CA 1: Chapter I - General provisions
=> Covers AMs EPP 1, EPP 2, EPP 3, EPP 17, EPP 19, EPP 20, EPP 21, Left 73, Greens 74, S&D 75, Greens 77, Left 79, Left 80, EPP 81, Greens 82, Renew 84, S&D 85, Renew 87, ID 88, Greens 91, Left 211, S&D 213, ID 220, EPP 225, ID 231, S&D 232, ECR 237, Left 238, S&D 241, Left 243

(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[1], 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 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***, without lock-in effects***.

(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 right to privacy, the right to protection of personal data,*** 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, ***clear,*** 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.

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

(5) 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[2], 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 ***responsibility to uphold fundamental rights***.

(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.

(8) Such a substantial connection to the Union should be considered to exist where the service provider has an establishment in the Union or, in its absence, on the basis of ~~the existence of a significant number of users in one or more Member States, or the~~ targeting of activities towards one or more Member States. The targeting of activities towards one or more Member States can be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in that Member State, or the possibility of ordering products or services, or using a national top level domain. The targeting of activities towards a Member State could also be derived from the availability of an application in the relevant national application store, from the provision of local advertising or advertising in the language used in that Member State, or from the handling of customer relations such as by providing customer service in the language generally used in that Member State. A substantial connection should also be assumed where a service provider directs its activities to one or more Member State as set out in Article 17(1)(c) of Regulation (EU) 1215/2012 of the European Parliament and of the Council[3]. On the other hand, mere technical accessibility of a website from the Union cannot, on that ground alone, be considered as establishing a substantial connection to the Union.

(9) This Regulation should not affect the application of rules resulting from other acts of Union law regulating certain aspects of the provision of intermediary services, in particular Directive 2000/31/EC, with the exception of those changes introduced by this

[2] 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).

[3] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L351, 20.12.2012, p.1).

Regulation, Directive 2010/13/EU of the European Parliament and of the Council as amended,[4] and Regulation (EU) …/.. of the European Parliament and of the Council[5] – proposed Terrorist Content Online Regulation. Therefore, this Regulation leaves those other acts, which are to be considered lex specialis in relation to the generally applicable framework set out in this Regulation, unaffected. ***In the event of a conflict between lex specialis legislation, including their implementing national measures, and the present Regulation, the lex specialis provisions shall prevail***.

(10) For reasons of clarity, it should also be specified that this Regulation is without prejudice to Regulation (EU) 2019/1148 of the European Parliament and of the Council[6] and Regulation (EU) 2019/1150 of the European Parliament and of the Council,[7], Directive 2002/58/EC of the European Parliament and of the Council[8] and Regulation […/…] on temporary derogation from certain provisions of Directive 2002/58/EC[9] as well as Union law on consumer protection, in particular Directive 2005/29/EC of the European Parliament and of the Council[10], Directive 2011/83/EU of the European Parliament and of the Council[11] and Directive 93/13/EEC of the European Parliament and of the Council[12], as amended by Directive (EU) 2019/2161 of the European Parliament and of the Council[13], and on the protection of personal data, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council.[14] 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. This Regulation is also without prejudice to the rules of Union law on working conditions.

---

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

[5] Regulation (EU) …/.. of the European Parliament and of the Council – proposed Terrorist Content Online Regulation

[6] Regulation (EU) 2019/1148 of the European Parliament and of the Council on the marketing and use of explosives precursors, amending Regulation (EC) No 1907/2006 and repealing Regulation (EU) No 98/2013 (OJ L 186, 11.7.2019, p. 1).

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

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

[9] Regulation […/…] on temporary derogation from certain provisions of Directive 2002/58/EC.

[10] 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')

[11] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.

[12] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

[13] 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

[14] 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).

(11) It should be clarified that this Regulation is without prejudice to the rules of Union law on copyright and related rights***, as implemented in national law in compliance with Union law so as to ensure the highest level of protection of those 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 ***to cover*** information relating to illegal content, products, services and activities. In particular, that concept should be understood to refer to information, irrespective of its form, that under the applicable ***Union or national*** 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***, dangerous*** or counterfeit products, ***illegally-traded animals,*** 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. ***The Commission should provide guidance on how to identify illegal content.***

(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***, content-sharing platforms, livestreaming platfroms*** 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***, or otherwise play an active role in the dissemination of user-generated content***. ***Search engines and equivalent services may also be considered online platforms, if these services meet the definition of online platform set out this Regulation.*** However, in order to avoid imposing overly broad obligations, providers of hosting services should not be considered as online platforms***, for the entirety or for part of their service,*** where the dissemination to the public is merely a minor and purely ancillary feature of ***the principal*** service and that feature cannot, for objective technical reasons, be used without that 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. ***Similarly, link-sharing options or similar features of cloud-based solutions for storing user-generated content could constitute such a feature, where the possibility of disseminating content to the public is clearly an ancillary feature to the principal service of storing information and content.***

(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. ***Accordingly, where access to information requires registration or admittance to a group*** of users, ***that***

information ***should be considered to be*** disseminated to the public ***only where users seeking to access the*** information ***are automatically registered or admitted without a human decision or selection of whom to grant access***. 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 ***limited*** number of predetermined persons, ***taking into account the potential for groups to become tools for wide dissemination of content to the public***. Interpersonal Interpersonal communication services, as defined in Directive (EU) 2018/1972 of the European Parliament and of the Council,[15] such as emails or private messaging services, fall outside the scope of the definition of online platform set out in this Regulation. ***To the extent they qualify as 'mere conduit', 'caching' or 'hosting' services, those services should be able to benefit from liability exemptions provided for by 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.

[15] 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

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.

   (c a) interoperability requirements for very large online platforms.

2. The aims of this Regulation are to:

   (a) contribute to the proper functioning of the internal market for ***digital*** services***, including by creating a level playing-field***;

   (b) set out uniform rules for a safe, ***accessible,*** predictable and trusted online environment, where fundamental rights enshrined in the Charter are effectively protected***;***

   (ba) facilitate innovation, support the digital transition, encourage economic growth and encourage competition for digital services, while protecting users' and consumers' rights.

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) Union law on copyright and related rights;

   (d) Regulation (EU) …/…. on preventing the dissemination of terrorist content online [TCO once adopted];

   (e) 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]

   (f) Regulation (EU) 2019/1148;

   (g) Regulation (EU) 2019/1150;

   (h) Union law on consumer protection and product safety, including Regulation (EU) 2017/2394;

(i) Union law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC***;***

(ia) Directive (EU) 2019/882.

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 ***or*** in the absence of such an establishment, ***where the provider targets its 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 ***applies specific terms and conditions and,*** 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 ***the principal*** service and, for objective and technical reasons cannot be used without that ***principal*** service, and the integration of the feature into the other service is not a means to circumvent the applicability of this Regulation.

(ha) 'online marketplace' means an online platform that allows consumers to conclude distance contracts with other traders or consumers on the platform;

(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 ***has its main establishment*** or***, in the case that the intermediary service is not established in the European Union,*** its legal representative 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 ***indirect and direct forms of*** remuneration specifically for promoting that information;

(o) 'recommender system' means a fully or partially automated system used by an online platform to ***rank, prioritise and*** 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***;***

CA 2: Chapter II - Liability of providers of intermediary services
=> Covers AMs EPP 4, EPP 6, EPP 7, EPP 22, EPP 23, Greens 93, S&D 98, Greens 102, S&D 104, EPP 105, Greens 106, Greens 108, ID 109, EPP 112, S&D 113, ID 114, S&D 116, ECR 118, Greens 119, S&D 120, EPP 121, Renew 122, Renew 123, S&D 246-50, Greens 251, S&D 252, ID 264, EPP 266, S&D 267, Greens 276, ID 277

(15a) Applying effective end-to-end encryption to data is essential for trust in, and security on, the internet, as it effectively prevents unauthorised third party access and helps to ensure confidentiality of communications.

(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**,** automatic ***and passive*** processing of the information provided by the recipient of the service, the provider of intermediary services plays an active role of such a kind as to give it knowledge of, or control over, that information. Those exemptions should accordingly not be available in respect of liability relating to information provided not by the recipient of the service but by the provider of intermediary service itself, including where the information has been developed under the editorial responsibility of that provider ***or where the provider intermediary service promotes or references such content.***

(19) In view of the different nature of the activities of 'mere conduit', 'caching' and 'hosting' and the different position and abilities of the providers of the services in question, it is necessary to distinguish the rules applicable to those activities, in so far as under this Regulation they are subject to different requirements and conditions and their scope differs, as interpreted by the Court of Justice of the European Union.

(20) ***Where the main purpose of the information society service is to engage in or facilitate illegal activities or where*** a provider of intermediary services ~~that~~ deliberately collaborates with a recipient of the services in order to undertake illegal activities**,** ***the*** service ***should be deemed not to have been provided*** 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 ***in*** the ***content of 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 ***assess the grounds for and, when necessary, proceed to removing or disabling*** access to ***all copies of*** that content***.*** The removal or disabling of access should be undertaken in the observance of ***the principles enshrined in the Charter of Fundamental Rights, including*** the principle of freedom of expression***.*** The provider can obtain such actual knowledge or awareness through, in particular, its ***periodic*** 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 ***marketplaces***, 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, is 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 specified in such orders, issued in compliance with Union law, or the disabling of access to it. ***As a general rule, injunctions addressed to intermediary services should be considered as a last resort, where any other reasonable and proportionate action closer to the content owner is not available.***

(25) In order to create legal certainty and not to discourage ***automated or non-automated*** 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 ***for the purpose of detecting, identifying and acting against illegal content. Such activities should be accompanied by additional safeguards***. 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 ***or national*** law, including those set out in this Regulation as regards the implementation of their terms and conditions, should not lead to the unavailability of ***the*** exemptions

from liability ***set out in this Regulation***. 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 II of this Regulation concentrate on the exemption from liability of providers of intermediary services, it is important to recall that, despite the generally important role played by 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. ***Only where that intermediary has not responded to the request, should requests or orders be addressed, as a last resort, to intermediaries lower in the internet stack, for removing or blocking access to content, including all the necessary information for localising as precisely as possible the 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 ***or providers of services deeper in the internet stack, such as IT infrastructure services (on-premise, cloud-based and hybrid hosting solutions)***, 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. ***Services deeper in the internet stack acting as online intermediaries could be required to take proportionate action where the customer fails to remove the illegal content, unless technically impracticable.***

(28) Providers of intermediary services should not be subject to a monitoring obligation with respect to obligations of a general nature***, nor should they be required to use automated tools for content moderation***. 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. ***Such orders referred should not consist in requiring a service provider to introduce, exclusively at its own expense, a screening system which entails general and permanent monitoring in order to prevent any future infringement. However, such orders may require a host provider to remove information which it stores, the content of which is identical or equivalent to the content of information which was previously declared to be unlawful, or to block access to that information, irrespective of who requested the storage of that information, provided that the monitoring of and search for the information concerned is limited to information properly identified in the injunction, such as the name of the person concerned by the infringement determined previously, the circumstances in which that infringement was determined and equivalent content to that which was declared to be illegal, and does not require the host provider to carry out an independent assessment of that content.*** Nothing in this Regulation should be construed as an imposition of a general monitoring obligation. ***The Regulation should not be considered to be impeding upon the ability of*** ~~active fact finding obligation, or as a general obligation for~~ providers to ***undertake*** proactive measures to ***identify and remove*** ~~relation to~~ illegal content ***and to prevent its reappearance***.

(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 orders to act against illegal content may require providers of intermediary services to take steps, in the specific case, to remove identical or equivalent illegal content, within the same context. The orders to act against illegal content may also require providers of intermediary services to take steps to prevent the reappearance of the illegal content.*** 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**,** ***national 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 ***under either Union law or national law in compliance with Union law***, 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.

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 ***the provider***:

   (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 ***illegal content*** 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.

2a. Paragraph 1 shall not apply when the main purpose of the information society service is to engage in or facilitate illegal activities or when the provider of the information society service deliberately collaborates with a recipient of the service in order to undertake illegal activities.

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 ***on the platform***, 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 ***take*** voluntary own-initiative ***investigation measures for the purpose of*** detecting, identifying and removing, or disabling ~~of~~ access to, illegal content,~~, or take the necessary measures~~ ***including through the use of technological tools and instruments, in order*** to comply with the requirements of Union law, including those set out in this Regulation.

Providers of intermediary services shall ensure that voluntary investigations are accompanied by appropriate safeguards, including, where necessary, human oversight, to ensure they are transparent, fair and non-discriminatory.

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 orders 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 ***mechanisms*** 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***;***

   (ca) compliance with the measures in the order is technically feasible taking into account the available technical capabilities of the service provider concerned.

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.

4. The conditions and requirements laid down in this article shall be without prejudice to requirements under national criminal procedural law in conformity with Union law.

4a. The orders to act against illegal content may require providers of intermediary services to take steps, in the specific case, to remove identical or equivalent illegal content.

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 of issuing the order of its receipt and the effect given to the order.

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 and proportionate to determine compliance by the recipients of the intermediary services with applicable Union or national rules, unless such a statement cannot be provided for reasons related to the prevention, investigation, detection and prosecution of criminal offences;

      – 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.

4. The conditions and requirements laid down in this article shall be without prejudice to requirements under national criminal procedural law in conformity with Union law.

CA 3: Chapter III - Due diligence obligations for a transparent and safe online environment
Section 1
Provisions applicable to all providers of intermediary services

=> Covers AMs EPP 9, EPP 26, EPP 27, EPP 28, EPP 29, Left 124, EPP 125, ECR 126, S&D 128, ECR 129, Left 279, EPP 283, S&D 287, S&D 288, Greens 289, S&D 290, S&D 291, Greens 296, Greens 297, Greens 302, Renew 314, EPP 315, Renew 316

(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***, effective*** and balanced set of harmonised due diligence obligations for providers of intermediary services. Those obligations should aim in particular to ***reinforce and*** guarantee different ***legislation and rights,*** ~~public policy objectives~~ such as the safety and trust of the recipients of the service, including minors ~~and vulnerable users~~, 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 ***and by users of services*** 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. ***Nothing in this Regulation prohibits providers of intermediary services from establishing collective representation or obtaining the services of a legal representative by other means, including contractual ones, provided that the legal representative can fulfil the role assigned to it by this Regulation. Providers of intermediary services that qualify as micro, small or medium-sized enterprises within the meaning of the Annex to Recommendation 2003/361/EC, and who have been***

unsuccessful in obtaining the services of a legal representative after reasonable effort, should be able to request that the Digital Services Coordinator of the Member State where the enterprise intends to establish a legal representative facilitates further cooperation and recommends possible solutions, including possibilities for collective representation.

(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.[1]

[1] 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).

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.

3a. Any requests to providers of intermediary services, made on the basis of this legislation, shall be transmitted through the Digital Service Coordinator in the Member State of establishment, who is responsible for collecting requests and communication from all relevant sources.

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.

5a. Providers of intermediary services that qualify as micro, small or medium-sized enterprises (SMEs) within the meaning of the Annex to Recommendation 2003/361/EC, and who have been unsuccessful in obtaining the services of a legal representative after reasonable effort, shall be able to request that the Digital Services Coordinator of the Member State where the enterprise intends to establish a legal representative facilitates further cooperation and recommends possible solutions, including possibilities for collective representation.

Article 12
Terms and conditions

1. Providers of intermediary services shall include information on ***the activities undertaken by them and*** 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 ***transparent, non-discriminatory, coherent, predictable,*** diligent, ***non-arbitrary*** ~~objective~~***, necessary*** and proportionate manner in applying and enforcing the ***terms and conditions*** ~~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.

2a. Those parts of the terms and conditions that do not comply with this Article shall not be binding on recipients of the services. Providers of intermediary services shall inform recipients of their services of all changes in terms and conditions in advance.

2b. Where very large online platforms within the meaning of Article 25 of this Regulation otherwise allow for the dissemination to the public of press publications within the meaning of Article 2(4) of Directive (EU) 2019/790, such platforms shall not remove, disable access to, suspend or otherwise interfere with such content or the related service or suspend or terminate the related account on the basis of the alleged incompatibility of such content with its terms and conditions.

2c. Any restrictions that providers of intermediary services may impose in relation to the use of their service and the information provided by the recipients of the service shall be in full compliance with the fundamental rights of the recipients of the services 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. ***Where possible, the information published shall be***

broken down per Member State in which services are offered. Those reports shall include, in particular, information on the following, as applicable:

(a) the number of orders received from Member States' authorities, categorised***, where possible,*** 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, ***the number of notices submitted by trusted flaggers***, any action taken pursuant to the notices by differentiating whether the action was taken on the basis of the law or the terms and conditions of the provider~~, 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~~***, as well as measures taken to train content moderators and the safeguards put in place to ensure that non-infringing content is not affected***;

(d) the number of complaints received through the internal complaint-handling system referred to in Article 17, ***where identifiable,*** 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 ***content moderation*** ~~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.

CA 4: Chapter III - Due diligence obligations for a transparent and safe online environment **Section 2** **Additional provisions applicable to providers of hosting services, including online platforms**
=> Covers AMs EPP 31, EPP 33, EPP, 34, EPP 35, EPP 36, EPP 40, EPP 41, S&D 131, Greens 138, EPP 139, Left 318, EPP 319, EPP 329, S&D 330, Greens 331, Greens 335, Greens 336, Greens 337, ID 340, Greens 342, Left 347, EPP 348, Left 351, EPP 352, Greens 353, EPP 358, EPP 360, EPP 362, ECR 363

(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 ***easy to access and*** user-friendly notice and action mechanisms that facilitate the notification of specific items of information that the notifying party considers to be illegal content to the provider of hosting services concerned ('~~notice~~ ***notification***'), pursuant to which that provider ***should assess the illegality of the identified content and, on the basis of that assessment,*** can decide whether or not it agrees with ~~that~~ ***the notification of illegal content*** ~~assessment~~ and wishes to remove or disable access to that content ('action'). ***In the event that provider of hosting services assesses the notice of illegal content to be positive and thus decides to remove or disable access to it, it shall ensure that such content remains inaccessible after take down.*** 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 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. ***While an absolute hierarchy between these rights does not exist, freedom of expression should be recognized as cornerstone of a democratic society***

(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.

(42a) Providers of hosting services should not be subject to the obligation to provide a statement of reasons when doing so would cause unintended safety concerns for the recipient of the service. Specifically in cases of one-to-one interface platforms, such as dating applications and other similar services, providing a statement of reasons should be considered as likely to cause unintended safety concerns for the reporting party. As a result of this, these services should by default refrain from providing statements of reasons. Additionally, other providers of hosting services should make reasonable efforts to assess if providing a statement of reasons could cause unintended safety concerns to the reporting party and, in such cases, refrain from providing a statement of reasons.

(42b) The service provider should ensure that staff that takes decision on or is otherwise frequently subjected to illegal content receives adequate training as well as appropriate working conditions, including, where necessary, the opportunity to seek professional support and qualified psychological assistance.

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 ***at scale and*** exclusively by electronic means. ***Those mechanisms may not replace a decision of an independent judicial and administrative authority as to whether content is illegal or not.***

2. The ~~mechanisms~~ ***notifications*** 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 ***and assess*** 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 ***identification*** ~~location~~ of that information, ***such as*** the ~~exact~~ URL or URLs ***where possible***, 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***, to the best of their knowledge,*** accurate and complete.

3. Notices that include the elements referred to in paragraph 2 ***and are thus sufficiently precise and adequately substantiated, and on the basis of which a diligent provider of hosting services can identify the illegality of the specific content,*** shall be considered to give rise to actual knowledge or awareness for the purposes of Article 5 in respect of the specific item of information concerned.

4. Where the ***notification*** 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 ***notification*** to that individual or entity.

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

6. Providers of hosting services shall***, where the information provided is sufficiently clear, act on any notifications*** ~~process any notices~~ that they receive under the mechanisms referred to in paragraph 1, ***taking into account their technical and operational ability to act against specific items of illegal content,*** and take their decisions in respect of the information to which the ***notifications*** relate, in a timely, diligent and ~~objective~~ ***non-arbitrary*** 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.

6a. ***Paragraphs 4 and 5 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. In addition, paragraph 4 and 5 shall not apply to enterprises that previously qualified for the status of a micro or small enterprise within the meaning of the Annex to Recommendation 2003/361/EC during the twelve months following their loss of that status pursuant to Article 4(2) thereof.***

Article 15
Statement of reasons

1. Where a provider of hosting services decides ***or not*** to remove or disable access to***, or otherwise moderate either the form or distribution of,*** 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, ***without undue delay and*** at the latest ***within 24 hours after such removal*** ~~at the time of the removal~~ or disabling of access ***or other content moderation and content curation measure,*** 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 ***used*** 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.~~

4a. Providers of hosting services shall not be obliged to provide a statement of reasons referred to in paragraph 1 where the statement of reasons could cause unintended safety concerns for the reporting party. In addition, providers of hosting services shall not be obliged to provide a statement of reasons referred to in paragraph 1 where the provider can demonstrate that the recipient of the service has repeatedly provided illegal content.

4b. Paragraphs 2 and 3 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. In addition, those paragraphs shall not apply to enterprises that previously qualified for the status of a micro or small enterprise within the meaning of the Annex to Recommendation 2003/361/EC during the twelve months following their loss of that status pursuant to Article 4(2) thereof.

Article 15a

Protection against repeated misuse and criminal offences

1. Providers of intermediary services shall, after having issued a prior warning, suspend or, in appropriate circumstances, terminate the provision of their services to recipients of the service that frequently provide illegal content after having provided a comprehensive explanation,

2. Where a provider of intermediary services 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. Where the provider of intermediary services cannot identify with reasonable certainty the Member State concerned, it shall inform the law enforcement authorities of the Member State in which it has its main establishment or legal representative, and shall also transmit this information to Europol for appropriate follow-up.

Article 15b

Market entrance protection

The provisions in this Section shall not be enforced against micro or small enterprises within the meaning of the Annex to Recommendation 2003/361/EC for a period of one year after their establishment. During this period, such enterprises shall make all reasonable efforts to comply with the provisions in this section and shall act in good faith.

CA 5: Chapter III - Due diligence obligations for a transparent and safe online environment
Section 3
Additional provisions applicable to online platforms

=> Covers AMs EPP 11, EPP 12, EPP 14, EPP 45, EPP 47, EPP 48, EPP 49, EPP 50, EPP 51, EPP 53, EPP 54, EPP 55, EPP 56, EPP 57, EPP 60, S&D 144, EPP 151, S&D 153, EPP 155, Greens 166, Greens 167, S&D 168, ECR 170, Greens 374, Greens 378, S&D 379, S&D 380, S&D 381, S&D 382, Greens 383, Left 387, EPP 388, Greens 390, EPP 391, Greens 393, S&D 394, S&D 403, Left 406, S&D 409, Greens 413, EPP 417, Greens 420, EPP 422, S&D 426, EPP 427, S&D 429, EPP 430, EPP 434, EPP 437, Greens 466, EPP 478, S&D 479, Left 483, Left 484, S&D 485, S&D 487, S&D 489, Greens 493, S&D 494

(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,[1] 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.

(43a) The additional obligations imposed on online platforms under this Regulation should not apply to not-for-profit scientific or educational repositories or to online platforms offering products and services from third-party traders, which are established in the European Union, where these traders' access is exclusive, curated and entirely controlled by the providers of the online platform and these traders' products and services are reviewed and pre-approved by the providers of the online platform before they are offered on the platform.

(43b) To avoid unnecessary regulatory burden, certain obligations should not apply to online marketplaces offering products and services from third-party traders, which are established in the European Union, where these traders' access is exclusive, curated and entirely controlled by the providers of the online marketplace and these traders' products and services are reviewed and pre-approved by the providers of the online marketplace before they are offered on the marketplace. These online platforms are often referred to as closed online platforms. As the products and services offered are reviewed and pre-approved by the online platforms, the prevalence of illegal content and products on these platforms is low, and these platforms cannot, in most cases, benefit from relevant liability exemptions outlined in this Regulation. These online platforms should subsequently not be subjected to the obligations that are necessary for platforms with different operational models where the prevalence of illegal content is more frequent and the relevant liability exemptions are available.

(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

[1] 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).

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, ***including on the freedom of expression,*** to carry out their activities in a fair and ~~swift and~~ cost-effective manner ***and within a reasonable period of time***. 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.

(44a) If an out-of-court dispute settlement body decides the dispute in favour of the recipient of the service, the online platform should 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 should not be required to reimburse fees or other expenses that the online platform paid or is to pay in relation to the dispute settlement, unless the body finds the complaint manifestly unfounded and abusive.

(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[2] 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.

(46) Action against illegal content can be taken more quickly and reliably where online platforms***, having received guidance from public authorities on how to identify illegal content,*** 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 ***and are known to flag content frequently with a high rate of accuracy***, that they represent collective interests and that they work in a diligent, ***effective*** 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 ***representing collective interests*** and of right-holders ***specifically created for that purpose*** could be awarded trusted flagger status, where they have demonstrated that they meet the applicable conditions, ***ensure independent collective interest representation and that their assessment of what constitutes an IPR infringement is***

[2] 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).

unbiased and consistent. 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.[43]

(47) The misuse of services of online platforms by frequently providing ***or disseminating*** ~~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. This is without prejudice to the freedom by online platforms to determine their terms and conditions and establish stricter measures in the case of ~~manifestly~~ illegal content related to serious crimes. For reasons of transparency, this possibility should be set out, clearly and in ***sufficient*** detail, in the terms and conditions of the online platforms. Redress should always be open to the decisions taken in this regard by 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 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[3]. 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 ***and other users***, as well as for other interested parties such as competing

[3] 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).

traders and holders of intellectual property rights, and to deter traders from selling ***and dissemination of*** products or services in violation of the applicable rules, online ***marketplaces*** should ensure that such traders are traceable. The trader should therefore be required to provide certain essential information to the ***provider of the online marketplace***, 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 ***marketplaces*** 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. ***Occasional traders who are natural persons should not be subject to disproportionate identification requirements on online marketplaces. Providers of the online marketplace***s ***should not ask for information from natural persons that goes beyond the mere registration of the marketplace users.***

(50) To ensure an efficient and adequate application of that obligation, without imposing any disproportionate burdens, the ***providers of*** online ***marketplaces*** 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[45] , 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 ***providers of*** online ***marketplaces*** should not be required to engage in excessive or costly online fact-finding exercises or to carry out verifications on the spot, ***as this would be disproportionate***. Nor should such ***providers of online marketplaces***, 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 ***or be liable for this information in case it proves to be inaccurate***. ***Providers of*** online ***marketplaces*** should also design and organise their online interface in a ***user-friendly*** way that enables traders to comply with their obligations under Union law, in particular the requirements set out in Articles 6 and 8 of Directive 2011/83/EU of the European Parliament and of the Council[46] , Article 7 of Directive 2005/29/EC of the European Parliament and of the Council[47] and Article 3 of Directive 98/6/EC of the European Parliament and of the Council[48] . ***The online interface should allow traders to provide the information allowing for the unequivocal identification of the product or the service, including labelling requirements, in compliance with legislation on product safety and product compliance.***

(50 a) Without prejudice to relevant exemptions for micro and small enterprises, and to strengthen the obligations of online marketplaces, further ex-ante provisions should be put in place, so as to ensure ex-ante that consumers have the necessary information for product offers, prevent unsafe and non-compliant products and product categories, strengthen ex-ante actions against product counterfeiting as well as to cooperate (ex post) where necessary with regard to dangerous products already sold. Providers of online marketplaces should inform recipients of their service when the service or product they have acquires through their services is illegal. Once they

have taken a decision to remove an illegal offering from their service, the providers of online marketplaces should take measures to prevent such illegal offerings, as well as identical or equivalent offerings, from being reuploaded on their marketplace.

(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 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***, in standardised formats and through standardised Application Programming Interfaces***.

(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~~ ***that can have*** an impact ***both*** on the equal treatment and opportunities of citizens ***and on the perpetuation of harmful stereotypes and norms. New advertising models have generated changes in the way information is presented and have created new personal data collection patterns and business models that might negatively affect privacy, personal autonomy, democracy, quality news reporting and facilitate manipulation and discrimination. Therefore, more transparency in online advertising markets and independent research needs to be carried out to assess the effectiveness of behavioural advertisements.*** In addition to the requirements resulting from Article 6 of Directive 2000/31/EC, online platforms should therefore be required to ensure ***that data collection is kept to a minimum, the maximisation of revenue from advertising does not limit the quality of the service and*** that the recipients of the service have ***extensive*** ~~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 in particular those regarding the storage of information in terminal equipment and the access to information stored therein.

(52 a) 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.

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***, unless they meet the criteria to qualify as very large online platforms under this Regulation***. ***This Section shall not apply to enterprises that previously qualified for the status of a micro or small enterprise within the meaning of the Annex to Recommendation 2003/361/EC during the twelve months following their loss of that status pursuant to Article 4(2) thereof, unless they meet the criteria to qualify as very large online platforms under this Regulation.***

Article 17
Internal complaint-handling system

1. Online platforms shall provide recipients of the service ***and qualified entities within the meaning of Article 3(4) of Directive (EU) 2020/1828***, 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***, demote, demonetise or restrict*** access to the information ***or otherwise impose sanctions against it***;

   (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 ***and include human review.***

3. Online platforms shall handle complaints submitted through their internal complaint-handling system in a timely, diligent and ***non-arbitrary*** ~~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. ***If the complaining entity so requests, the online platform shall publicly confirm the reversal of the decision.***

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. ***Such delay shall not exceed three weeks from the lodging of the complaint.***

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. ***After internal complaint handling mechanisms are exhausted,*** recipients of the service addressed by the decisions referred to in Article 17(1) ***and qualified entities within the meaning of Article 3(4) of Directive (EU) 2020/1828*** shall be entitled to select any out-of-court dispute ***settlement body*** 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 ***by the recipient*** 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 ***legal*** 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) ***it offers*** ~~the~~ dispute settlement ***that*** is easily accessible through electronic communication technology;

   (d) it is capable of settling dispute in a swift, efficient***, transparent*** and cost-effective manner and in at least one official language of the Union;

   (e) ***it offers*** ~~the~~ dispute settlement ***that*** takes place in accordance with clear and fair rules of procedure ***and sufficient confidentiality safeguards***;

   (e a) where applicable, particular legal expertise in relation to the applicable laws relating to freedom of expression and its limitations and the applicable case law, including the case law of the European Court of Human Rights.

   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, ***unless the body finds the complaint manifestly unfounded and abusive***.

   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. ***Any attempt to reach an out-of-court agreement on the settlement of a dispute in accordance with this Article shall not affect the rights of the providers of online platform services and of the recipients of the service concerned to initiate judicial proceedings at any time before, during or after the out-of-court dispute settlement process.***

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 with priority and without delay. ***Similar priority may be given to other notices, when the trustworthiness of those submitting them and the severity and urgency of the situations concerned is considered to be exceptional***.

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 ***demonstrated*** particular expertise ~~and competence~~***, accuracy and expertise*** for the purposes of detecting, identifying and notifying illegal content;

(b) it represents collective interest and is independent from any online platform;

(c) it carries out its activities for the purposes of submitting notices in ~~a timely, diligent and~~ ***an*** objective manner.'

(c a) where applicable, it has particular legal expertise in relation to the applicable laws relating to freedom of expression and its limitations and the applicable case law, including the case law of the European Court of Human Rights.

Digital Services Coordinator of the Member State may award the status of trusted flagger to an entity established in another Member State, if the said entity already holds the status of a trusted flagger in the Member State where it is established.

Where several Member States have awarded such status to the same entity, the entity may be referred to as European trusted flagger.

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. ***The Digital Services Coordinator of the Member State of establishment of the platform shall engage in dialogue with platforms and stakeholders for maintaining the accuracy and efficacy of a trusted flagger system.***

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 ***or notices regarding legal content*** 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.

7a. Online platforms shall, where possible, provide trusted flaggers with access to technical means that help them detect illegal content on a large scale.

Article 20
Measures and protection against misuse

1. Online platforms shall suspend, for a reasonably period of time, ***or in appropriate circumstances terminate,*** after having issued a prior warning ***and having provided a comprehensive explanation***, the provision of their services to recipients of the service that frequently provide manifestly illegal content. ***A termination of the service can be issued in case the recipients fail to comply with the applicable provisions set out in this Regulation or in case the suspension has occurred at least three times following verification of the repeated provision of 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) ***where identifiable,*** 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***, and the circumstances in which they will terminate their services***.

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 ***has its main establishment*** ~~established~~ or legal representative ~~inform~~ ***and also transmit this information to*** Europol ***for appropriate follow-up***.

   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. ***Providers of online marketplaces*** 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 ***their*** services, online ***marketplaces have*** obtained the following information ***from the trader***:

   (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[4];

~~(c) the bank account details of the trader, where the trader is a natural person;~~

(d) ***to the extent the contract relates to products that are subject to the Union Regulations listed in Article 4(5) of Regulation (EU) 2019/1020 of the European Parliament and the Council,*** the name, address, telephone number and electronic mail address of the economic operator, ***established in the Union, referred to in*** Article ***4(1)*** of Regulation (EU) 2019/1020 of the European Parliament and the Council 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 provider of*** the online ***marketplace*** shall, upon receiving that information, ***take effective steps that would reasonably be taken by a diligent operator in accordance with a high industry standard of professional diligence*** to assess whether the information referred to in points (a), (d) and (e) of paragraph 1 is ***accurate, current and*** reliable through the use of ***independent and reliable sources including*** any freely accessible official online database or online interface made available by an ***an authorized administrator,*** Member States or the Union or through requests to the trader to provide supporting documents from reliable sources.

3. Where ***the provider of*** the online ***marketplace*** obtains indications that any item of information referred to in paragraph 1 obtained from the trader concerned is inaccurate or incomplete, that ***marketplace*** 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.

3a. The provider of online marketplace shall require that traders promptly inform them of any changes to the information referred to in paragraph 1 and, in such cases, repeat the relevant steps referred to in paragraph 2. Where the provider of the online marketplace obtains indication that an item of information referred to in Article 22 is inaccurate, the provider of the online marketplace shall request the trader to provide evidence of the accuracy of that item of information or to correct it without delay. Where the trader fails to ***provide evidence of accuracy,*** 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 provider of*** the online ***marketplace*** 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 ***including the period for redress***. They shall subsequently delete the information.

5. Without prejudice to paragraph 2, the ***provider of the online marketplace*** shall only disclose the information to third parties where so required in accordance with the

[4] 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

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 provider of*** the online ***marketplace*** 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.

7. ***The provider of*** the online ***marketplace*** shall design and organise its online interface in a ***fair and user-friendly*** way that enables traders to comply with their obligations regarding pre-contractual information and product safety information under applicable Union law.

7 a. The provider of the online marketplace shall design its service in a way that allows traders to communicate to their customers all relevant information for the identification of the product or the service, and, where applicable, the information concerning labelling, including CE marking.

7 b. The online platforms shall ensure that traders are approved without undue delay once the online platform has received the information referred to in paragraph 1 and taken the steps referred to in paragraph 2.

Article 22a
Additional provisions for online marketplaces related to illegal offers

1. Where a provider of the online marketplace becomes aware of the illegal nature of a product or service offered through its services, it shall inform those recipients of the service that had acquired such product or contracted such service.

2. The provider of the online marketplace shall suspend without undue delay the provision of its services to traders that provide, in a repeated manner, illegal offers for a product or a service. It shall immediately notify its decision to the trader.

3. For products, categories or groups of products, which are susceptible to bear a serious risk to health and safety of consumers, based on accidents registered in the Safety Business Gateway, the Safety Gate statistics, the results of the joint activities on product safety and other relevant indicators or evidence, as outlined in the Regulation (EU) […/…] on general product safety, amending Regulation (EU) No 1025/2012 and repealing Directive 87/357/EEC and Directive 2001/95/EC, the provider of the online marketplace shall verify, with regard to the information referred to in paragraph 7a of Article 22, and before the trader's offer is made available on the online marketplace, if the offer that the trader wishes to propose to consumers located in the Union is mentioned in the list, or the lists, of products or categories of products identifies as non-compliant, as classified in any freely accessible official online database or online interface, and shall not authorise the trade to provide the offer if that the product is on such list.

4. The provider of the online marketplace shall ensure that content identified as illegal remain inaccessible after take down, and take steps, in the specific case, to remove identical or equivalent illegal content.

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;

   (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 ***requirements***

1. 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***, meaningful*** and unambiguous manner ***and at all times***:

(a) that the information displayed ***or parts thereof*** is an advertisement;

(b) the natural or legal person on whose behalf the advertisement is displayed;

(ba) the natural or legal person who finances the advertisement, if different from the natural or legal person identified pursuant to point (b);

(c) ***clear,*** meaningful information about the main parameters used to determine the recipient to whom the advertisement is displayed***, and how to change those parameters***.

(c a) whether the advertisement was selected using an automated system and, in that case, the identity of the natural or legal person responsible for the system.

2. Online platforms shall offer users the possibility to easily opt-out from micro-targeted tracking and advertisements that are based on their behaviour data or other

profiling techniques, within the meaning of Article 4(4) of Regulation (EU) 2016/679.

CA 6: Chapter III - Due diligence obligations for a transparent and safe online environment
Section 4
Additional obligations for very large online platforms to manage systemic risks

=> Covers AMs EPP 16, EPP 64, EPP 65, EPP 67, EPP 69, EPP 70, EPP 71, Greens 174, Left 177, Greens 178, Renew 181, Greens 184, EPP 185, Renew 525, Left 531, EPP 534, S&D 535, Left 538, Renew 540, S&D 552, Greens 556, Left 558, S&D 564, Greens 567, Left 574, Greens 575, Left 580, EPP 582, EPP 584, EPP 587, EPP 588, Left 589, EPP 591, S&D 599, S&D 604, EPP 616, S&D 618, S&D 619, EPP 620, S&D 627, Left 628, S&D 634, Renew 641

(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 ***challenges to fundamental rights*** ~~public policy concerns~~, there being no alternative and less restrictive measures that would effectively achieve the same result. ***Only in very exceptional cases, user should be permanently denied access to a very large online platform. The decision to permanently deny access should always be able to be revoked by a competent court.***

(54) Very large online platforms may cause societal risks, different in scope and impact from those caused by smaller platforms. Once the number of recipients 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. Such significant reach should be considered to exist where the number of recipients exceeds an operational threshold set at 45 million, that is, a number equivalent to 10% of the Union population. The operational threshold should be kept up to date through amendments enacted by delegated acts, where necessary. Such very large online platforms should therefore bear the highest standard of due diligence obligations, proportionate to their societal impact and means. ***In certain cases, online platforms whose number of recipients does not exceed the operational threshold set at 10% of the Union population may also be considered very large online platforms due to their turnover, role in facilitating public debate, economic transactions and the dissemination of information, opinions and ideas and in influencing how recipients obtain and communicate information online.***

(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~~ ***were able to*** 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 ***to address in particular filtering bubbles and effects***.

(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 ***and illegally-traded animals***. 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 health, civic discourse, electoral processes, public security and protection of minors, having regard to the need to safeguard public order, protect privacy and fight fraudulent and deceptive commercial practices. 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, in the interest of safeguarding public order, protecting privacy and fighting fraudulent and deceptive

commercial practices, 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 ***external*** auditing, for their compliance with the obligations laid down by this Regulation and, where relevant, any complementary commitments undertaking 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. ***As an indication of independence, at the time of the performance of the audit, auditors should not have provided services, other than auditing services, to the very large online platform over the course of the previous 12 months.*** 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***, without prejudice to the platform remaining solely responsible for its compliance with this Regulation and its freedom to conduct a business and, in particular, its ability to design and implement effective measures that are aligned with its specific business model***. 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. ***A disclaimer should be added to an opinion where the auditor does not have enough information to conclude the opinion due to the novelty of the issues audited.***

(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 ***on the use of recommender systems, and that recipients can easily control the way*** information presented to them. They should clearly ***and separately*** present the main parameters for such recommender systems in ***a clear, concise, accessible and*** 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. ***Very large online platforms should ensure that their online interface is designed in such a way that it does not risk misleading or manipulating the recipients of the service.***

~~(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.~~

(63 a) By associating advertisement with content uploaded by users, very large online platform could indirectly lead to the promotion of illegal content, or content that is in breach of their terms and condition and could risk to considerably damage to the buyers of advertising space. In order to prevent such practice, very large online platforms should take steps, including through contractual guarantees to the purchasers of advertising space, to ensure that the content to which they associate advertisements is legal and compliant with their terms and conditions. These steps could include independent audits entailing a quantitative and qualitative assessment of cases where advertising is associated with illegal content or with content incompatible with platforms' terms and conditions.

(63b) Very large online platforms should use their best efforts not to permit behavioural and micro-targeted advertising towards children below 18, in accordance with the General Data Protection Regulation.

(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 ***information or*** 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 provide information and access to data*** to vetted researchers. All requirements ***for providing information and*** 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. ***Research conducted under this regime should, where possible, be built on open access principles and use standardised data sets to ensure high level of transparency and accountability on proper use of provided data.***

(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.

(65a) Interoperability with very large online platforms is desirable as it can create new opportunities for the development of innovative services, overcome the lock-in effect and ensure competition and user choice. These possibilities could allow recipients to benefit from cross-platform interaction. Very large online platforms may provide an application programming interface through which third-party platforms and their recipients can interoperate with the main functionalities and recipients of the core services offered by the platform. Among the main functionalities may be the ability to receive information from certain accounts, to share provided content and react to it. Additionally, very large online platforms may make the core functionalities of their services interoperable with other online platforms to enable cross-platform communication. This possibility should not limit, hinder or delay the very large online platform's ability to solve security issues and should be in compliance with all their responsibilities, especially regarding fundamental rights and protection of privacy. The Commission should request European standardisation bodies to develop the necessary technical standards for interoperability, such as protocol on interoperability and data interoperability and portability.

(65b) Very large online platforms should ensure the portability of reviews to the reputation system of another platform operator upon the termination of the platform-user contract. For the sake of transparency, information about the processes, technical requirements, timeframes and charges that apply in case a platform user wants to transfer reviews to the reputation system of another platform operator should be provided beforehand. When displaying reviews imported from another platform, the receiving platform operator should indicate the origin of such reviews, where possible.

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, ***or where the platform has been designated as a very large online platform in accordance with paragraph 4a.***

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 or, after adjustment by means of a delegated act, of its population in the year in which the latest delegated act was adopted. 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 ***and whether the turnover, operating model and nature of platform constitutes a systemic risk***, 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***, as well as how to determine whether the turnover, operating model and size of platform constitutes a systemic risk***.

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.

4a. The Commission shall adopt delegated acts in accordance with Article 69 to designate online platforms, which provide ***their services to a number of average monthly active recipients of the service in the Union lower than 45 million but pose a very high systemic risk, as very large online platforms. The assessment of a systemic risk shall be based on following criteria:***

a) the annual turnover of the online platform, with EUR 50 million as a threshold that shall be exceeded for an online platform to qualify for further assessment based on points b) to d).

b) the role of the online platform as a public forum;

c) the role, nature and volume of economic transactions on the online platform;

d) the role of the online platform in disseminating information, opinions and ideas and in influencing how recipients of the service obtain and communicate information online; and

e) the depth and scope of the systemic risks stemming from the functioning and use made of the services of the online platform, as defined in Article 26, as well as the historical prevalence of illegal content on the service.

4b. 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. ***The risk assessment shall be broken down per Member State in which services are offered and in the Union as a whole.*** 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 fundamental ***rights, including the*** rights to respect for private and family life, freedom of expression and information, ***freedom and pluralism of the media,*** the prohibition of discrimination and the rights of the child, as enshrined in Articles 7, 11, 21 and 24 of the Charter***, as well as any other fundamental rights enshrined in the Charter that can be negatively affected by such risks now or in the future***;

   (c) intentional manipulation of their service, ~~including by means of inauthentic use or automated exploitation of the service,~~ with an actual or foreseeable ***systemic*** negative ***effects*** on the protection of public health, minors, civic discourse, or actual or foreseeable effects related to electoral processes and public security**,** ***including the risk of manipulation of their service by means of inauthentic use, deep fakes or automated exploitation of the service***.

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 ***cease, prevent and mitigate*** 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;

   (a a) ensuring appropriate staffing to deal with notices and complaints;

(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;

(e) initiating or adjusting cooperation with other online platforms 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 ***cease, prevent and*** mitigate the systemic risks identified.

3. The Commission, in cooperation with the Digital Services Coordinators, may issue general ***recommendations*** ~~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 ***recommendations*** guidelines the Commission shall organise public consultations.

3 a. The reports referred to in paragraph 2 shall be disseminated to the public and include standardised, open data describing the systemic risks, especially risks to fundamental rights.

Article 28
Independent audit

1. Very large online platforms shall be subject, at their own expense and at least once a year, to ***independent*** audits to assess compliance with the following:

(a) the obligations set out in Chapter III;

(b) any commitments undertaken pursuant to the codes of conduct referred to in Articles 35 and 36 and the crisis protocols referred to in Article 37.

2. Audits performed pursuant to paragraph 1 shall be performed by ***organisations or associations which have been constituted in accordance with the law of a Member State and*** ~~organisations~~ which:

(a) are independent from the very large online platform concerned ***and have not provided any service other than audits or relevant ancillary services to that platform in the previous 12 months***;

(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***;***

(ca) have not audited the very large online platform concerned for more than three consecutive years.

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 ***negative*** ~~not positive~~, ~~operational~~ recommendations on specific measures to achieve compliance ***and risk-based remediation timelines, with a focus on rectifying issues that have the potential to cause most harm to users of the service as a priority;***

(fa) where the organisation that performs the audit does not have enough information to conclude the audit opinion due to the novelty of the issues audited, a relevant disclaimer.

4. Very large online platforms receiving an audit report that ***contains evidence that the platform is not properly assessing or mitigating such risks systemic risks stemming from the functioning and use made of their services in the Union*** ~~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.

4a. Digital Services Coordinators shall provide very large online platforms under their jurisdiction with an annual audit plan outlining the key areas of focus for the upcoming audit cycle.

4b. The audits shall be submitted to Digital Services Coordinators, European Union Agency for Fundamental Rights and to the Commission. Summary of audit findings, not including sensitive information, shall be made public. Digital Services Coordinators, European Union Agency for Fundamental Rights and the Commission may provide a public comment on the audits.

Article 29
Recommender systems

1. ***Very large online platforms shall not make the recipients of their services subject to recommender system based on profiling, unless the recipient of the service has***

expressed a freely given, specific, informed and unambiguous consent. 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 ***technical*** parameters used in their recommender systems, ***and they shall provide*** options for the recipients of the service to modify or influence those main ***technical*** parameters that they ***shall make*** available, including at least one option which is not based on profiling, within the meaning of Article 4 (4) of Regulation (EU) 2016/679, ***and, where possible, keep a log of the significant changes implemented to the recommender system***.

2. Where several options are available pursuant to paragraph 1, very large online platforms shall provide an easily accessible ***and user-friendly*** 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.

2a. The parameters referred to in paragraph 1 shall include:

(a) whether the recommender system is an automated system and, in that case, the identity of the natural or legal person responsible for the recommender system, if different from the platform provider;

(b) clear information about the main criteria used by recommender systems;

(c) where possible, the relevance and weight of each main criteria which leads to the information recommended;

(b) the goals the system has been optimised for,

(d) if applicable, explanation of the role that the behaviour of the recipients of the service plays in how the relevant system produces its outputs.

Article 29 b
Portability of data and reviews

1. Very large online platforms shall provide effective portability of data generated through the activity of a business user or end user and shall, in particular, provide tools for end users to facilitate the exercise of data portability, in line with Regulation EU 2016/679, including by the provision of continuous and real-time access;

2. Very large online platforms shall ensure the portability of reviews to the reputation system of another platform operator upon the termination of the platform-user contract.

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;

(ba) the natural or legal person who finances the advertisement, if different from the natural or legal person identified pursuant to point (b);

(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, ***and whether other groups have been explicitly excluded.***

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, ***information and*** 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 ***information and*** access to data to vetted researchers, ***not-for-profit bodies, organisations or associations which have been constituted in accordance with the law of a Member State,*** who meet the requirements in paragraphs 4 of this Article***,*** for the sole purpose of ***facilitating and*** conducting research that contributes to the identification and understanding of systemic risks as set out in Article 26(1) ***and to enable verification of the effectiveness and proportionality of the mitigation measures as set out in Article 27(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. ***The period for which information and data is to be provided pursuant to paragraphs 1 and 2 shall be specified in the request. The data provided to vetted researchers shall be as disaggregated as possible, unless the researcher requests it otherwise.***

4. In order to be vetted, researchers shall be affiliated with academic institutions, ***be*** independent from commercial interests, ***disclose the funding financing the research,*** 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.

7 b. Upon completion of their research, the vetted researchers that have been granted access to data shall publish their findings without disclosing personal data.

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).

   (d a) relevant information on content moderation broken down per Member State in which the services are offered and in the Union as a whole

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. ***In such cases, the platform shall indicate that information was removed from the report, the scope of the information removed and the reason for the removal.***

CA 7: Chapter III - Due diligence obligations for a transparent and safe online environment
Section 5
other provisions concerning due diligence obligations

=> Covers AMs Greens 657, Greens 661

(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 conduct. In particular, risk mitigation measures concerning specific types of illegal content should be explored via self- and co-regulatory agreements. Another area for consideration is the possible negative impacts of systemic risks on society and democracy, such as disinformation or manipulative and abusive activities. This includes coordinated operations aimed at amplifying information, including disinformation, 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 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 rules on codes of conduct under this Regulation could serve as a basis for already established self-regulatory efforts at Union level, including the Product Safety Pledge, the Memorandum of Understanding against counterfeit goods, the Code of Conduct against illegal hate speech as well as the Code of practice on disinformation. In particular for the latter, the Commission will issue guidance for strengthening the Code of practice on disinformation as announced in the European Democracy Action Plan.

(70) 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. ***The codes should contain clear and precise consumer protection and human rights objectives and be governed in a transparent manner. The effectiveness of the codes of conduct should be regularly assessed.***

(71) 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 and other serious cross-border threats to public health, 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.

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***;***

   (ba) the different types of data that can be used.

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.

1a. The Commission shall be responsible for the drafting and scrutiny of the crisis protocols referred to in paragraph 1. It shall report annually thereon to the European Parliament.

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.

CA 8: Chapter IV - Implementation, cooperation, sanctions and enforcement
=> Covers AMs Left 205, Greens 207, Left 664, S&D 665, Left 666, ID 667, ECR 668, ID 670, S&D 671, ID 673, ECR 676, ECR 678, S&D 681, S&D 684, S&D 698, Left 699, S&D 704, S&D 705, S&D 706, ECR 707

(72) 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.

(73) 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.

(74) 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.

(75) 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.

(76) 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 Chapters III and IV 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.

(77) 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.

(78) 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.

(79) 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.

(80) 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.

(81) 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.

(82) Member States should ensure that Digital Services Coordinators can take measures that are effective in addressing and proportionate to certain particularly serious and persistent infringements. Especially where those measures can affect the rights and interests of third parties, as may be the case in particular where the access to online interfaces is restricted, it is appropriate to require that the measures be ordered by a competent judicial authority at the Digital Service Coordinators' request and are subject to additional safeguards. In particular, third parties potentially affected should be afforded the opportunity to be heard and such orders should only be issued when powers to take such measures as provided by other acts of Union law or by national law, for instance to protect collective interests of consumers, to ensure the prompt removal of web pages containing or disseminating child pornography, or to disable access to services are being used by a third party to infringe an intellectual property right, are not reasonably available.

(83) Such an order to restrict access should not go beyond what is necessary to achieve its objective. For that purpose, it should be temporary and be addressed in principle to a provider of intermediary services, such as the relevant hosting service provider, internet service provider or domain registry or registrar, which is in a reasonable position to achieve that objective without unduly restricting access to lawful information.

(84) 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.

(85) 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

(86) 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.

(87) 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, on a voluntary basis, the Commission to intervene and exercise its investigatory and enforcement powers under this Regulation.

(88) 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.

(89) 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.

(90) For that purpose, the Board should be able to adopt opinions, requests and recommendations addressed to Digital Services Coordinators or other competent national authorities. While not legally binding, the decision to deviate therefrom should be properly explained and could be taken into account by the Commission in assessing the compliance of the Member State concerned with this Regulation.

(91) 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.

(92) 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.

(93) 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.

(94) 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.

(95) 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 of one of the provisions that solely apply to very large online platforms 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. That Digital Services Coordinator should be able to ask, where appropriate, for an additional, specific audit to be carried out, on a voluntary basis, to establish whether those measures are sufficient to address the infringement. At the end of that procedure, it should inform the Board, the Commission and the platform concerned of its views on whether or not that platform addressed the infringement, specifying in particular the relevant conduct and its assessment of any measures taken. 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.

(96) Where the infringement of the provision that solely applies to very large online platforms is not effectively addressed by that platform pursuant to the action plan, only

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, to the exclusion of the Digital Services Coordinator of establishment. 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. It should also have such a possibility to intervene in cross-border situations where the Digital Services Coordinator of establishment did not take any measures despite the Commission's request, or in situations where the Digital Services Coordinator of establishment itself requested for the Commission to intervene, in respect of an infringement of any other provision of this Regulation committed by a very large online platform.

(97) The Commission should remain free to decide whether or not it wishes to intervene in any of the situations where it is empowered to do so under this Regulation. ***However, it should justify any inaction.*** Once the Commission initiated the proceedings, the Digital Services Coordinators of establishment concerned should be precluded from exercising their investigatory and enforcement powers in respect of the relevant conduct of the very large online platform concerned, so as to avoid duplication, inconsistencies and risks from the viewpoint of the principle of *ne bis in idem.* However, in the interest of effectiveness, those Digital Services Coordinators should not be precluded from exercising their powers either to assist the Commission, at its request in the performance of its supervisory tasks, or in respect of other conduct, including conduct by the same very large online platform that is suspected to constitute a new infringement. Those Digital Services Coordinators, as well as the Board and other Digital Services Coordinators where relevant, should provide the Commission with all necessary information and assistance to allow it to perform its tasks effectively, whilst conversely the Commission should keep them informed on the exercise of its powers as appropriate. 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.

(98) 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.

(99) 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 relevant persons, and to interview, with their consent, 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

(100) 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.

(101) 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.

Chapter IV
Implementation, cooperation, sanctions and enforcement

Section 1
Competent authorities and National Digital Services Coordinators

Article 38
Competent authorities and Digital Services Coordinators

1. Member States shall designate one or more competent authorities as responsible for the application and enforcement of this Regulation ('competent authorities').

   The competent authorities referred to it the first subparagraph shall have relevant expertise in the field of data protection, consumer protection or the regulation of user-generated content.

   Supervisory authorities designated under Regulation (EU) 2016/679 shall be tasked with the application and enforcement of measures related to data processing set out in this Regulation.

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~~ ***the*** 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 ***related to this Regulation*** 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***, including sharing information on cross-border cases and providing support for each other during ongoing interventions and investigations***.

   The Board shall create a publicly accessible list of all Digital Services Coordinators and competent authorities. It shall regularly update and monitor this list.

   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.

The Commission shall provide guidance to Member States to ensure a consistent approach on how national, local and regional authorities should relate to their Digital Services Coordinator.

The Commission shall publish and update a register containing the name and contact information of the Digital Service Coordinator responsible in each Member State.

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, ***independent,*** transparent and timely manner. Member States shall ensure that their Digital Services Coordinators have ~~adequate~~ ***all necessary*** technical, financial and human resources***, including skills and competence building, as well as infrastructure*** to carry out their tasks. ***Such resources may include access to training and regular exchanges with service providers to understand the specificities of their business model.***

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~~ ***not*** take instructions from any other public authority or any private party.

Digital Services Coordinators may seek information from a public authority or private party if it deems it necessary to carry out its duties, without compromising its independence and neutrality.

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 Chapters III and IV 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, for the purposes of Chapters III and IV, 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 for the purposes of Chapters III and IV. 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, 2 and 3 are without prejudice to the second subparagraph of Article 50(4) and the second subparagraph of Article 51(2) 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.

   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 others 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.

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

   (a) require the management body of the providers, within a reasonable time period, to examine the situation, adopt and submit an action plan setting out the necessary measures to terminate the infringement, ensure that the provider takes those measures, and report on the measures taken;

   (b) where the Digital Services Coordinator considers that the provider has not sufficiently complied with the requirements of the first indent, that the infringement persists and causes serious harm, and that the infringement entails a serious criminal offence involving a threat to the life or safety of persons, request the 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.

   The Digital Services Coordinator shall, except where it acts upon the Commission's request referred to in Article 65, prior to submitting the request referred to in point (b) of the first subparagraph, 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 provider, the intended addressee or addressees and any other third party demonstrating a legitimate interest shall be entitled to participate in the proceedings before the competent judicial authority. Any measure ordered shall be proportionate to the nature, gravity, recurrence and duration of the infringement, without unduly restricting access to lawful information by recipients of the service concerned.

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

   (a) the provider has failed to take the necessary measures to terminate the infringement;

   (b) the temporary restriction does not unduly restrict access to lawful information by recipients of the service, having regard to the number of recipients affected and whether any adequate and readily accessible alternatives exist.

   Where the Digital Services Coordinator considers that those two conditions have been met but it cannot further extend the period pursuant to the third subparagraph, it shall

submit a new request to the competent judicial authority, as referred to in point (b) of the first subparagraph.

4. The powers listed in paragraphs 1, 2 and 3 are without prejudice to Section 3.

5. The measures taken by the Digital Services Coordinators in the exercise of their powers listed in paragraphs 1, 2 and 3 shall be effective, dissuasive and proportionate, having regard, in particular, to the nature, gravity, recurrence and duration of the infringement or suspected infringement to which those measures relate, as well as the economic, technical and operational capacity of the provider of the intermediary services concerned where relevant.

6. Member States shall ensure that any exercise of the powers pursuant to paragraphs 1, 2 and 3 is subject to ***the highest*** safeguards laid down in the applicable national law, in ***absolute*** 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 ***global*** 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 ***global*** 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 ***global*** 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***, as well as other parties having a legitimate interest and being independent from any provider of intermediary 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.

   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.

2. 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***;***

   (ea) issue own-initiative opinions.

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 it has reasons to suspect that a very large online platform infringed 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 the first subparagraph of paragraph 1 to the very large online platform concerned, the Digital Services Coordinator of establishment shall request it to draw up and communicate to the Digital Services Coordinator of establishment, the Commission and the Board, within one month from that decision, an action plan, specifying how that platform intends to terminate or

remedy the infringement. 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.

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 to assess the effectiveness of those measures in terminating or remedying the infringement. In that case, that platform shall send the audit report to that Digital Services Coordinator, the Commission and the Board within four months from the decision referred to in the first subparagraph. 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 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 and the reasons thereof. It shall do so within the following time periods, as applicable:

(a) within one month from the receipt of the audit report referred to in the second subparagraph of paragraph 3, where such an audit was performed;

(b) within three months from the decision on the action plan referred to in the first subparagraph of paragraph 3, where no such audit was performed;

(c) immediately upon the expiry of the time period set out in paragraph 2, where that platform failed to communicate the action plan within that time period.

Pursuant to that communication, the Digital Services Coordinator of establishment 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.

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, may 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:

(a) 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, pursuant to the request of the Commission referred to in Article 45(7), upon the expiry of the time period set in that request;

(b) 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), upon the reception of that request;

(c) has been found to have infringed any of the provisions of Section 4 of Chapter III, upon the expiry of the relevant time period for the communication referred to in Article 50(4).

2. 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.

As regards points (a) and (b) of paragraph 1, pursuant to that notification, 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.

3. The Digital Services Coordinator referred to in Articles 45(7), 46(2) and 50(1), as applicable, shall, without undue delay upon being informed, transmit to the Commission:

(a) 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;

(b) the case file of that Digital Services Coordinator relating to the infringement or the suspected infringement, as applicable;

(c) any other information in the possession of that Digital Services Coordinator that may be relevant to the proceedings initiated by the Commission.

4. The Board, and the Digital Services Coordinators making the request referred to in Article 45(1), shall, without undue delay 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 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 where they have no legal personality, the persons authorised to represent them by law or by their constitution shall supply the information requested on behalf of the 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 the 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 the very large online platform concerned and declare that there are no further grounds for action.

2. The Commission may, upon request or on its own initiative, reopen the proceedings:

   (a) where there has been a material change in any of the facts on which the decision was based;

   (b) where the 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 the 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 ***global*** 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 ***global*** 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 nature, gravity, duration and recurrence of the infringement and, for fines imposed pursuant to paragraph 2, the 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 ***global*** 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***, along, where possible, with non-confidential documents or other forms of information on which the decision is based.***

2. The publication shall have regard to the rights and legitimate interests of the very large online platform concerned, 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, the infringement persists and causes serious harm which cannot be avoided through the exercise of other powers available under Union or national law, the Commission may request the Digital Services Coordinator of establishment of the very large online platform concerned to act pursuant to Article 41(3).

   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.

2. Where the coherent application of this Regulation so requires, the Commission, acting on its own initiative, may submit written observations to the competent judicial

authority referred to Article 41(3). With the permission of the judicial authority in question, it may also make oral observations.

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

Article 66
Implementing acts relating to Commission intervention

1. In relation to the Commission intervention covered by 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[1], 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;

---

1 [Reference]

(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.

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.

CA 9: Chapter V - Final provisions
=> Covers S&D 713, ECR 714, S&D 715, ID 716

(102) 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.

(103) 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[1].

(104) 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.

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

(106) 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,

[1] 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).

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, ***and pay specific attention to small and medium-sized enterprises (SMEs) and the position of new competitors.***

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].