue decisions finding an infringement and imposing sanctions in respect of very large online platforms where that is justified, including in cross-border situations where the Digital Services Coordinator of establishment did not take any measures despite the Commission's request or where the Digital Services Coordinator of establishment issued a request for the Commission to intervene. In that regard, the Commission should, where appropriate, take account of any relevant assessments carried out by the Board or by the Digital Services Coordinators concerned and of any relevant evidence and information gathered by them, without prejudice to the Commission's powers and responsibility to carry out additional investigations as necessary.
- (96) In view of both the particular challenges that may arise in seeking to ensure compliance by very large online platforms 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 certain of the rules laid down in this Regulation, in full respect of the principle of proportionality and the rights and interests of the affected parties.
- (97) 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 that the very large online platform concerned or relevant third parties, or than individuals 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, or from any natural person or legal person for the purpose of this Regulation. The Commission should be empowered to require access to, and explanations relating to, data-bases and algorithms of undertakings, and to interview any persons who may be in possession of useful information and to record the statements made. 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

- (98) 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.
- (99) The very large online platforms 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 lead up to the decision.
- (100) In the interest of effectiveness and efficiency, in addition to the general evaluation of the Regulation, to be performed within five years of entry into force, after the initial start-up phase and on the basis of the first three years of application of this Regulation, the Commission should also perform an evaluation of the activities of the Board and on its structure.
- (101) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council<sup>43</sup>.
- (102) In order to fulfil the objectives of this Regulation, the power to adopt acts in accordance with Article 290 of the Treaty should be delegated to the Commission to supplement this Regulation. In particular, delegated acts should be adopted in respect of criteria for identification of very large online platforms and of technical specifications for access requests. It is of particular importance that the Commission carries out appropriate consultations and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016. 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.
- (103) 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 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

<sup>43</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).

fundamental rights conflict, a fair balance between the rights concerned, in accordance with the principle of proportionality.

- (104) Since the objective of this Regulation, namely 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 its 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 that objective,

HAVE ADOPTED THIS REGULATION:

## **Chapter I – General provisions**

### *Article 1*

#### *Subject matter and scope*

1. 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.
2. The aims of this Regulation are to:
  - (a) contribute to the proper functioning of the internal market for intermediary services;
  - (b) set out uniform rules for a safe, predictable and trusted online environment, where fundamental rights enshrined in the Charter are effectively protected.
3. This Regulation shall apply to intermediary services provided to recipients of the service that have their place of establishment or residence in the Union, irrespective of the place of establishment of the providers of those services.
4. 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.
5. This Regulation is without prejudice to the rules laid down by the following:
  - (a) Directive 2000/31/EC;
  - (b) Directive 2010/13/EC;
  - (c) Regulation (EU) .../.... on preventing the dissemination of terrorist content online [TCO once adopted];
  - (d) Regulation (EU) .../....on European Production and Preservation Orders for electronic evidence in criminal matters and Directive (EU) .../....laying down

harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings [e-evidence once adopted]

- (e) Regulation (EU) 2019/1148;
- (f) Regulation (EU) 2019/1150;
- (g) Union law on consumer protection and product safety, including Regulation (EU) 2017/2394;
- (h) Union law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC;
- (i) Union law on copyright and related rights.

*Article 2*  
*Definitions*

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

- (a) ‘information society services’ means services within the meaning of Article 1(1)(b) of Directive (EU) 2015/1535;
- (b) ‘recipient of the service’ means any natural or legal person who uses the relevant intermediary service;
- (c) ‘consumer’ means any natural person who is acting for purposes which are outside his or her trade, business or profession;
- (d) ‘to offer services in the Union’ means enabling legal or natural persons in one or more Member States to use the services of the provider of information society services which has a substantial connection to the Union; such a substantial connection is deemed to exist where the provider has an establishment in the Union; in the absence of such an establishment, the assessment of a substantial connection is based on specific factual criteria, such as:
  - a significant number of users in one or more Member States; or
  - the targeting of activities towards one or more Member States.
- (e) ‘trader’ means any natural person, or any legal person irrespective of whether 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;
- (f) ‘intermediary service’ means one of the following services:
  - a ‘mere conduit’ service 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;
  - a ‘caching’ service that consists 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, for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request;
  - a ‘hosting’ service that consists of the storage of information provided by, and at the request of, a recipient of the service;

- (g) ‘illegal content’ means any information, which, in itself or by its reference to an activity, including the sale of products or provision of services is not in compliance with Union law or the law of a Member State, irrespective of the precise subject matter or nature of that law;
- (h) ‘online platform’ means a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information, unless that activity is a minor and purely ancillary feature of another service and, for objective and technical reasons cannot be used without that other service, and the integration of the feature into the other service is not a means to circumvent the applicability of this Regulation.
- (i) ‘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;
- (j) ‘distance contract’ means a contract within the meaning of Article 2(7) of Directive 2011/83/EU;
- (k) ‘online interface’ means any software, including a website or a part thereof, and applications, including mobile applications;
- (l) ‘Digital Services Coordinator of establishment’ means the Digital Services Coordinator of the Member State where the provider of an intermediary service is established or its legal representative resides or is established;
- (m) ‘Digital Services Coordinator of destination’ means the Digital Services Coordinator of a Member State where the intermediary service is provided;
- (n) ‘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 displayed by an online platform on its online interface against remuneration specifically for promoting that information;
- (o) ‘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, including as a result of a search initiated by the recipient or otherwise determining the relative order or prominence of information displayed;
- (p) ‘content moderation’ means the activities undertaken by providers of intermediary services aimed 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, disabling of access to, or removal thereof, or the recipients’ ability to provide that information, such as the termination or suspension of a recipient’s account;
- (q) ‘terms and conditions’ means all terms and conditions or specifications, irrespective of their name or form, which govern the contractual relationship between the provider of intermediary services and the recipients of the services.

## Chapter II – Liability of providers of intermediary services

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

### *Article 4* *'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 the information's onward transmission to other recipients of the service upon their request, on condition that:
  - (a) the provider does not modify the information;
  - (b) the provider complies with conditions on access to the information;
  - (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
  - (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
  - (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.
2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

*Article 5*  
*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 liability under consumer protection law of online platforms allowing 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 and reasonably well-informed 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 court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

*Article 6*  
*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 3, 4 and 5 solely because they carry out voluntary own-initiative investigations or other activities aimed at detecting, identifying and removing, or disabling of access to, illegal content, or take the necessary measures to comply with the requirements of Union law, including those set out in this Regulation.

*Article 7*  
*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 8*  
*Orders to act against illegal content*

1. Providers of intermediary services shall, upon the receipt of an order to act against a specific item of illegal content, issued by the relevant national judicial or administrative authorities, on the basis of the applicable Union or national law, in conformity with Union law, inform the authority issuing the order of the effect given to the orders, without undue delay, specifying the action taken and the moment when the action was taken.

2. Member States shall ensure that the orders referred to in paragraph 1 meet the following conditions:
  - (a) the order contains the following elements:
    - a statement of reasons explaining why the information is illegal content, by reference to the specific provision of Union or national law infringed;
    - one or more exact uniform resource locators and, where necessary, additional information enabling the identification of the illegal content concerned;
    - information about redress available to the provider of the service and to the recipient of the service who provided the content;
  - (b) the territorial scope of the order, on the basis of the applicable rules of Union and national law, including the Charter, and, where relevant, general principles of international law, does not exceed what is strictly necessary to achieve its objective;
  - (c) the order is drafted in the language declared by the provider and is sent to the point of contact, appointed by the provider, in accordance with Article 10.
3. The Digital Services Coordinator from the Member State of the judicial or administrative authority issuing the order shall, without undue delay, transmit a copy of the orders referred to in paragraph 1 to all other Digital Services Coordinators through the system established in accordance with Article 67.

*Article 9*  
*Orders to provide information*

1. Providers of intermediary services shall, upon receipt of an order to provide a specific item of 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 or national law, in conformity with Union law, inform without undue delay the authority issuing the order of its receipt.
2. Member States shall ensure that orders referred to in paragraph 1 meet the following conditions:
  - (a) the order contains the following elements:
    - a statement of reasons explaining the objective for which the information is required and why the requirement to provide the information is necessary for and proportionate to determine compliance by the recipients of the intermediary services with applicable Union or national rules, clearly identified in the order;
    - information about redress available to the provider and to the recipients of the service concerned;
  - (b) the order only requires the provider to provide information already collected for the purposes of providing the service and which lies within its control;
  - (c) the order is drafted in the language declared by the provider and is sent to the point of contact appointed by that provider, in accordance with Article 10;
3. The Digital Services Coordinator from the Member State of the national judicial or administrative authority issuing the order shall, without undue delay, transmit a copy

of the order referred to in paragraph 1 to all Digital Services Coordinators through the system established in accordance with Article 67.

## **Chapter III**

### **Due diligence obligations for a transparent and safe online environment**

#### **SECTION 1**

#### **PROVISIONS APPLICABLE TO ALL PROVIDERS OF INTERMEDIARY SERVICES**

##### *Article 10* *Points of contact*

1. Providers of intermediary services shall establish a single point of contact allowing for direct communication, by electronic means, with Member States' authorities, the Commission and the Board referred to in Article 47 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.
3. Providers of intermediary services shall specify in the information referred to in paragraph 2, the official language or languages of the Union, which 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 11* *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 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 to be addressed in addition to or instead of the provider by the Member States' 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 the necessary powers and resource to cooperate with the Member States' authorities, the Commission and the Board and comply with those decisions.
3. The designated legal representative can be held liable for non-compliance with obligations under this Regulation, without prejudice to the liability and legal actions that could be initiated against the provider of intermediary services.
4. Providers of intermediary services shall notify the name, address, the electronic mail address and telephone number of their legal representative to the Digital Service Coordinator in the Member State where that legal representative resides or is established. They shall ensure that that information is up to date.



5. The designation of a legal representative within the Union pursuant to paragraph 1 shall not amount to an establishment in the Union.

*Article 12*  
*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. It shall be set out in clear and unambiguous language and shall be publicly available in an easily accessible format.
2. 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 applicable fundamental rights of the recipients of the service as enshrined in the Charter.

*Article 13*  
*Transparency reporting obligations for providers of intermediary services*

1. Providers of intermediary services shall publish, at least once a year, clear, easily comprehensible and detailed reports on any content moderation they engaged in during the relevant period. Those reports shall include, in particular, information on the following, as applicable:
  - (a) the number of orders received from Member States' authorities, categorised by the type of illegal content concerned, including orders issued in accordance with Articles 8 and 9, and the average time needed for taking the action specified in those orders;
  - (b) the number of notices submitted in accordance with Article 14, categorised by the type of alleged illegal content concerned, 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, and the average time needed for taking the action;
  - (c) the content moderation engaged in at the providers' own initiative, including 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, categorised by the type of reason and basis for taking those measures;
  - (d) the number of complaints received through the internal complaint-handling system referred to in Article 17, the basis for those complaints, decisions taken in respect of those complaints, the average time needed for taking those decisions and the number of instances where those decisions were reversed.
2. Paragraph 1 shall not apply to providers of intermediary services that qualify as micro or small enterprises within the meaning of the Annex to Recommendation 2003/361/EC.

## SECTION 2

### ADDITIONAL PROVISIONS APPLICABLE TO PROVIDERS OF HOSTING SERVICES, INCLUDING ONLINE PLATFORMS

#### *Article 14*

##### *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, user-friendly, and 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, on the basis of which a diligent economic operator can identify the illegality of the content in question. To that end, the providers shall take the necessary measures to enable and facilitate the submission of notices containing all of the following elements:
  - (a) an explanation of the reasons why the individual or entity considers the information in question to be illegal content;
  - (b) a clear indication of the electronic location of that information, in particular the exact URL or URLs, and, where necessary, additional information enabling the identification of the illegal content;
  - (c) the name and an electronic mail 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 good faith belief of the individual or entity submitting the notice that the information and allegations contained therein are accurate and complete.
3. Notices that include the elements referred to in paragraph 2 shall be considered to give rise to actual knowledge or awareness of the purposes of Article 5 in respect of the specific item of information concerned.
4. Where the notice contains the name and an electronic mail address of the individual or entity that submitted it, the provider of hosting services shall promptly 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 redress possibilities 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 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 4.

*Article 15*  
*Statement of reasons*

1. Where a provider of hosting services decides to remove or disable access to specific items of information provided by the recipients of the service, irrespective of the means used for detecting, identifying or removing or disabling access to that information and of the reason for its decision, it shall inform the recipient, at the latest at the time of the removal or disabling of access, of the decision and provide a clear and specific statement of reasons for that decision.
2. The statement of reasons referred to in paragraph 1 shall at least contain the following information:
  - (a) whether the decision entails either the removal of, or the disabling of access to, the information and, where relevant, the territorial scope of the disabling of access;
  - (b) the facts and circumstances relied on in taking the decision, including where relevant whether the decision was taken pursuant to a notice submitted in accordance with Article 14;
  - (c) where applicable, information on the use made of automated means in taking the decision, including where 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, a reference to the contractual ground relied on and explanations as to why the information is considered to be incompatible with that ground;
  - (f) information on the redress possibilities available to the recipient of the service in respect of the decision, in particular through internal complaint-handling mechanisms, out-of-court dispute settlement and judicial redress.
3. 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 redress possibilities referred to in point (f) of paragraph 2.
4. Providers of hosting services shall publish the decisions and the statements of reasons, referred to in paragraph 1 in a publicly accessible database managed by the Commission. That information shall not contain personal data.

**SECTION 3**  
**ADDITIONAL PROVISIONS APPLICABLE TO ONLINE PLATFORMS**

*Article 16*  
*Exclusion for micro and small enterprises*

This Section shall not apply to online platforms that qualify as micro or small enterprises within the meaning of the Annex to Recommendation 2003/361/EC.

*Article 17*  
*Internal complaint-handling system*

1. Online platforms shall provide recipients of the service, for a period of at least six months following the decision referred to in this paragraph, the access to an effective internal complaint-handling system, which enables the complaints to be lodged electronically and free of charge, against the following decisions taken by the online platform on the ground that the information provided by the recipients is illegal content or incompatible with its terms and conditions:
  - (a) decisions to remove or disable access to the information;
  - (b) decisions to suspend or terminate the provision of the service, in whole or in part, to the recipients;
  - (c) decisions to suspend or terminate the recipients' account.
2. 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.
3. Online platforms shall handle complaints submitted through their internal complaint-handling system in a timely, diligent and objective manner. Where a complaint contains sufficient grounds for the online platform to consider 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 suspension or termination of the service or the account, it shall reverse its decision referred to in paragraph 1 without undue delay.
4. Online platforms shall inform complainants without undue delay of the decision they have taken in respect of the information to which the complaint relates and shall inform complainants of the possibility of out-of-court dispute settlement provided for in Article 18 and other available redress possibilities.
5. Online platforms shall ensure that the decisions, referred to in paragraph 4, are not solely taken on the basis of automated means.

*Article 18*  
*Out-of-court dispute settlement*

1. Recipients of the service addressed by the decisions referred to in Article 17(1), shall be entitled to select any out-of-court dispute that has been certified in accordance with paragraph 2 in order to resolve disputes relating to those decisions, including complaints that could not be resolved by means of the internal complaint-handling system referred to in that Article. Online platforms shall engage, in good faith, with the body selected with a view to resolving the dispute and shall be bound by the decision taken by the body.

The first subparagraph is without prejudice to the right of the recipient concerned to redress against the decision before a court in accordance with the applicable law.
2. The Digital Services Coordinator of the Member State where the out-of-court dispute settlement body is established shall, at the request of that body, certify the body, where the body has demonstrated that it meets all of the following conditions:
  - (a) it is impartial and independent of online platforms and recipients of the service provided by the online platforms;

- (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 platforms, allowing the body to contribute effectively to the settlement of a dispute;
- (c) the dispute settlement is easily accessible through electronic communication technology;
- (d) it is capable of settling dispute in a swift, efficient and cost-effective manner and in at least one official language of the Union;
- (e) the dispute settlement takes place in accordance with clear and fair rules of procedure.

The Digital Services Coordinator shall, where applicable, specify in the certificate the particular issues to which the body's expertise relates and the official language or languages of the Union in which the body is capable of settling disputes, as referred to in points (b) and (d) of the first subparagraph, respectively.

3. If the body decides the dispute in favour of the recipient of the service, the online platform shall reimburse the recipient for any fees and other reasonable expenses that the recipient has paid or is to pay in relation to the dispute settlement. If the body decides the dispute in favour of the online platform, the recipient shall not be required to reimburse any fees or other expenses that the online platform paid or is to pay in relation to the dispute settlement.

The fees charged by the body for the dispute settlement shall be reasonable and shall in any event not exceed the costs thereof.

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 services and the online platform concerned before engaging in the dispute settlement.

4. 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 2.

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 2.

5. Digital Services Coordinators shall notify to the Commission the out-of-court dispute settlement bodies that they have certified in accordance with paragraph 2, including where applicable the specifications referred to in the second subparagraph of that paragraph. The Commission shall publish a list of those bodies, including those specifications, on a dedicated website, and keep it updated.
6. This Article is without prejudice to Directive 2013/11/EU and alternative dispute resolution procedures and entities for consumers established under that Directive.

#### *Article 19* *Trusted flaggers*

1. Online platforms shall take the necessary technical and organisational measures to ensure that notices submitted by trusted flaggers through the mechanisms referred to in Article 14, are processed and decided upon without delay.

2. The status of trusted flaggers under this Regulation shall be awarded, upon application by any entities, by the Digital Services Coordinator of the Member State in which the applicant is established, where the applicant has demonstrated to meet all of the following conditions:
  - (a) it has particular expertise and competence for the purposes of detecting, identifying and notifying illegal content;
  - (b) it represents collective interests and is independent from any online platform;
  - (c) it carries out its activities for the purposes of submitting notices in a timely, diligent and objective manner.
3. Digital Services Coordinators shall communicate to the Commission and the Board the names, addresses and electronic mail addresses of the entities to which they have awarded the status of the trusted flagger in accordance with paragraph 2.
4. The Commission shall publish the information referred to in paragraph 3 in a publicly available database and keep the database updated.
5. Where an online platform has information indicating that a trusted flagger submitted a significant number of insufficiently precise or inadequately substantiated notices through the mechanisms referred to in Article 14, including information gathered in connection to the processing of complaints through the internal complaint-handling systems referred to in Article 17(3), 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.
6. 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 by third parties, including the information provided by an online platform pursuant to paragraph 5, 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
7. The Commission, after consulting the Board, may issue guidance to assist online platforms and Digital Services Coordinators in the application of paragraphs 5 and 6.

#### *Article 20*

##### *Measures and protection against misuse*

1. 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. 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 14 and 17, respectively, by individuals or entities or by complainants that frequently submit notices or complaints that are manifestly unfounded.
3. Online platforms shall assess, on a case-by-case basis and in a timely, diligent and objective manner, whether a recipient, individual, entity or 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 online platform. 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 in the past year;
  - (b) the relative proportion thereof in relation to the total number of items of information provided or notices submitted in the past year;
  - (c) the gravity of the misuses and its consequences;
  - (d) the intention of the recipient, individual, entity or complainant.
4. Online platforms shall set out, in a clear and detailed manner, their policy in respect of the misuse referred to in paragraphs 1 and 2 in their terms and conditions, including as regards the facts and circumstances that they take into account when assessing whether certain behaviour constitutes misuse and the duration of the suspension.

#### *Article 21*

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

1. Where an online platform becomes aware of any information giving rise to a suspicion that a serious criminal offence involving a threat to the life or safety of 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 online platform 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 has its legal representative or inform Europol.

For the purpose of this Article, the Member State concerned shall be the Member State where the offence is suspected to have taken place, be taking place and 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.

#### *Article 22*

##### *Traceability of traders*

1. Where an online platform allows consumers to conclude distance contracts with traders, it shall ensure that traders can only use its services to promote messages on or to offer products or services to consumers located in the Union if, prior to the use of its services, the online platform has obtained the following information:
  - (a) the name, address, telephone number and electronic mail 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>44</sup>;
  - (c) the bank account details of the trader, where the trader is a natural person;

<sup>44</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

- (d) the name, address, telephone number and electronic mail address of the economic operator, within the meaning of Article 3(13) and Article 4 of Regulation (EU) 2019/1020 of the European Parliament and the Council<sup>45</sup> or any relevant act of Union law;
  - (e) 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;
  - (f) a self-certification by the trader committing to only offer products or services that comply with the applicable rules of Union law.
2. The online platform shall, upon receiving that information, make reasonable efforts to assess whether the information referred to in points (a), (d) and (e) of paragraph 1 is reliable through the use of any freely accessible official online database or online interface made available by a Member States or the Union or through requests to the trader to provide supporting documents from reliable sources.
3. Where the online platform obtains indications that any item of information referred to in paragraph 1 obtained from the trader concerned is inaccurate or incomplete, that platform shall request the trader to correct the information in so far as necessary to ensure that all information is accurate and complete, without delay or within the time period set by Union and national law.

Where the trader fails to correct or complete that information, the online platform shall suspend the provision of its service to the trader until the request is complied with.
4. The online platform shall store the information obtained pursuant to paragraph 1 and 2 in a secure manner for the duration of their contractual relationship with the trader concerned. They shall subsequently delete the information.
5. Without prejudice to paragraph 2, the platform shall only disclose the information to third parties where so required in accordance with the applicable law, including the orders referred to in Article 9 and any orders issued by Member States' competent authorities or the Commission for the performance of their tasks under this Regulation.
6. The online platform shall make the information referred to in points (a), (d), (e) and (f) of paragraph 1 available to the recipients of the service, in a clear, easily accessible and comprehensible manner.

### *Article 23*

#### *Transparency reporting obligations for providers of online platforms*

1. In addition to the information referred to in Article 13, 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 18, the outcomes of the dispute settlement and the average time needed for completing the dispute settlement procedures;

<sup>45</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).



- (b) the number of suspensions imposed pursuant to Article 20, distinguishing between suspensions enacted for the provision of manifestly illegal content, the submission of manifestly unfounded notices and the submission of manifestly unfounded complaints;
  - (c) any use made of automatic means for the purpose of content moderation, including a specification of the precise purposes, indicators of the accuracy of the automated means in fulfilling those purposes and any safeguards applied.
2. Online platforms shall publish, at least once every six months, information on the average monthly active recipients of the service in each Member State, calculated as an average over the period of the past six months, in accordance with the methodology laid down in the delegated acts adopted pursuant to Article 25(2).
3. Online platforms shall communicate to the Digital Services Coordinator of establishment, upon its request, the information referred to in paragraph 2, updated to the moment of such request. That Digital Services Coordinator may require the online platform 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. The Commission may adopt implementing acts to lay down templates concerning the form, content and other details of reports pursuant to paragraph 1.

#### *Article 24*

##### *Online advertising transparency*

Online platforms that display advertising on their online interfaces shall ensure that the recipients of the service can identify, for each specific advertisement displayed to each individual recipient, in a clear and unambiguous manner and in real time:

- (a) that the information displayed is an advertisement;
- (b) the natural or legal person on whose behalf the advertisement is displayed;
- (c) meaningful information about the main parameters used to determine the recipient to whom the advertisement is displayed.

#### **SECTION 4**

##### **ADDITIONAL OBLIGATIONS FOR VERY LARGE ONLINE PLATFORMS TO MANAGE SYSTEMIC RISKS**

#### *Article 25*

##### *Very large online platforms*

1. This Section shall apply to online platforms which provide their services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, calculated in accordance with the methodology set out in the delegated acts referred to in paragraph 3.
2. The Commission shall adopt delegated acts in accordance with Article 69 to adjust the number of average monthly recipients of the service in the Union referred to in paragraph 1, where the Union's population increases or decreases at least with 5 % in relation to its population in 2020. In that 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 shall adopt delegated acts in accordance with Article 69, after consulting the Board, to lay down a specific methodology for calculating the number of average monthly active recipients of the service in the Union, for the purposes of paragraph 1. The methodology shall specify, in particular, how to determine the Union's population and criteria to determine the average monthly active recipients of the service in the Union, taking into account different accessibility features.
4. The Digital Services Coordinator of establishment shall verify, at least every six months, whether the number of average monthly active recipients of the service in the Union of online platforms under their jurisdiction is equal to or higher than the number referred to in paragraph 1. On the basis of that verification, it shall adopt a decision designating the online platform as a very large online platform for the purposes of this Regulation, or terminating that designation, and communicate that decision, without undue delay, to the online platform concerned and to the Commission.

The Commission shall ensure that the list of designated very large online platforms is published in the Official Journal of the European Union and keep that list updated. The obligations of this Section shall apply, or cease to apply, to the very large online platforms concerned from four months after that publication.

*Article 26*  
*Risk assessment*

1. Very large online platforms shall identify, analyse and assess, from the date of application referred to in the second subparagraph of Article 25(4), at least once a year thereafter, any significant systemic risks stemming from the functioning and use made of their services in the Union. This risk assessment shall be specific to their services and shall include the following systemic risks:
  - (a) the dissemination of illegal content through their services;
  - (b) any negative effects for the exercise of the fundamental rights to respect for private and family life, freedom of expression and information, the prohibition of discrimination and the rights of the child, as enshrined in Articles 7, 11, 21 and 24 of the Charter respectively;
  - (c) intentional manipulation of their service, including by means of inauthentic use or automated exploitation of the service, with an actual or foreseeable negative effect on the protection of public health, minors, civic discourse, or actual or foreseeable effects related to electoral processes and public security.
2. When conducting risk assessments, very large online platforms shall take into account, in particular, how their content moderation systems, recommender systems and systems for selecting and displaying advertisement influence any of the systemic risks referred to in paragraph 1, including the potentially rapid and wide dissemination of illegal content and of information that is incompatible with their terms and conditions.

*Article 27*  
*Mitigation of risks*

1. Very large online platforms shall put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified pursuant to Article 26. Such measures may include, where applicable:
  - (a) adapting content moderation or recommender systems, their decision-making processes, the features or functioning of their services, or their terms and conditions;
  - (b) targeted measures aimed at limiting the display of advertisements in association with the service they provide;
  - (c) reinforcing the internal processes or supervision of any of their activities in particular as regards detection of systemic risk;
  - (d) initiating or adjusting cooperation with trusted flaggers in accordance with Article 19 or other online platforms, including through the codes of conduct and the crisis protocols referred to in Article 35 and 37 respectively.
2. The Board, in cooperation with the Commission, shall publish comprehensive reports, once a year, which shall include the following:
  - (a) identification and assessment of the most prominent and recurrent systemic risks reported by very large online platforms or identified through other information sources, in particular those provided in compliance with Article 31 and 33;
  - (b) best practices for very large online platforms to mitigate the systemic risks identified.
3. The Commission, in cooperation with the Digital Services Coordinators, may issue general 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 28*  
*Independent audit*

1. Very large online platforms shall be subject, at their own expense and at least once a year, to 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 35 and 36 and the crisis protocols referred to in Article 37.
2. Audits performed pursuant to paragraph 1 shall be performed by organisations which:
  - (a) are independent from the very large online platform concerned;
  - (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.
3. The organisations that perform the audits shall establish an audit report for each audit. The report shall be in writing and include at least the following:
- (a) the name, address and the point of contact of the very large online platform subject to the audit and the period covered;
  - (b) the name and address of the organisation performing the audit;
  - (c) a description of the specific elements audited, and the methodology applied;
  - (d) a description of the main findings drawn from the audit;
  - (e) an audit opinion on whether the very large online platform subject to the audit complied with the obligations and with the commitments referred to in paragraph 1, either positive, positive with comments or negative;
  - (f) where the audit opinion is not positive, operational recommendations on specific measures to achieve compliance.
4. Very large online platforms receiving an audit report that is not positive shall take due account of any 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 they may have taken to address any instances of non-compliance identified.

*Article 29*  
*Recommender systems*

1. Very large online platforms that use recommender systems shall set out in their terms and conditions, in a clear, accessible and easily comprehensible manner, 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 that they may have made available, including at least one option which is not based on profiling, within the meaning of Article 4 (4) of Regulation (EU) 2016/679.
2. Where several options are available pursuant to paragraph 1, very large online platforms shall provide an easily accessible functionality on their online interface allowing the recipient of the service to select and to modify at any time their preferred option for each of the recommender systems that determines the relative order of information presented to them.

*Article 30*  
*Additional online advertising transparency*

1. Very large online platforms that display advertising on their online interfaces shall compile and make publicly available through application programming interfaces a repository containing the information referred to in paragraph 2, until one year after the advertisement was displayed 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 displayed.

2. The repository shall include at least all of the following information:
  - (a) the content of the advertisement;
  - (b) the natural or legal person on whose behalf the advertisement is displayed;
  - (c) the period during which the advertisement was displayed;
  - (d) whether the advertisement was intended to be displayed specifically to one or more particular groups of recipients of the service and if so, the main parameters used for that purpose;
  - (e) the total number of recipients of the service reached and, where applicable, aggregate numbers for the group or groups of recipients to whom the advertisement was targeted specifically.

*Article 31*  
*Data access and scrutiny*

1. Very large online platforms shall provide the Digital Services Coordinator of establishment or the Commission, upon their reasoned request and within a reasonable period, specified in the request, access to data that are necessary to monitor and assess compliance with this Regulation. That Digital Services Coordinator and the Commission shall only use that data for those purposes.
2. Upon a reasoned request from the Digital Services Coordinator of establishment or the Commission, very large online platforms shall, within a reasonable period, as specified in the request, provide access to data to vetted researchers who meet the requirements in paragraphs 4 of this Article, for the sole purpose of conducting research that contributes to the identification and understanding of systemic risks as set out in Articles 26(1).
3. Very large online platforms shall provide access to data pursuant to paragraphs 1 and 2 through online databases or application programming interfaces, as appropriate.
4. In order to be vetted, researchers shall be affiliated with academic institutions, be independent from commercial interests, have proven records of expertise in the fields related to the risks investigated or related research methodologies, and shall commit and be in a capacity to preserve the specific data security and confidentiality requirements corresponding to each request.
5. The Commission shall, after consulting the Board, adopt delegated acts laying down the technical conditions under which very large online platforms are to share data pursuant to paragraphs 1 and 2 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 vetted researchers can take place in compliance with Regulation (EU) 2016/679, taking into account the rights and interests of the very large online platforms and the recipients of the service concerned, including the protection of confidential information, in particular trade secrets, and maintaining the security of their service.
6. Within 15 days following receipt of a request as referred to in paragraph 1 and 2, a very large online platform may request the Digital Services Coordinator of establishment or the Commission, as applicable, to amend the request, where it considers that it is unable to give access to the data requested because one of following two reasons:

- (a) it does not have access to the data;
  - (b) giving access to the data will lead to significant vulnerabilities for the security of its service or the protection of confidential information, in particular trade secrets.
7. Requests for amendment pursuant to point ( b) of paragraph 6 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 or the Commission shall decide upon the request for amendment within 15 days and communicate to the very large online platform its decision and, where relevant, the amended request and the new time period to comply with the request.

*Article 32*  
*Compliance officers*

1. Very large online platforms shall appoint one or more compliance officers responsible for monitoring their compliance with this Regulation.
2. Very large online platforms shall only designate as compliance officers persons who have the professional qualifications, knowledge, experience and ability necessary to fulfil the tasks referred to in paragraph 3. Compliance officers may either be staff members of, or fulfil those tasks on the basis of a contract with, the very large online platform concerned.
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) organising and supervising the very large online platform's activities relating to the independent audit pursuant to Article 28;
  - (c) informing and advising the management and employees of the very large online platform about relevant obligations under this Regulation;
  - (d) monitoring the very large online platform's compliance with its obligations under this Regulation.
4. Very large online platforms shall take the necessary measures to ensure that the compliance officers can perform their tasks in an independent manner.
5. Very large online platforms shall communicate the name and contact details of the compliance officer to the Digital Services Coordinator of establishment and the Commission.
6. Very large online platforms shall support the compliance officer in the performance of his or her tasks and provide him or her with the resources necessary to adequately carry out those tasks. The compliance officer shall directly report to the highest management level of the platform.

### *Article 33*

#### *Transparency reporting obligations for very large online platforms*

1. Very large online platforms shall publish the reports referred to in Article 13 within six months from the date of application referred to in Article 25(4), and thereafter every six months.
2. In addition to the reports provided for in Article 13, very large online platforms shall make publicly available and transmit to the Digital Services Coordinator of establishment and the Commission, at least once a year and within 30 days following the adoption of the audit implementing report provided for in Article 28(4):
  - (a) a report setting out the results of the risk assessment pursuant to Article 26;
  - (b) the related risk mitigation measures identified and implemented pursuant to Article 27;
  - (c) the audit report provided for in Article 28(3);
  - (d) the audit implementation report provided for in Article 28(4).
3. Where a very large online platform considers that the publication of information pursuant to paragraph 2 may result in the disclosure of confidential information of that platform or of the recipients of the service, may cause significant vulnerabilities for the security of its service, may undermine public security or may harm recipients, the platform may remove such information from the reports. In that case, that platform 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 public reports.

## **SECTION 5**

### **OTHER PROVISIONS CONCERNING DUE DILIGENCE OBLIGATIONS**

### *Article 34*

#### *Standards*

1. The Commission shall support and promote the development and implementation of voluntary industry standards set by relevant European and international standardisation bodies at least for the following:
  - (a) electronic submission of notices under Article 14;
  - (b) electronic submission of notices by trusted flaggers under Article 19, including through application programming interfaces;
  - (c) specific interfaces, including application programming interfaces, to facilitate compliance with the obligations set out in Articles 30 and 31;
  - (d) auditing of very large online platforms pursuant to Article 28;
  - (e) interoperability of the advertisement repositories referred to in Article 30(2);
  - (f) transmission of data between advertising intermediaries in support of transparency obligations pursuant to points (b) and (c) of Article 24.
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.

*Article 35*  
*Codes of conduct*

1. The Commission and the Board shall encourage and facilitate the drawing up of 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 26(1) emerge and concern several very large online platforms, the Commission may invite the very large online platforms concerned, other very large online platforms, other online platforms and other providers of intermediary services, as appropriate, as well as civil society organisations and other interested parties, 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 shall aim to ensure that the codes of conduct clearly set out their 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, including 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 Service Coordinators of establishment on any measures taken and their outcomes, as measured against the key performance indicators that they contain.
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. They shall publish their conclusions.
5. The Board shall regularly monitor and evaluate the achievement of the objectives of the codes of conduct, having regard to the key performance indicators that they may contain.

*Article 36*  
*Codes of conduct for online advertising*

1. The Commission shall encourage and facilitate the drawing up of codes of conduct at Union level between, online platforms and other relevant service providers, such as providers of online advertising intermediary services or organisations representing recipients of the service and civil society organisations or relevant authorities to contribute to further transparency in online advertising beyond the requirements of Articles 24 and 30.
2. The Commission shall aim to ensure that the codes of conduct pursue an effective transmission of information, in full respect for the rights and interests of all parties involved, and a competitive, transparent and fair environment in online advertising, in accordance with Union and national law, in particular on competition and the protection of personal data. The Commission shall aim to ensure that the codes of conduct address at least:
  - (a) the transmission of information held by providers of online advertising intermediaries to recipients of the service with regard to requirements set in points (b) and (c) of Article 24;



- (b) the transmission of information held by providers of online advertising intermediaries to the repositories pursuant to Article 30.
3. The Commission shall encourage the development of the codes of conduct within one year following the date of application of this Regulation and their application no later than six months after that date.

*Article 37*  
*Crisis protocols*

1. The Board may recommend the Commission to initiate the drawing up, in accordance with paragraphs 2, 3 and 4, of crisis protocols for addressing crisis situations strictly limited to extraordinary circumstances affecting public security or public health.
2. The Commission shall encourage and facilitate very large online platforms and, where appropriate, other online platforms, with the involvement of the Commission, to participate in the drawing up, testing and application of those crisis protocols, which include one or more of the following measures:
  - (a) displaying prominent information on the crisis situation provided by Member States' authorities or at Union level;
  - (b) ensuring that the point of contact referred to in Article 10 is responsible for crisis management;
  - (c) where applicable, adapt the resources dedicated to compliance with the obligations set out in Articles 14, 17, 19, 20 and 27 to the needs created by the crisis situation.
3. The Commission may involve, as appropriate, Member States' authorities and 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 point (e) of paragraph 4, it may request the participants to revise the crisis protocol, including by taking additional measures.

## **Chapter IV**

### **Implementation, cooperation, sanctions and enforcement**

#### **SECTION 1**

#### **COMPETENT AUTHORITIES AND NATIONAL DIGITAL SERVICES COORDINATORS**

##### *Article 38*

##### *Competent authorities and Digital Services Coordinator*

1. Member States shall designate one or more competent authorities as responsible for the application 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 application 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 application 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 regular exchanges of views with other authorities where relevant for the performance of the tasks of those other authorities and of the Digital Services Coordinator.

Where a Member State designates more than one competent authority 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. The Member State concerned shall communicate the name of the other competent authorities as well as their respective tasks to the Commission and the Board.

3. Member States shall designate the Digital Services Coordinators within two months from the date of entry into force of this Regulation.  
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.
4. The requirements applicable to Digital Services Coordinators set out in Articles 39, 40 and 41 shall also apply to any other competent authorities that the Member States designate pursuant to paragraph 1.

*Article 39*  
*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 adequate technical, financial and human resources to carry out their tasks.
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 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 38(2). Paragraph 2 shall not prevent supervision of the authorities concerned in accordance with national constitutional law.

*Article 40*  
*Jurisdiction*

1. The Member State in which the main establishment of the provider of intermediary services is located shall have jurisdiction for the purposes of this Regulation.
2. A provider of intermediary services which does not have an establishment in the Union but which offers services in the Union shall be deemed to be under the jurisdiction of the Member State where its legal representative resides or is established.
3. Where a provider of intermediary services fails to appoint a legal representative in accordance with Article 11, all Member States shall have jurisdiction. Where a Member State decides to exercise jurisdiction under this paragraph, it shall inform all other Member States and ensure that the principle of *ne bis in idem* is respected.
4. Paragraphs 1 and 2 are without prejudice to Article 51(3) and the tasks and powers of the Commission under Section 3.

*Article 41*  
*Powers of Digital Services Coordinators*

1. Where needed for carrying out their tasks, Digital Services Coordinators shall have at least the following powers of investigation, in respect of conduct by providers of intermediary services under the jurisdiction 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 Articles 28 and 50(3), to provide such information within a reasonable time period;
  - (b) the power to carry out on-site 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.

2. Where needed for carrying out their tasks, Digital Services Coordinators shall have at least the following enforcement powers, in respect of providers of intermediary services under the jurisdiction 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;
- (c) the power to impose fines in accordance with Article 42 for failure to comply with this Regulation, including with any of the orders issued pursuant to paragraph 1;
- (d) the power to impose a periodic penalty payment in accordance with Article 42 to ensure that an infringement is terminated in compliance with an order issued pursuant to point (b) of this paragraph or for failure to comply with any of the orders issued pursuant to paragraph 1;
- (e) the power to adopt interim measures to avoid the risk of serious harm;
- (f) where all powers pursuant to this Article to bring about the cessation of an infringement have been exhausted without achieving such cessation and the infringement causes serious harm which cannot be avoided through the exercise of other powers available under Union or national law, the power to take, in a phased manner the following measures:
  - require the management body of the provider subject to reasonable deadlines, to examine the situation, identify measures to overcome any problems identified and draw up an action programme to overcome those problems and a timetable for its implementation;
  - where the provider has not complied within the reasonable deadline set by the Digital Services Coordinator with requirements imposed under the first indent of this sub-paragraph, and where the recurrent infringements relate to serious criminal offences involving a threat to the life or safety of persons, request a competent judicial authority of that Member State to order the temporary restriction of access of recipients of 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.

As regards points (c) and (d) of the first subparagraph, 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 having provided those other persons in good time with all relevant information relating to such orders, including the applicable time period, the fines or

periodic payments that may be imposed for failure to comply and redress possibilities.

As regards point (f) of the first subparagraph, the Digital Services Coordinator shall, except where it acts upon the Commission's request referred to in Article 65, prior to submitting the request, invite interested parties to submit written observations within a time 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 intended addressee or addressees and any other third parties 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 services concerned. The period of temporary restriction under the second indent of point (f) shall initially not exceed one week and shall be extended for further periods of one week only where the Digital Services Coordinator is satisfied, in light of the representations of the provider and of interested third parties, that adequate measures to prevent recurring infringements have not been put in place and that, by virtue of the reach of the service in question and the existence of adequate and readily accessible alternatives, recipients of the service concerned will continue to have free and ample access to lawful information of their choice.

3. The powers listed in paragraph 1 and 2 are without prejudice to Section 3.
4. The measures taken by the Digital Services Coordinators in the exercise of their powers listed in paragraphs 1 and 2 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.
5. Member States shall ensure that any exercise of the powers pursuant to paragraphs 1 and 2 is subject to adequate safeguards laid down in the applicable national law in conformity 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 42* *Penalties*

1. Member States shall lay down the rules on penalties applicable to infringements of this Regulation by providers of intermediary services under their jurisdiction and shall take all the necessary measures to ensure that they are implemented in accordance with Article 41.
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 penalties imposed for a failure to comply with the obligations laid down in this Regulation shall not exceed 6 % of the annual income or turnover of the provider of intermediary services

concerned. Penalties for the supply of incorrect, incomplete or misleading information, failure to reply or rectify incorrect, incomplete or misleading information and to submit to an on-site inspection shall not exceed 1% of the annual income or turnover of the provider concerned.

4. Member States shall ensure that the maximum amount of a periodic penalty payment shall not exceed 5 % of the average daily turnover of the provider of intermediary services concerned in the preceding financial year per day, calculated from the date specified in the decision concerned.

#### *Article 43*

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

Recipients of the service 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 resides or is established. The Digital Services Coordinator shall assess the complaint and, where appropriate, transmit it to the Digital Services Coordinator of establishment. Where the complaint falls under the responsibility of another competent authority in its Member State, the Digital Service Coordinator receiving the complaint shall transmit it to that authority.

#### *Article 44*

##### *Activity reports*

1. Digital Services Coordinators shall draw up an annual report on their activities under this Regulation. They shall make the annual reports available to the public, and shall communicate them to the Commission and to the Board.
2. The annual report shall include at least 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 8 and 9 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 8 and 9.
3. Where a Member State has designated several competent authorities pursuant to Article 38, 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.

#### *Article 45*

##### *Cross border cooperation among Digital Services Coordinators*

1. Where a Digital Services Coordinator has reasons to suspect that a provider of an intermediary service, not under the jurisdiction of the Member State concerned, infringed this Regulation, it shall 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.

Where the Board has reasons to suspect that a provider of intermediary services infringed this Regulation in a manner involving at least three Member States, it may

recommend the Digital Services Coordinator of establishment to assess the matter and take the necessary investigatory and enforcement measures to ensure compliance with this Regulation.

2. A request or recommendation pursuant to paragraph 1 shall at least indicate:
  - (a) the point of contact of the provider of the intermediary services concerned as provided for in Article 10;
  - (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;
  - (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.
3. The Digital Services Coordinator of establishment shall take into utmost account the request or recommendation pursuant to paragraph 1. Where it considers that it has insufficient information to act upon the request or recommendation and has reasons to consider that the Digital Services Coordinator that sent the request, or the Board could provide additional information, it may request such information. The time period laid down in paragraph 4 shall be suspended until that additional information is provided.
4. The Digital Services Coordinator of establishment shall, without undue delay and in any event not later than two months following receipt of the request or recommendation, communicate to the Digital Services Coordinator that sent the request, or the Board, its assessment of the suspected infringement, or that of any other competent authority pursuant to national law where relevant, and an explanation of any investigatory or enforcement measures taken or envisaged in relation thereto to ensure compliance with this Regulation.
5. Where the Digital Services Coordinator that sent the request, or, where appropriate, the Board, did not receive a reply within the time period laid down in paragraph 4 or where it does not agree with the assessment of the Digital Services Coordinator of establishment, it 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, any additional information provided pursuant to paragraph 3 and the communication referred to in paragraph 4.
6. The Commission shall assess the matter within three months following the referral of the matter pursuant to paragraph 5, after having consulted the Digital Services Coordinator of establishment and, unless it referred the matter itself, the Board.
7. Where, pursuant to paragraph 6, the Commission concludes that the assessment or the investigatory or enforcement measures taken or envisaged pursuant to paragraph 4 are incompatible with this Regulation, it shall request the Digital Service Coordinator of establishment to further assess the matter and take the necessary investigatory or enforcement measures to ensure compliance with this Regulation and to inform it about those measures taken within two months from that request.

*Article 46*

*Joint investigations and requests for Commission intervention*

1. Digital Services Coordinators may participate in joint investigations, which may be coordinated with the support of the Board, with regard to matters covered by this Regulation, concerning providers of intermediary services operating in several Member States.
2. Such joint investigations are without prejudice to the tasks and powers of the participating Digital Coordinators and the requirements applicable to the performance of those tasks and exercise of those powers provided in this Regulation. The participating Digital Services Coordinators shall make the results of the joint investigations available to other Digital Services Coordinators, the Commission and the Board through the system provided for in Article 67 for the fulfilment of their respective tasks under this Regulation.
3. Where a Digital Services Coordinator of establishment has reasons to suspect that a very large online platform infringed this Regulation, it may request the Commission to take the necessary investigatory and enforcement measures to ensure compliance with this Regulation in accordance with Section 3. Such a request shall contain all information listed in Article 45(2) and set out the reasons for requesting the Commission to intervene.

**SECTION 2**

**EUROPEAN BOARD FOR DIGITAL SERVICES**

*Article 47*

*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 guidance 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 48*

*Structure of the Board*

1. The Board shall be composed of the Digital Services Coordinators, who shall be represented by high-level officials. 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 shall participate in the Board. Other national authorities may be invited to the meetings, where the issues discussed are of relevance for them.

2. Each Member State shall have one vote. The Commission shall not have voting rights.

The Board shall adopt its acts by simple majority.

3. The Board shall be chaired by the Commission. The Commission shall convene the meetings and prepare the agenda in accordance the tasks of the Board pursuant to this Regulation and with its rules of procedure.
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 shall adopt its rules of procedure, following the consent of the Commission.

*Article 49*  
*Tasks of the Board*

1. Where necessary to meet the objectives set out in Article 47(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 to be transmitted pursuant to this Regulation;
  - (c) issue opinions, recommendations or advice to Digital Services Coordinators in accordance with this Regulation;
  - (d) advise the Commission to take the measures referred to in Article 51 and, where requested by the Commission, adopt opinions on draft Commission measures concerning very large online platforms in accordance with this Regulation;
  - (e) support and promote the development and implementation of European standards, guidelines, reports, templates and code of conducts as provided for in this Regulation, as well as the identification of emerging issues, with regard to matters covered by this Regulation.
2. Digital Services Coordinators and other national 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 when reporting pursuant to this Regulation or when adopting their relevant decisions, as appropriate..

**SECTION 3**  
**SUPERVISION, INVESTIGATION, ENFORCEMENT AND MONITORING IN RESPECT**  
**OF VERY LARGE ONLINE PLATFORMS**

*Article 50*

*Enhanced supervision for very large online platforms*

1. Where the Digital Services Coordinator of establishment adopts a decision finding that a very large online platform has infringed any of the provisions of Section 4 of Chapter III, it shall make use of the enhanced supervision system laid down in this Article. It shall take utmost account of any opinion and recommendation of the Commission and the Board pursuant to this Article.

The Commission acting on its own initiative, or the Board acting on its own initiative or upon request of at least three Digital Services Coordinators of destination, may, where they have serious concerns about a suspected infringement of any of those provisions, recommend the Digital Services Coordinator of establishment to investigate the suspected infringement with a view to that Digital Services Coordinator adopting such a decision within a reasonable time period.

2. When communicating the decision referred to in paragraph 1 to the very large online platform concerned, the Digital Services Coordinator of establishment shall request it to draw up an action plan within one month, specifying how that platform intends to terminate or remedy the infringement. The platform shall communicate the action plan to the Digital Services Coordinator of establishment, the Commission and the Board. The measures set out in the action plan may include, where appropriate, participation in a code of conduct as provided for in Article 35.
3. Within one month following receipt of the action plan, the Board shall communicate its opinion on the action plan to the Digital Services Coordinator of establishment. Within one month following receipt of that opinion, that Digital Services Coordinator shall decide whether the action plan is appropriate to terminate or remedy the infringement it has established.

Where it considers the action plan inappropriate or where the very large online platform does not present an action plan pursuant to paragraph 2, the Digital Services Coordinator shall communicate its views and the reasons therefor to the Commission and the Board. Where the Digital Services Coordinator of establishment has concerns on the ability of the measures to terminate or remedy the infringement, it may request the very large online platform concerned to subject itself to an additional, independent audit within two months of the implementation of the action plan or the relevant part thereof, to assess the effectiveness of those measures in terminating or remedying the infringement. The platform concerned shall communicate the results of the audit to the Digital Services Coordinator of establishment, the Commission and the Board. When requesting such an additional audit, the Digital Services Coordinator may specify a particular audit organisation that is to carry out the audit, at the expense of the platform concerned, selected on the basis of criteria set out in Article 28(2).

4. The Digital Services Coordinator of establishment shall, within one month following receipt of the results of the audit where such an audit was performed, or within three months from the decision pursuant to the first subparagraph of paragraph 3, communicate to the Commission, the Board and the very large online platform

concerned its views as to whether the very large online platform has terminated or remedied the infringement established and the reasons thereof.

*Article 51*

*Intervention by the Commission and opening of proceedings*

1. The Commission, acting either upon the Board's recommendation or on its own initiative after consulting the Board, initiate proceedings in view of the possible adoption of decisions pursuant to Articles 58 and 59 in respect of the relevant conduct by the very large online platform that:
2. infringed any of the provisions of Section 4 of Chapter III, pursuant to the communication referred to in Article 50(4);
3. is suspected of having infringed any of the provisions of this Regulation and the Digital Services Coordinator of establishment did not take any investigatory or enforcement measures, or did not inform the Commission of those measures within the set time period, pursuant to the request of the Commission referred to in Article 45(7);
4. is suspected of having infringed any of the provisions of this Regulation and the Digital Services Coordinator of establishment requested the Commission to intervene in accordance with Article 46(2)
5. Where the Commission decides to initiate proceedings pursuant to paragraph 1, it shall notify all Digital Services Coordinators, the Board and the very large online platform concerned.
6. Pursuant to the notification referred to in paragraph 2, the Digital Services Coordinator of establishment concerned shall no longer be entitled to take any investigatory or enforcement measures in respect of the relevant conduct by the very large online platform concerned, without prejudice to Article 66 or any other measures that it may take at the request of the Commission.
7. The Digital Services Coordinator referred to in Article 50(1) or in Article 45(7), as applicable, shall, without undue delay upon being informed, transmit to the Commission:
8. any information that that Digital Services Coordinator exchanged relating to the infringement or the suspected infringement, as applicable, with the Board and with the very large online platform concerned;
9. the case file of that Digital Services Coordinator relating to the infringement or the suspected infringement, as applicable;
10. any other information in the possession of that Digital Services Coordinator that may be relevant to the proceedings initiated by the Commission.
11. The Board and the Digital Services Coordinators making the request referred to in Article 45(1) shall, without undue upon being informed, transmit to the Commission any information in their possession that may be relevant to the proceedings initiated by the Commission.

*Article 52*  
*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 very large online platforms concerned, as well as any other persons acting for purposes related to their trade, business, craft or profession that may be reasonably be aware of information relating to the suspected infringement or the infringement, as applicable, including organisations performing the audits referred to in Articles 28 and 50(3), to provide such information within a reasonable time period.
2. When sending a simple request for information to the very large online platform concerned or other person referred to in Article 52(1), the Commission shall state the legal basis and the purpose of the request, specify what information is required and set the time period within which the information is to be provided, and the penalties provided for in Article 59 for supplying incorrect or misleading information.
3. Where the Commission requires the very large online platform concerned or other person referred to in Article 52(1) 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 time period within which it is to be provided. It shall also indicate the penalties provided for in Article 59 and indicate or impose the periodic penalty payments provided for in Article 60. It shall further indicate the right to have the decision reviewed by the Court of Justice of the European Union.
4. The owners of the the very large online platform concerned or other person referred to in Article 52(1) or their representatives and, in the case of legal persons, companies or firms, or associations having no legal personality, the persons authorised to represent them by law or by their constitution shall supply the information requested on behalf of the the very large online platform concerned or other person referred to in Article 52(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.

*Article 53*  
*Power to take interviews and statements*

In order to carry out the tasks assigned to it under this Section, the Commission may interview any natural or legal person which consents to being interviewed for the purpose of collecting information, relating to the subject-matter of an investigation, in relation to the suspected infringement or infringement, as applicable.

*Article 54*  
*Power to conduct on-site inspections*

1. In order to carry out the tasks assigned to it under this Section, the Commission may conduct on-site inspections at the premises of the very large online platform concerned or other person referred to in Article 52(1).

2. On-site inspections may also be carried out with the assistance of auditors or experts appointed by the Commission pursuant to Article 57(2).
3. During on-site inspections the Commission and auditors or experts appointed by it may require the very large online platform concerned or other person referred to in Article 52(1) to provide explanations on its organisation, functioning, IT system, algorithms, data-handling and business conducts. The Commission and auditors or experts appointed by it may address questions to key personnel of the very large online platform concerned or other person referred to in Article 52(1).
4. The very large online platform concerned or other person referred to in Article 52(1) is required to submit to an on-site inspection ordered by decision of the Commission. The decision shall specify the subject matter and purpose of the visit, set the date on which it is to begin and indicate the penalties provided for in Articles 59 and 60 and the right to have the decision reviewed by the Court of Justice of the European Union.

*Article 55*  
*Interim measures*

1. In the context of proceedings which may lead to the adoption of a decision of non-compliance pursuant to Article 58(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 such very large online platform 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 56*  
*Commitments*

1. If, during proceedings under this Section, the very large online platform concerned offers commitments to ensure compliance with the relevant provisions of this Regulation, the Commission may by decision make those commitments binding on that respective very large online platform 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 very large online platform concerned acts contrary to its commitments; or
  - (c) where the decision was based on incomplete, incorrect or misleading information provided by the very large online platform concerned or other person referred to in Article 52(1).
3. Where the Commission considers that the commitments offered by the very large online platform 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 57*  
*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 that very large online platform concerned. The Commission may also order that platform to provide access to, and explanations relating to, its databases and algorithms.
2. The actions pursuant to paragraph 1 may include the appointment of independent external experts and auditors to assist the Commission in monitoring compliance with the relevant provisions of this Regulation and to provide specific expertise or knowledge to the Commission.

*Article 58*  
*Non-compliance*

1. The Commission shall adopt a non-compliance decision where it finds that the very large online platform 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 55;
  - (c) commitments made binding pursuant to Article 56,
2. Before adopting the decision pursuant to paragraph 1, the Commission shall communicate its preliminary findings to the very large online platform concerned. In the preliminary findings, the Commission shall explain the measures that it considers taking, or that it considers that the very large online platform 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 very large online platform concerned to take the necessary measures to ensure compliance with the decision pursuant to paragraph 1 within a reasonable time period and to provide information on the measures that that platform intends to take to comply with the decision.
4. The very large online platform 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.

*Article 59*  
*Fines*

1. In the decision pursuant to Article 58, the Commission may impose on the very large online platform concerned fines not exceeding 6% of its total turnover in the preceding financial year where it finds that that platform, intentionally or negligently:
  - (a) infringes the relevant provisions of this Regulation;
  - (b) fails to comply with a decision ordering interim measures under Article 55; or

- (c) fails to comply with a voluntary measure made binding by a decision pursuant to Articles 56.
2. The Commission may by decision impose on the very large online platform concerned or other person referred to in Article 52(1) fines not exceeding 1% of the total turnover in the preceding financial year, where they intentionally or negligently:
  - (a) supply incorrect, incomplete or misleading information in response to a request pursuant to Article 52 or, when the information is requested by decision, fail to reply to the request within the set time period;
  - (b) fail to rectify within the time period set by the Commission, incorrect, incomplete or misleading information given by a member of staff, or fail or refuse to provide complete information;
  - (c) refuse to submit to an on-site inspection pursuant to Article 54.
3. Before adopting the decision pursuant to paragraph 2, the Commission shall communicate its preliminary findings to the very large online platform concerned or other person referred to in Article 52(1).
4. In fixing the amount of the fine, the Commission shall have regard to the gravity, duration, recurrence, and, for fines imposed pursuant to paragraph 2, delay caused to the proceedings.

*Article 60*  
*Periodic penalty payments*

1. The Commission may, by decision, impose on the very large online platform concerned or other person referred to in Article 52(1), as applicable, periodic penalty payments not exceeding 5 % of the average daily 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 52;
  - (b) submit to an on-site inspection which it has ordered by decision pursuant to Article 54;
  - (c) comply with a decision ordering interim measures pursuant to Article 55(1);
  - (d) comply with commitments made legally binding by a decision pursuant to Article 56(1);
  - (e) comply with a decision pursuant to Article 58(1).
2. Where the very large online platform concerned or other person referred to in Article 52(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 which would arise under the original decision.

*Article 61*  
*Limitation period for the imposition of penalties*

1. The powers conferred on the Commission by Articles 59 and 60 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) on-site inspection;
  - (c) the opening of a proceeding by the Commission pursuant to Article 51(2).
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 is 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 62*

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

1. The power of the Commission to enforce decisions taken pursuant to Articles 59 and 60 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.



*Article 63*  
*Right to be heard and access to the file*

1. Before adopting a decision pursuant to Articles 58(1), 59 or 60, the Commission shall give the very large online platform concerned or other person referred to in Article 52(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 very large online platform concerned or other person referred to in Article 52(1) may submit their observations on the Commission's preliminary findings within a reasonable time 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 very large online platform concerned or other person referred to in Article 52(1) in the protection of their business secrets. The right of access to the file shall not extend to confidential information and internal documents of the Commission or Member States' authorities. 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 52, 53 and 54 shall be used only for the purpose of this Regulation.
6. Without prejudice to the exchange and to the use of information referred to in Articles 51(3) and 52(5), the Commission, the Board, Member States' 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 57(2) shall not disclose information acquired or exchanged by them pursuant to this Section and of the kind covered by the obligation of professional secrecy.

*Article 64*  
*Publication of decisions*

1. The Commission shall publish the decisions it adopts pursuant to Articles 55(1), 56(1), 58, 59 and 60. 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 very large online platform concern, any other person referred to in Article 52(1) and any third parties in the protection of their confidential information.

#### *Article 65*

##### *Requests for access restrictions and cooperation with national courts*

1. Where all powers pursuant to this Article to bring about the cessation of an infringement of this Regulation have been exhausted without achieving such cessation and the infringement causes serious harm which cannot be avoided through the exercise of other powers available under Union or national laws, the Commission may request the Digital Services Coordinator of establishment of the very large platform to act pursuant to point (f) of Article 41(2).
2. Prior to making such request to the Digital Services Coordinator, the Commission shall invite interested parties to submit written observations within a time period that shall not be less than two weeks, describing the measures it intends to request and identifying the intended addressee or addressees thereof.
3. 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 in point (f) of Article 41(2). With the permission of the judicial authority in question, it may also make oral observations.
4. 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.

#### *Article 66*

##### *Implementing acts relating to Commission intervention*

1. In relation to the Commission intervention covered by in this Section, the Commission may adopt implementing acts concerning the practical arrangements for:
  - (c) the proceedings pursuant to Articles 54 and 57;
  - (a) the hearings provided for in Article 63;
  - (b) the negotiated disclosure of information provided for in Article 63.
2. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 70. Before the adoption of any measures pursuant to paragraph 1, the Commission shall publish a draft thereof and invite all interested parties to submit their comments within the time period set out therein, which shall not be less than one month.

### **SECTION 4**

#### **COMMON PROVISIONS ON ENFORCEMENT**

#### *Article 67*

##### *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.
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 70.

*Article 68*  
*Representation*

Without prejudice to Directive 2020/XX/EU of the European Parliament and of the Council<sup>46</sup>, recipients of intermediary services shall have the right to mandate a body, organisation or association to exercise the rights referred to in Articles 17, 18 and 19 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.

**SECTION 5**  
**DELEGATED ACTS**

*Article 69*  
*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 23, 25, and 31 shall be conferred on the Commission for an indeterminate period of time from [date of expected adoption of the Regulation].
3. The delegation of power referred to in Articles 23, 25 and 31 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. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
5. A delegated act adopted pursuant to Articles 23, 25 and 31 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.

---

<sup>46</sup> [Reference]

*Article 70  
Committee*

1. The Commission shall be assisted by 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 Article, Article 4 of Regulation (EU) No 182/2011 shall apply.

**Chapter V  
Final provisions**

*Article 71  
Deletion of certain provisions of Directive 2000/31/EC*

1. Articles 12 to 15 of Directive 2000/31/EC shall be deleted.
2. References to Articles 12 to 15 of Directive 2000/31/EC shall be construed as references to Articles 3, 4, 5 and 7 of this Regulation, respectively.

*Article 72  
Amendments to Directive 2020/XX/EC on Representative Actions for the Protection of the  
Collective Interests of Consumers*

3. The following is added to Annex I:  
“(X) Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC”

*Article 73  
Evaluation*

1. By five years after the entry into force of this Regulation at the latest, 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.
2. For the purpose of paragraph 1, Member States and the Board shall send information on the request of the Commission.
3. In carrying out the evaluations referred to in paragraph 1, the Commission shall take into account the positions and findings of the European Parliament, the Council, and other relevant bodies or sources.
4. By three years from the date of application of this Regulation at the latest, the Commission, after consulting the Board, shall carry out an assessment of the functioning of the Board 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 into utmost account 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 74*  
*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. It shall apply from [date - three months after its entry into force].

This Regulation shall be binding in its entirety and directly applicable in all Member States. Done at Brussels,

*For the European Parliament*  
*The*

*For the Council*