Council of the European Union

Brussels, 10 February 2021
(OR. en)

6086/21

Interinstitutional File:
2020/0361(COD)

COMPET 89
MI 79
JAI 130
TELECOM 51
CT 11
PI 8
AUDIO 13
CONSOM 37
CODEC 177

COVER NOTE

From:	Mr Wojciech Rafal WIEWIOROWSKI, European Data Protection Supervisor
date of receipt:	10 February 2021
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
Subject:	Opinion of the European Data Protection Supervisor on the proposal for a Digital Services Act

Delegations will find attached the above document.

Encl.: Opinion 01/2021

EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
SUPERVISOR

H.E. Nuno BRITO
Permanent Representative of Portugal
to the European Union
Presidency of the Council of the
European Union

Mr Jeppe TRANHOLM-MIKKELSEN
Secretary General
Council of the European Union

1048 Brussels

Brussels, 10 February 2021
WRW/BVA/mt/D(2021)0283 **C2020-1195**
Please use edps@edps.europa.eu for all correspondence

Subject: **Opinion of the European Data Protection Supervisor on the proposal for Digital Services Act**

Your Excellency,
Mr Secretary-General,

Having regard to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC article 42(1), we send you an Opinion on the proposal for Digital Services Act.

We have sent this opinion to the President of the European Commission and the President of the European Parliament as well.

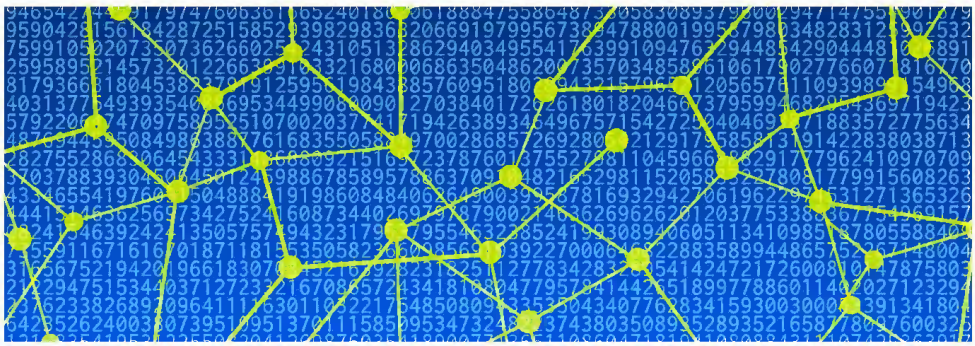
Yours sincerely,

Wojciech Rafał WIEWIÓROWSKI
(e-signed)

Encl.: Opinion

Cc: Mr Ralph KAESSNER, Secretariat General of the Council
Ms Ana RAMÍREZ FUEYO, Head of Unit, Internal Market, Consumer Protection and Intellectual Property
Mr Ilkka SAARILAHTI, Head of Unit, Competition, Industry, Research and Space

Contact persons: *Brendan Van Alsenoy (tel: 02 2831968), Mario Guglielmetti (tel: 02 2831925)*



EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 01/2021

on the Proposal for a Digital Services Act

EDPS

10 February 2021

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 52(2) of Regulation 2018/1725 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies', and under Article 52(3) '…for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data'.

Wojciech Wiewiorówski was appointed as Supervisor on 5 December 2019 for a term of five years.

Under article 42(1) of Regulation 2018/1725, the Commission shall 'following the adoption of proposals for a legislative act, of recommendations or of proposals to the Council pursuant to Article 218 TFEU or when preparing delegated acts or implementing acts, consult the EDPS where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data' and under article 57(1)(g), the EDPS shall 'advise on his or her own initiative or on request, all Union institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data'.

This Opinion is issued by the EDPS, within the period of eight weeks from the receipt of the request for consultation laid down under Article 42(3) of Regulation (EU) 2018/1725, having regard to the impact on the protection of individuals' rights and freedoms with regard to the processing of personal data of the Commission Proposal for a Regulation of the European Parliament and of the Council on Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC.

Executive Summary

On 15 December 2020, the Commission adopted a Proposal for a Regulation of the European Parliament and of the Council on Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC ("DSA").

The EDPS supports the Commission's aim to promote **a transparent and safe online environment**, by defining responsibilities and accountability for intermediary services, in particular online platforms such as social media and marketplaces.

The EDPS welcomes that the Proposal **seeks to complement rather than replace existing protections under Regulation (EU) 2016/679 and Directive 2002/58/EC**. That being said, the Proposal will clearly have an impact on processing of personal data. The EDPS considers it **necessary to ensure complementarity in the supervision and oversight** of online platforms and other providers of hosting services.

Certain activities in the context of online platforms present increasing risks not only for the rights of individuals, but for society as a whole. While the Proposal includes a set of risk mitigation measures, **additional safeguards** are warranted, in particular in relation to **content moderation, online advertising and recommender systems**.

Content moderation should take place in accordance with the **rule of law**. Given the already **endemic monitoring** of individuals' behaviour, particularly in the context of online platforms, the DSA should delineate when efforts to combat "illegal content" legitimise the use of automated means to detect, identify and address illegal content. Profiling for purposes of content moderation should be **prohibited** unless the provider can demonstrate that such measures are *strictly* necessary to address the systemic risks explicitly identified by the DSA.

Given the multitude of risks associated with **online targeted advertising**, the EDPS urges the co-legislators to consider **additional rules going beyond transparency**. Such measures should include **a phase-out leading to a prohibition of targeted advertising on the basis of pervasive tracking**, as well as **restrictions** in relation to the categories of data that can be processed for targeting purposes and the categories of data that may be disclosed to advertisers or third parties to enable or facilitate targeted advertising.

In accordance with the requirements of data protection by design and by default, **recommender systems** should by default not be based on profiling. Given their significant impact, the EDPS also recommends additional measures to **further promote transparency and user control** in relation to recommender systems.

More generally, the EDPS recommends introducing minimum **interoperability requirements** for very large online platforms and to promote the development of technical standards at European level, in accordance with the applicable Union legislation on European standardisation.

Having regard to the experience and developments related to the **Digital Clearinghouse**, the EDPS strongly recommends providing for an explicit and comprehensive legal basis for the **cooperation and exchange of relevant information** among supervisory authorities, each acting within their respective areas of competence. The Digital Services Act should ensure **institutionalised and structured cooperation** between the competent oversight authorities, including data protection authorities, consumer protection authorities and competition authorities.

TABLE OF CONTENTS

1. INTRODUCTION....5

2. GENERAL COMMENTS....6

3. SPECIFIC RECOMMENDATIONS....8

3.1. RELATIONSHIP TO REGULATION (EU) 2016/679 AND DIRECTIVE 2002/58/EC....8

3.2. "ILLEGAL CONTENT" AND NO GENERAL MONITORING OBLIGATIONS....8

3.3. INFORMATION ABOUT CONTENT MODERATION....9

3.4. NOTICE AND ACTION AND THE DUTY TO GIVE REASONS....11

3.5. COMPLAINT HANDLING....12

3.6. ADDITIONAL SAFEGUARDS FOR CONTENT MODERATION....12

3.7. NOTIFICATION OF SUSPICIONS OF CRIMINAL OFFENCES....14

3.8. ONLINE ADVERTISING TRANSPARENCY....15

3.9. RECOMMENDER SYSTEMS....16

3.10. ACCESS BY VETTED RESEARCHERS....17

3.11. PLATFORM INTEROPERABILITY....18

3.12. IMPLEMENTATION, COOPERATION, SANCTIONS AND ENFORCEMENT....19

4. CONCLUSIONS....20

Notes....25

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to 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)[1],

Having regard to Regulation (EC) No 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[2], and in particular Article 42(1) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

1. On 15 December 2020, the Commission adopted a Proposal for a Regulation of the European Parliament and of the Council on Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC[3].

2. The Proposal follows the Communication *Shaping Europe's Digital Future*, in which the Commission confirmed its intention to develop new and revised rules to deepen the Internal Market for Digital Services, by increasing and harmonising the responsibilities of online platforms and information service providers and reinforce the oversight over platforms' content policies in the EU[4].

3. According to the Explanatory Memorandum, new and innovative digital services have contributed deeply to societal and economic transformations in the Union and across the world. At the same time, the use of those services has also become the source of new risks and challenges, both for society as a whole and individuals using such services[5].

4. The aim of the Proposal is to ensure the best conditions for the provision of **innovative digital services** in the internal market, to contribute to **online safety** and the protection of **fundamental rights**, and to set a robust and durable **governance structure** for the effective supervision of providers of intermediary services[6]. To this end, the Proposal:
   - contains provisions on the exemption of liability of providers of intermediary services (Chapter II);
   - sets out "due diligence obligations", adapted to the type and nature of the intermediary service concerned (Chapter III); and
   - contains provisions concerning the implementation and enforcement of the proposed Regulation (Chapter IV).

5. The EDPS was consulted informally on the draft Proposal for a Digital Services Act on 27 November 2020. The EDPS welcomes the fact that he has been consulted at this early stage of the procedure.

6. In addition to the Proposal for a Digital Services Act, the Commission has also adopted a Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)[7]. In accordance with Article 42(1) of Regulation 2018/1725, the EDPS has also been consulted on the Proposal for a Digital Markets Act, which is the subject matter of a separate Opinion.

2. GENERAL COMMENTS

7. The EDPS recalls that the digital future of Europe is at the heart of the EDPS Strategy for 2020-2024, which aims to shape a safer, fairer and more sustainable digital Europe, particularly for the most vulnerable in our societies[8].

8. The EDPS supports the Commission's aim to promote a **transparent and safe online environment**, by defining responsibilities and accountability for intermediary services, in particular online platforms such as social media and marketplaces.

9. The EDPS welcomes the recognition that certain online activities, in particular in the context of online platforms, present increasing risks **not only for the fundamental rights of individuals, but for society as a whole**[9]. This is all the more evident for providers of very online large platforms and well reflected in the consideration that providers of very large platforms should bear the highest standard of due diligence obligations, proportionate to their societal impact[10].

10. In his Opinion on online manipulation and personal data, the EDPS identified several risks and harms resulting from **how personal data is used to determine the online experience**[11]. The Opinion also highlighted how the existing business models behind many online services has contributed to increased political and ideological **polarisation, disinformation and manipulation**. Similar risks have also been highlighted by the European Data Protection Board (EDPB) in its Guidelines on the targeting of social media users[12].

11. The EDPS welcomes the recognition that the **design of digital services** provided by very large online platforms is generally optimised to benefit their often **advertising-driven business models** and can **cause societal concerns**[13]. The Proposal also recognises the potential harms resulting from the use of **algorithmic systems**, in particular as regards their potential for **amplifying** certain content, including disinformation[14]. The EDPS considers both phenomena and harms are intrinsically linked to the so-called "**attention economy**", with services and applications being designed to maximise attention and engagement in order to gather more data on customers, to better target advertising and increase returns[15].

12. While the Proposal includes a set of risk mitigation measures, most provisions are designed to promote **transparency and accountability**, **without directly addressing the root cause** by way of *ex ante* rules. To be clear, the EDPS fully supports measures seeking to enhance transparency and accountability of platforms. At the same time, **additional measures are warranted** to properly address the systemic risks identified above, in particular in relation to very large online platforms. In this regard, the Proposal must be

seen also in light of the Proposal for a Digital Markets Act, which includes additional rules to promote fair and open markets and the fair processing of personal data[16]. The present Opinion will also recommend further measures in this regard, including in relation to online advertising.

13. The EDPS welcomes that the Proposal seeks to complement rather than replace existing protections under Regulation (EU) 2016/679 and Directive 2002/58/EC. For example, the measures concerning advertising on online platforms complement but do not amend existing rules on consent and the right to object to processing of personal data[17]. In doing so, the Proposal promotes **complementarity** (as opposed to interference) **with existing Union data protection legislation**. That being said, the EDPS also considers that certain provisions and possible measures **will clearly have an impact** on the processing of personal data and therefore it is necessary to ensure **complementarity in the supervision and oversight** of online platforms and other providers of hosting services.

14. The EDPS observes that the proposed obligations incumbent upon platforms may in practice **increase reliance upon platforms to safeguard public values**. Platforms are rightly to be held accountable for the societal harms resulting from activities under their control. It is also proper for platforms to take responsibility, for example, for content which promotes abuse of children and other vulnerable groups[18]. At the same time, appropriate safeguards should be included to ensure that measures to reduce harms are taken **in accordance with the rule of law** and do not disproportionality interfere with the rights and freedoms of others.

15. The EDPS recalls that the right to data protection is not **an absolute right** and interferences may be justified, provided such measures remain limited to what is necessary and proportionate. Moreover, there is **no inherent conflict** between the right to data protection and the objectives of the Proposal to ensure an innovative, transparent and safe online environment. **Data protection and privacy are an essential component of a vibrant digital economy, including online platforms**. Data protection and privacy are necessary for individuals to be able to express themselves freely, to access information freely and to be creative[19]. Online safety and mechanisms to ensure accountability of online platforms can further promote the effective enjoyment of fundamentals rights.

16. The remainder of this Opinion contains specific recommendation to ensure that the Proposal **complements Regulation (EU) 2016/679 effectively** and increases protection for the fundamental rights and freedoms of the individuals concerned.

3. SPECIFIC RECOMMENDATIONS

3.1. Relationship to Regulation (EU) 2016/679 and Directive 2002/58/EC

17. Article 1(5)(i) of the Proposal states that the Digital Services Act is "**without prejudice**" to the rules laid down by Union law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC. Recital (10) of the Proposal further clarifies that "*[t]he 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.*"

18. The EDPS **welcomes** that the Proposal does not seek to affect the application of existing EU laws governing the processing of personal data, including the tasks and powers of the supervisory authorities competent to monitor compliance with those instruments.

19. In the interest of legal certainty, however, the EDPS recommends **aligning** the wording of Article 1(5)(i) of the Proposal with the current wording of **Article 1(5) b) of Directive 2000/31/EC** (e-Commerce Directive)[20]. Doing so would help maintain consistency with existing case law of the Court of Justice of the European Union. In *La Quadrature du Net*, for example, the Court explicitly referred to Article 1(5) b) of the e-Commerce Directive to confirm that the e-Commerce Directive cannot, in any event, undermine the requirements under Directive 2002/58/EC and Regulation (EU) 2016/679[21].

20. As a far as the question of liability is concerned, the Proposal maintains the **liability rules for providers of intermediary services** set out in the e-Commerce Directive, while taking into account the clarifications provided by the case law of the Court of Justice of the European Union. Recital (17) states that "*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.*"[22] The EDPS recalls that Regulation (EU) 2016/679 contains specific rules that govern the liability of controllers and processors[23]. In the interest of legal certainty, the EDPS recommends to clarify that the Proposal does not apply to questions relating to information society services covered by Regulation (EU) 2016/679 and Directive 2002/58/EC, including the liability of controllers and processors.

3.2. "Illegal content" and no general monitoring obligations

21. Article 2(g) defines "illegal content" as "*any information, which, in itself or by its reference to an activity, [...] 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.*"

22. Recital (12) clarifies that the **concept of illegal content** should be **understood broadly** to cover information "relating to" illegal content, products, services and activities. Examples provided include illegal hate speech, terrorist content, unlawful discriminatory content, sharing of images depicting child sexual abuse, unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit products, the non-authorised use of copyright protected material or activities involving infringements of consumer protection law. Recital (12) also indicates that national law defining the illegality should be "consistent with Union law". In the interest of legal certainty, the EDPS recommends to make reference to Article 52 of the Charter of Fundamental Rights of the

EU, which sets out the conditions for any limitations on the exercise of the rights and freedoms recognised by the Charter.

23. The EDPS notes that the Proposal **does not impose a general monitoring obligation or active fact-finding obligation**, or a general obligation for providers to take proactive measures to relation to illegal content[24]. Article 7 in fact **prohibits** the imposition of such obligations, without prejudice to possible orders to act against specific items of illegal content issued by relevant national or judicial authorities in accordance with Article 8.

24. The Proposal does, however, **seek to eliminate existing disincentives towards voluntary own-initiative investigations** undertaken by providers of intermediary services (Article 6)[25]. Moreover, several provisions make clear that in practice efforts to identify, detect or remove illegal content can involve processing of personal data, in particular where they make use of automated means.

25. The EDPS stresses that not all forms of content moderation require attribution to a specific data subject. In accordance with the requirements of **data minimisation and data protection by design and by default**, content moderation should, insofar as possible, not involve any processing of personal data. The EDPS encourages the co-legislature to include a recital to this effect. Where processing of personal data is necessary, such as for the complaint mechanism, such data should only concern data necessary for this specific purpose, while applying all the other principles of the Regulation (EU) 2016/679[26].

26. In the interest of legal certainty for all parties involved, the EDPS recommends further **specifying in which circumstances efforts to combat "illegal content" legitimise processing of personal data** in particular when they might involve automated means to "detect, identify and address" illegal content, regardless of whether they are conducted

    - on a voluntary or mandatory basis;
    - on the basis of notices or own-initiative investigation; or
    - in the context of addressing "systemic risks" as envisaged by Article 26-27.

    The Proposal should also clarify whether, and if so, to what extent, providers of intermediary services are **authorised to voluntarily notify** suspicions of criminal offences to law enforcement or judicial authorities (e.g., in the context of information giving rise to a suspicion of a possible criminal offence other than those envisaged by Article 21).

27. The EDPS recalls that even voluntary measures can constitute an interference with the rights to data protection and privacy[27]. Absent further safeguards, there is a risk that the Proposal will indirectly contribute to processing of personal data which is not proportionate to the aims pursued, in particular by not qualifying the types of illegal content that may actually warrant use of automated detection techniques involving the processing of personal data, or by not delineating the circumstances in which voluntary notification may take place). Additional recommendations for safeguards concerning the use of automated means involving processing of personal to detect, identify and address illegal content are provided later on in this Opinion (section 3.6).

3.3. Information about content moderation

28. Chapter III of the Proposal sets out the due diligence obligations for a transparent and safe online environment, adapted to the type and nature of the intermediary service concerned[28].

29. The first set of obligations applies to all providers of intermediary services, including the obligation to set out in their **terms and conditions** any restrictions imposed on the use of their services. Every provider must also act responsibly in applying and **enforcing** those restrictions.

30. According to Article 12(1), information to be provided 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.*"

31. "Content moderation" refers to activities undertaken by providers of intermediary services aimed at "***detecting, identifying and addressing illegal content or information incompatible with their terms and conditions***". It includes measures taken that affect the availability, visibility and accessibility of such content or 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[29].

32. The definition of content moderation makes clear that it **can** - but does not necessarily - **involve processing of personal data**, in ways that affect the rights and interests of the individuals concerned. The EDPS wishes to underline that depending on the categories of data that are processed and nature of the processing, automated content moderation may significantly impact both the right to **freedom of expression** and the **right to data protection**.

33. The EDPS understands that the duty to provide information contained in Article 12(1) of the Proposal is **complementary and without prejudice** to the obligation of providers to provide information to data subjects in accordance with Articles 12-14 of Regulation (EU) 2016/679[30]. The EDPS welcomes this provision insofar as it intends to **further increase transparency** of content moderation practices, including those involving the processing of personal data.

34. In the same vein, the EDPS also welcomes Article 13 of the Proposal, which **institutes transparency reporting obligations** requiring publication, at least once a year, of reports on any content moderation engaged in during the relevant period. As far as online platforms are concerned, the obligation is usefully complemented by Article 23(1)(c), which stipulates that the report must also include *inter alia* information on "*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***." As far as very large online platforms are concerned, Article 33 additionally requires publication (subject to possible redaction) of the results of its risk assessment, risk mitigation measures and audit (implementation) reports pursuant to Article 26-28 of the Proposal. The EDPS **strongly supports** Articles 26-28 and 33 of the Proposal, and in particular the requirement that very large online platforms to submit themselves to external and independent audits and to **publish the related audit and risk assessment reports**.

35. The potential impact of content moderation on fundamental rights is confirmed by Article 11(2) of the Proposal, which requires providers to act in "*a diligent, objective and **proportionate** manner in applying and enforcing the restrictions referred to in paragraph 1, with due regard to the rights and legitimate interests of all parties involved, including the **applicable fundamental rights** of the recipients of the service as enshrined in the Charter.*"

36. The potential impact on fundamental rights **may vary considerably** depending on the means that are used as well as their consequences, which may range from demotion of content to termination of a recipient's account, as well as possible notification of perceived criminal offences to law enforcement authorities[31].

37. The EDPS welcomes that the Proposal provides important safeguards to minimise the potential adverse effect on fundamental rights, yet recommends **enhancing the relevant provisions from a data protection point of view**, especially in situations where **profiling** or **automated decision-making** may be involved, as described later on in this Opinion[32].

3.4. Notice and action and the duty to give reasons

38. Articles 14 and 15 contain additional provisions applicable to providers of hosting services, including online platforms (who in addition to storing information at the request of the recipient of the service, also disseminate information to the public[33]).

39. Providers of hosting services shall put in place mechanisms 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[34]. Such notices should be sufficiently precise and substantiated for a diligent economic operator to be able to identify the illegality of the content in question[35].

40. Article 14(6) indicates that providers of hosting services might make use of **automated means to process or make decisions** about the notices received (in which case they must inform the individual or entity that submitted the notice with information on such use, provided the notice contains the name and an electronic mail address of the individual that submitted it)[36].

41. Article 15 requires the provider of hosting services to **provide a clear and specific statement of reasons** for any decision to remove or disable access to specific items of information provided by the recipients of the service, **irrespective of the means used for detecting, identifying, removing or disabling access** to that information.

42. The EDPS recalls that **Article 22 of Regulation (EU) 2016/679** imposes strict conditions on decisions based solely on automated processing, including profiling, leading to decisions that may produce legal effects, or similarly significantly affect the individual concerned. Moreover, even in the absence of solely automated decision-making, any profiling may present significant risks to the rights and freedoms of the individuals concerned[37].

43. The EDPS welcomes the requirement that hosting service providers must provide, "*where applicable, **information on the use made of automated means** in taking the decision, including where the decision was taken in respect of content detected or identified using*

automated means"[38]. Significantly, this requirement applies in situations where decisions are not taken solely on the basis of automated means and/or does not involve profiling. To further promote transparency, the EDPS recommends to modify Article 15(2) to state unambiguously that **information should in any event be provided on the automated means used for detection and identification of illegal content**, regardless of whether the subsequent decision involved use of automated means or not[39].

44. To ensure meaningful transparency, the EDPS recommends strengthening the **transparency requirements** set out in Article 14(6) and 15(2)(c) by further detailing the information to be provided to the individuals concerned when being informed about the relevant decision. The EDPS considers that online platforms using automated means for that content moderation or decision-making should at least inform affected individuals about the procedure followed, the technology used and the criteria and reasoning supporting the decision, without prejudice to the duty to inform and the rights of data subjects under Regulation (EU) 2016/679.

45. The EDPS **welcomes**, as an additional safeguard, the obligation of providers of hosting services to publish their decisions and the statements of reasons in a **publicly accessible database** managed by the Commission, with the explicit requirement that such information shall not contain personal data[40].

3.5. Complaint handling

46. Article 17 requires online platforms to provide for an **internal complaint-handling** system, which enables complaints to be lodged against the platforms' decisions to remove or disable access to information or to suspend or terminate the provision of the service (or account). Article 17(5) stipulates that platforms must ensure that decisions regarding such complaints are **not solely taken on the basis of automated means**.

47. The EDPS supports Article 17 of the proposal, yet recommends introducing a similar safeguard in relation to **all providers of hosting services**, not just online platforms, whenever the detection and identification of illegal content involves processing of personal data. Indeed, the Proposal itself alludes to the possibility that any hosting provider might potentially make use of automated means for the detection, identification and possible decisions concerning illegal content[41]. Where such mechanisms involve processing of personal data, individuals should be provided with an easily accessible complaint mechanism as envisaged by Article 17, regardless of whether the provider of the hosting service also disseminates information to the public.

48. Finally, the EDPS also recommends inserting in Article 17 **a deadline** for the platform decision on the complaint, as well as the indication that the complaint mechanism to be established is without prejudice to the rights and remedies available to data subjects in accordance with Regulation (EU) 2016/679 and Directive 2002/58/EC)[42].

3.6. Additional safeguards for content moderation

49. As indicated above, the EDPS welcomes that the Proposal includes several safeguards to minimise the risk of undue interference with fundamental rights, in particular by providing for a duty to inform, a duty to give reasons, and a duty to provide for an internal complaint mechanism which shall decide upon complaints not solely on the basis of automated means.

50. While Article 11(2) states that measures to enforce restrictions contained in terms and conditions shall be proportionate, additional safeguards are warranted to ensure that measures to detect and identify possible infringements remain limited to what is necessary.

51. First, the EDPS recommends extending the requirement of Article 12(2) **to all forms of content moderation**, regardless of whether such moderation takes place pursuant to the terms and conditions of the provider or any other basis. In addition, it should be specified that the measures must be "**necessary**" in addition to being "proportionate" to the aims pursued[43].

52. The requirement that the processing must be both necessary and proportionate implies also that the measures in question shall be as targeted as possible and designed in accordance with principles such as **data minimisation** and to prevent, **by default**, both the collection and disclosure of personal data, in accordance with Article 25 of Regulation (EU) 2016/679[44]. The EDPS recalls that not all forms of content moderation require attribution to a specific data subject. In so far as possible, no personal data should be processed when performing content moderation[45].

53. The EDPS reiterates that the Proposal does not aim to mandate or otherwise legitimate general surveillance of individuals' online activities. **Given, however, the already endemic monitoring of individuals' behaviour, in particular on online platforms, there is a risk that this proposal would exacerbate the situation if the measures taken prove not to be proportionate[46]. In such a delicate area, EU law must be as precise and clear as possible.**

54. The EDPS has already previously stressed that automated tools to detect potential illegal content should only be used in a **cautious and targeted** way, on the basis of the outcome of the risk assessment, subject to periodic review and reporting.[47] The EDPS also notes that, in accordance with the EDPB Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk", automated content moderation systems are likely to fulfil several criteria that would indicate that carrying out of a DPIA shall be required[48]. The EDPS recommends to require all online platforms using automated content moderation tools to publish the resulting DPIA (or at a minimum the risks identified and their associated mitigation measures).

55. **The EDPS recommends to specify that content moderation shall not involve the monitoring or profiling of the behaviour of individuals, unless the provider can demonstrate, on the basis of a risk assessment, that such measures are strictly necessary to mitigate the categories of systemic risks identified in Article 26** of the Proposal (i.e. dissemination of "illegal content"[49]; negative effects for the exercise of the fundamental rights; intentional manipulation of service). Doing so would make clear that use of such techniques (a) shall be subject to stricter scrutiny and (b) delineate the types of harms which may possibly justify the use of such techniques in the context of content moderation. Needless to say, any use of profiling or automated decision-making should remain subject to the requirements of Regulation (EU) 2016/679 and the oversight of the competent supervisory authorities[50].

56. Finally, the EDPS recommends to specify that any provider of hosting services using automated means of content moderation should ensure that such means **do not produce discriminatory or unjustified results**.[51]

3.7. Notification of suspicions of criminal offences

57. Article 21 requires online platforms to promptly inform the law enforcement or judicial authorities as they become 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. Recital (48) mentions, by way of example, offences specified in the Child Sexual Abuse Directive (Directive 2011/93/EU). 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.

58. The EDPS welcomes the clear delineation of the criminal offences which may give rise to a reporting obligation, i.e. "*serious criminal offences involving a threat to the life or safety of persons*". In the interest of meeting the requirements of legal certainty including foreseeability, the EDPS **strongly advises further specifying**, by listing in an Annex, any **other criminal offences** (other than child sexual abuse) that meets this threshold and may give rise to a notification obligation.

59. The EDPS welcomes the explicit clarification, in recital (48), that **the Proposal does not provide a legal basis for online platforms to profile recipients of the services with a view to the possible identification of criminal offences,** as well as the confirmation that 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.

60. The EDPS observes that Proposal does not contain any provision that seeks to restrict transparency obligation or the exercise of data subject rights under Regulation (EU) 2016/679. Insofar as the Proposal is "without prejudice" to Regulation (EU) 2016/679, the duties of the provider to inform individuals and to accommodate data subject rights therefore in principle remain unaffected. Nevertheless, the EDPS recommends the co-legislature to **introduce additional measures to ensure transparency and exercise of data subject rights**, subject, where strictly necessary, to narrowly defined restrictions (e.g., where necessary to protect the confidentiality of an ongoing investigation). Such restrictions must, in any case, comply with the requirements set out in Article 23(1) and (2) of Regulation (EU) 2016/679[52].

61. The Proposal does not provide a definition of the "relevant information" available to the online platform in the context of notification. Recital (48) mentions, by way of example "the content in question and an explanation of its suspicion". The EDPS considers that a **clear definition of "relevant information" is necessary** in order to ensure legal certainty for all parties involved, including the platforms themselves. The EDPS therefore recommends to **clearly define the term "relevant information**", by providing an exhaustive list of data categories that should be communicated, as well as any categories of data that should be preserved with a view of supporting further investigations by the relevant law enforcement authorities, if necessary[53].

3.8. Online advertising transparency

62. Article 24 requires online platforms to ensure that the recipients of the service can identify, for each specific advertisement, the natural or legal person *on whose behalf* the advertisement is displayed as well as meaningful information about the *main parameters* used to determine the recipient to whom the advertisement is displayed. Article 30 specifies that very large online platforms shall additionally make publicly available, through application programming interfaces, a repository containing the same information, as well as additional information to further increase transparency.

63. The EDPS strongly supports the aim of Articles 24 and 30, which are aimed to provide increased transparency and therefore accountability in relation to targeted advertising in a manner that is **complementary to data protection law** (e.g., by stipulating that the relevant information must be provided to the recipient in real-time and requiring a public repository from very large online platforms)[54]. The EDPS also welcomes the clarification in recital (52) that Article 24 and 30 are without prejudice to the application of the relevant provisions of Regulation (EU) 2016/679 and Directive 2002/58/EC. Finally, the EDPS also very much welcomes the reference to the need to obtain consent of the data subject prior to the processing of personal data for targeted advertising.

64. Both Articles 24 and 30 require online platforms to inform about the "**natural or legal person on whose behalf the advertisement is displayed**". It is not entirely clear however, if this refers to the advertiser (e.g., the company whose products or services are being advertised) or to possible third parties who may have delivered the advertisement to the online platform (e.g. an ad platform[55]). The EDPS therefore recommends to clarify this requirement further.

65. The EDPS notes that most, but not all, of online advertising is managed automatically. The EDPS recommends to add to the requirements of Article 24 a new item informing data subjects **whether the advertisement was selected using an automated system** (e.g., ad exchange or platform) and, in that case, the identity of the **natural or legal person(s) responsible** for the system(s) (which may be one or more other parties than the natural or legal or person "on whose behalf" the advertisement is displayed).

66. Article 30(2)(d) requires very large online platforms to include in the repository information about "whether the advertisement was intended to be displayed specifically to one or more particular groups of recipients of the service". The EDPS is of the view that **exclusion criteria are at least as relevant as inclusion criteria**, especially with a view of detect potential unfairness or discriminatory impact. The EDPS therefore recommends to specify that the register should also include information whether one or more particular groups of recipients of the service were *excluded* from the advertisement target group.

67. In order to ensure meaningful transparency, the EDPS suggests to replace the reference to "the main parameters" by "parameters" and to provide further clarification as to **what parameters would need to be disclosed at a minimum to constitute "meaningful information"** within the meaning of Article 24 and 30. In particular, the EDPS recommends requiring transparency on each of the criteria used to target advertising.

68. In order to ensure **accountability of advertisers**, the EDPS recommends to consider similar requirements that apply to ensure traceability of traders (Article 22) in relation to the users of online advertisement services (Articles 24 and 30)[56].

69. Given the many risks associated with online targeted advertising[57], the EDPS urges the co-legislature to consider **additional rules going beyond transparency**. In this regard, the EDPS strongly supports the Resolution of the European Parliament, which stated targeted advertising must be **regulated more strictly** in favour of less intrusive forms of advertising that do not require any tracking of user interaction with content[58]. The EDPS therefore similarly urges the co-legislature to consider **a phase-out leading to a prohibition of targeted advertising on the basis of pervasive tracking**.[59]

70. Finally, complementary to the above, the EDPS invites the co-legislature to consider further restrictions in relation to (a) the **categories of data that can be processed for targeting purposes** (e.g., limitations regarding the combination of data collected "off platform"); (b) **categories of data or criteria on the basis of which ads may be targeted or served** (e.g., criteria that directly or indirectly correspond with special categories of data or might be used to exploit vulnerabilities); and (c) **the categories of data that may be disclosed** to advertisers or third parties to enable or facilitate targeted advertising.

3.9. Recommender systems

71. Article 2(o) defines a "recommender system" as "*a fully or partially automated system used by an online platform to **suggest** in its online interface specific information to recipients of the service, including as a result of a search initiated by the recipient or otherwise determining the relative order or prominence of information displayed*". The EDPS considers that recommender systems in practice **go far beyond "suggesting"** online content. Indeed, recital (62) explains that recommender systems may involve "*algorithmically suggesting, ranking and prioritising information, distinguishing through text or other visual representations, or otherwise curating information provided by recipients*".

72. The EDPS welcomes the recognition that recommender systems **can have a significant impact** on the ability of recipients to retrieve and interact with information online and also play an important role in the **amplification** of certain messages, the viral dissemination of information and the stimulation of online behaviour.[60] Certain recommender systems feed on data subjects' profiles and define the content these can access in online platforms, with all the attendant risks.

73. The risks of profiling and micro-targeting in the context of recommender systems or online advertising was already raised by the EDPS in his Opinion on online manipulation and personal data[61]. The EDPS recommends the EU legislator to clarify that that, in accordance with the requirements of data protection by design and by default, recommender systems **should by default not be based on "profiling"** within the meaning Article 4(4) of Regulation (EU) 2016/679.

74. Article 29(1) provides that very large online platforms that use recommender systems shall ensure that recipients of the service shall have at least the option to make use of a recommender system which is not based on profiling, within the meaning of Article 4(4) of Regulation (EU) 2016/679. In accordance with the requirements of data protection by

design and by default and data minimisation, the EDPS strongly recommends to modify the requirement to **opt-in rather than opt-out**, making the option not based on profiling the default one.

75. Article 29(1) requires very large online platforms to set out, in their terms and conditions, the "main parameters" used in their recommenders system, as as well as any options for the recipients of the service to modify or influence those main parameters that they may have made available. Notwithstanding the requirement that the information shall be presented in a "clear, accessible and easily comprehensible manner", the EDPS considers that **terms and conditions are generally lengthy and legalistic documents** that average users have difficulties to understand. Terms and conditions of very large online platforms are often even more complex because they inform about the many related services platform offer. Consequently, including information about the recommender system parameters and options in the terms and conditions would only make them difficult to find and understand for data subjects. The EDPS strongly recommends to require that such information concerning the role and functioning of recommender systems to be presented separately, in a manner that should be easily accessible, clear for average users and concise.

76. In the same vein as the recommendations regarding online advertising transparency, it is also necessary to **ensure meaningful transparency in the context of recommender systems and their use of data subjects' profiles**. Therefore, the EDPS recommends to replace the reference to the "main parameters" by "parameters", or at least to provide further clarification as to what parameters would need to be disclosed at a minimum to constitute "meaningful information" in this context[62].

77. Despite their significant impact, recommender systems are frictionless from a user perspective. To improve the transparency and user control, the EDPS recommends to include the following additional requirements in Article 29:

- to indicate in a prominent part of the platform the fact that the platform uses a recommender system and to offer controls with the available options in a user-friendly manner;
- to inform the platform user whether the recommender system is an automated system and, in that case, the identity of the natural or legal person responsible for the system, if different from the platform provider;
- to enable data subjects to view, in a user-friendly manner, any profile or profiles used to curate the platform content for the recipient of the service;
- to allow the recipients of the service to customise the recommender systems based at least on basic natural criteria (e.g., time, topics of interest, ...); and
- to provide users with an easily accessible option to delete any profile or profiles used to curate the content they see.

3.10. Access by vetted researchers

78. Article 31 provides that, upon a reasoned request from the Digital Services Coordinator of establishment or the Commission, very large online platforms shall, within a reasonable period, as specified in the request, provide access to data to "vetted researchers" for the sole purpose of conducting research that contributes to the identification and understanding of systemic risks as set out in Article 26(1).

79. The EDPS welcomes the aim of Proposal to subject very large online platforms to the scrutiny of "vetted researchers", in compliance with Regulation (EU) 2016/679[63]. The EDPS recommends that the Commission deploy strict standards when determining the criteria for a researcher to qualify as "*independent from commercial interests*".

80. Scientific research serves a valuable function in a democratic society to hold powerful players to account. The EDPS reiterates that **data protection should not be misappropriated as a means for powerful players to escape transparency and accountability**. Researchers operating within ethical governance frameworks should therefore be able to access necessary API and other data, with a valid legal basis and subject to the principle of proportionality and appropriate safeguards[64].

81. The EDPS notes that under the Proposal vetted researchers would be allowed to investigate the systemic risks put forward in Article 26 (Article 31(2)). The EDPS welcomes the Proposal's inclusion in Article 26 of both systemic risks to individual rights and to societal interests, but urges the co-legislature to further clarify what "systemic risks" and "societal harms" (Recitals 54, 56 and 94) are. With respect to Article 26(1)(c), the EDPS notes that the services of very large online platforms may pose systemic risks for "the protection of public health, minors, civic discourse, or actual or foreseeable effects related to electoral processes and public security" independently of whether they are manipulated or not. The EDPS therefore suggests rephrasing this paragraph as follows: "(c) 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, **in particular in relation to the risk of the intentional manipulation of their service, including by means of inauthentic use or automated exploitation of the service.**"

82. The EDPS considers that Article 31 is narrow in scope, given that access shall be given to vetted researchers for the sole purpose of conducting research that contributes to the *identification and understanding* of systemic risks as set out in Article 26(1) in the context of assessing and monitoring compliance with the Proposal. The EDPS considers that Article 31 should be expanded to at least **enable verification of the effectiveness and proportionality of the mitigation measures**.

83. Finally, the EDPS recommends the co-legislature to consider ways to **facilitate public interest research more generally**, including outside the context of monitoring compliance with the Proposal (and in addition the provision of publically available API's for online advertising), provided such research is genuinely carried out in the public interest. In this context, the EDPS refers also to his Preliminary Opinion on data protection and scientific research[65].

3.11. Platform interoperability

84. The EDPS considers that issues of algorithmic amplification and other harms that the Proposal seeks to address are exacerbated due to closed nature of very large online platforms, which limit the ability of users to communicate across platforms ("walled gardens"). Increased interoperability has the potential to facilitate the development of a more open, pluralistic environment, as well as create new opportunities for the development of innovative digital services.

85. The EDPS recommends the co-legislature to consider introducing minimum interoperability requirements for very large online platforms, with explicit obligations on very large online platforms to support interoperability, as well as obligations not to take measures that impede such interoperability. The EDPS suggests to draw up at European level **technical standards on interoperability** which should be supported by very large online platforms (in its various specifications, namely protocol interoperability, data interoperability, full protocol interoperability[66]). Such technical standards should be in compliance with European data protection law, not lower the level of security provided by platforms and not hinder innovation via too detailed interoperability standards. The European standardisation organisations, in consultation with the European Data Protection Board where appropriate, should draw up standards which satisfy these requirements. The Commission should have the possibility to request the European standardisation organisations to develop such European standards, in accordance with the applicable Union legislation on European standardisation[67].
.

3.12. Implementation, cooperation, sanctions and enforcement

86. The EDPS welcomes the recognition of the **cross-sectorial relevance** of the aspects regulated in the Proposal, including in relation to the protection of individuals with regard to the processing of personal data. Certain provisions and possible measures adopted pursuant to the Proposal will clearly have an impact on the processing of personal data. The cross-sectorial relevance of the Proposal is further made evident by a number of provisions, including Articles 26-27 (identification and mitigation of systemic risks), Article 35(1) (codes of conduct), Article 36 (codes of conduct for online advertising).

87. The EDPS considers it necessary to **ensure complementarity in the oversight** in the supervision of online platforms and other providers of hosting services. Such complementary is necessary not only to mitigate risks of undue interference with fundamental rights, but also to increase transparency and accountability of the actors regulated by the Proposal. Building on the experiences related to the Digital Clearinghouse[68], the EDPS strongly recommends that the Proposal:

    (1) **provide for an explicit legal basis for cooperation** among the relevant authorities, each acting within their respective areas of competence;

    (2) require an **institutionalised and structured** cooperation between the competent oversight authorities, including data protection authorities;

    (3) **make explicit reference** to the competent **authorities** that involved in the cooperation and identify the **circumstances in which cooperation should take place**.

88. Recital (91) already indicates that the European Digital Services Board should be allowed to cooperate with other Union bodies, offices, agencies and advisory groups with responsibilities in fields such as data protection and consumer protection, as necessary for the performance of its tasks. Given the importance of cooperation with **competent authorities in the area of competition law**, the EDPS recommends adding explicit reference to such authorities here, in addition to those already mentioned. The EDPS also recommends to introduce an explicit **reference to the European Data Protection Board** in the recitals of the Proposal.

89. The EDPS recommends to ensure that the Digital Services Coordinators, other competent authorities and the Commission should also have the power and a duty to consult with

relevant competent authorities, including data protection authorities, **in the context of their investigations and assessments** of compliance with the Proposal. In addition, the EDPS recommends clarifying that competent supervisory authorities under the Proposal should be able to provide to the competent supervisory authorities under Regulation (EU) 2016/679, upon request or on their own initiative, any **information obtained in the context of any audits and investigations** that relate to the processing of personal data and to include an **explicit legal basis** to that this effect.

90. Additional circumstances in which cooperation should take place include, without being limited to :

- identification and assessment of the most prominent and recurrent systemic risks, as well as best practices to mitigate such risks (Articles 27(2)-(3));
- codes of conduct for challenges relating to different types of illegal content and systemic risks (Article 35); and
- codes of conduct for online advertising (Article 36).

91. Article 41(5) stipulates that 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"*. Article 42(2) provides that penalties shall be "effective, proportionate and dissuasive". To be consistent, the EDPS recommends also to refer to the relevant criteria in Article 59 (fines imposed by the Commission).

92. Article 49(1)(e) says the Board shall "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". The EDPS recommends to allow the Board to (1) issue own-initiative opinions; and (2) to enable the Board to issue opinions on matters other than the *measures* taken by the Commission.

4. CONCLUSIONS

93. In light of the above, the EDPS makes the following recommendations:

Concerning the relationship to Regulation (EU) 2016/679 and Directive 2002/58/EC:

- to align the wording of Article 1(5)i of the Proposal with the current wording of Article 1(5) b) of Directive 2000/31/EC; and
- to clarify that the Proposal does not apply to questions relating to the liability of controllers and processors;

Concerning content moderation and notification of suspicions of criminal offences:

- to clarify that not all forms of content moderation require attribution to a specific data subject and that in accordance with the requirements of data minimisation and data

protection by design and by default, content moderation should, insofar as possible, not involve any processing of personal data;

- to ensure content moderation takes place in accordance with the rule of law, by delineating when efforts to combat "illegal content" legitimise the use of automated means and processing of personal data to detect, identify and address illegal content;

- to specify that profiling for purposes of content moderation should be prohibited unless the provider can demonstrate that such measures are strictly necessary to adress the systemic risks explicitly identified by the Proposal;

- to clarify whether, and if so, to what extent, providers of intermediary services are authorised to voluntarily notify suspicions of criminal offences to law enforcement or judicial authorities, outside the case envisaged by Article 21 of the Proposal;

- to specify that any provider of hosting services using automated means of content moderation should ensure that such means do not produce discriminatory or unjustified results;

- to extend the requirement of Article 12(2) of the Proposal to all forms of content moderation, regardless of whether such moderation takes place pursuant to the terms and conditions of the provider or any other basis; and to specify that the measures must be "necessary" in addition to being "proportionate" to the aims pursued;

- to strengthen the transparency requirements set out in Article 14(6) and 15(2)(c) of the Proposal, by further detailing the information to be provided to the individuals concerned, in particular in case of use of automated means for that content moderation, without prejudice to the duty to inform and the rights of data subjects under Regulation (EU) 2016/679;

- to modify Article 15(2) of the Proposal to state unambiguously that information should in any event be provided on the automated means used for detection and identification of illegal content, regardless of whether the subsequent decision involved use of automated means or not;

- to require all providers of hosting services, not just online platforms, to provide easily accessible complaint mechanism as envisaged by Article 17 of the Proposal;

- to insert a deadline in Article 17 of the Proposal for the platform decision on the complaint, as well as the indication that the complaint mechanism to be established is without prejudice the rights and remedies available to data subjects in accordance with Regulation (EU) 2016/679 and Directive 2002/58/EC;

- to further specify, by listing in an Annex, any other criminal offences (other than child sexual abuse) that meets the threshold of Article 21 of the Proposal and may give rise to a notification obligation;

- to consider introducing additional measures to ensure transparency and exercise of data subject rights, subject, where strictly necessary, to narrowly defined restrictions (e.g., where necessary to protect the confidentiality of an ongoing investigation)in

compliance with the requirements set out in Article 23(1) and (2) of Regulation (EU) 2016/679; and

- to clearly define the term "relevant information", referred to in Article 21 of the Proposal, by providing an exhaustive list of data categories that should be communicated, as well as any categories of data that should be preserved with a view of supporting further investigations by the relevant law enforcement authorities, if necessary.

Concerning online advertising:

- to consider additional rules going beyond transparency, including a phase-out leading to a prohibition of targeted advertising on the basis of pervasive tracking;

- to consider restrictions in relation to (a) the categories of data that can be processed for targeting purposes; (b) categories of data or criteria on the basis of which ads may be targeted or served; and (c) the categories of data that may be disclosed to advertisers or third parties to enable or facilitate targeted advertising; and

- to further clarify the reference to natural or legal person on whose behalf the advertisement is displayed in Articles 24 and 30 of the Proposal;

- to add to the requirements of Article 24 a new item that requires the platform provider to inform data subjects whether the advertisement was selected using an automated system (e.g., ad exchange or platform) and, in that case, the identity of the natural or legal person(s) responsible for the system(s);

- to specify in Article 30(2)(d) specifying that the register should also include information whether one or more particular groups of recipients of the service were *excluded* from the advertisement target group;

- replacing the reference to "the main parameters" by "parameters" and to provide further clarification as to what parameters would need to be disclosed at a minimum to constitute "meaningful information" within the meaning of Article 24 and 30of the Proposal; and

- to consider similar requirements that apply to ensure traceability of traders (Article 22 of the Proposal) in relation to the users of online advertisement services (Articles 24 and 30 of the Proposal).

Concerning recommender systems:

- to clarify that that, in accordance with the requirements of data protection by design and by default, recommender systems should by default not be based on "profiling" within the meaning Article 4(4) of Regulation (EU) 2016/679;

- to provide that information concerning the role and functioning of recommender systems to be presented separately, in a manner that should be easily accessible, clear for layman and concise;

- to provide that, in accordance with the requirements of data protection by design and by default, recommender systems should by default not be based on "profiling" within the meaning Article 4(4) of Regulation (EU) 2016/679; and

- to include the following additional requirements in Article 29 of the Proposal:
  - to indicate in a prominent part of the platform the fact that the platform uses a recommender system and a control with the available options in a user-friendly manner;
  - to inform the platform user whether the recommender system is an automated decision-making system and, in that case, the identity of the natural or legal person liable for the decision.
  - to enable data subjects to view, in a user-friendly manner, any profile or profiles relating used to curate the platform content for the recipient of the service;
  - to allow the recipients of the service to customise the recommender systems based at least on basic natural criteria (e.g., time, topics of interest, ...); and
  - to provide users with an easily accessible option to delete any profile or profiles used to curate the content they see.

Concerning access by vetted researchers:

- to provide that, in accordance with the requirements of data protection by design and by default, recommender systems should by default not be based on "profiling" within the meaning Article 4(4) of Regulation (EU) 2016/679;

- to rephrase Article 26(1)(c) of the Proposal paragraph to make reference to actual or foreseeable systemic negative effect on the protection of public health, minors, civic discourse, or actual or foreseeable effects related to electoral processes and public security, in particular in relation to the risk of the intentional manipulation of their service, including by means of inauthentic use or automated exploitation of the service;

- to expand Article 31 to at least enable verification of the effectiveness and proportionality of the mitigation measures; and

- to consider way to facilitate public interest research more generally, including outside the context of monitoring compliance with the Proposal;

Concerning platform interoperability:

- to consider introducing minimum interoperability requirements for very large online platforms and to promote the development of technical standards at European level, in accordance with the applicable Union legislation on European standardisation.

Concerning implementation, cooperation, sanctions and enforcement:

- to ensure complementarity in the oversight in the supervision of online platforms and other providers of hosting services, in particular by

- providing for an explicit legal basis for cooperation among the relevant authorities, each acting within their respective areas of competence;
- requiring an institutionalised and structured cooperation between the competent oversight authorities, including data protection authorities; and
- making explicit reference to the competent authorities that involved in the cooperation and identify the circumstances in which cooperation should take place.

- to make reference to competent authorities in the area of competition law, as well as the European Data Protection Board in the recitals of the Proposal;

- to ensure that the Digital Services Coordinators, competent authorities Commission should also have the power and duty to consult with relevant competent authorities, including data protection authorities, in the context of their investigations and assessments of compliance with the Proposal;

- to clarify that competent supervisory authorities under the Proposal should be able provide, upon request of competent supervisory authorities under the Regulation (EU) 2016/679 or on their own initiative, any information obtained in the context of any audits and investigations that relate to the processing of personal data and to include an explicit legal basis to that this effect;

- to ensure greater consistency among the criteria included in Article 41(5), Article 42(2) and Article 59 of the Proposal; and

- to allow the European Digital Services Board to issue own-initiative opinions and to enable the Board to issue opinions on matters other than the measures taken by the Commission.

Brussels, 10 February 2021

Wojciech Wiewiorówski

(e-signed)

Notes

[1] OJ L 119, 4.5.2016, p. 1.
[2] OJ L 295, 21.11.2018, p. 39.
[3] COM (2020) 825 final.
[4] COM(2020) 67 final, p. 12.
[5] COM (2020) 825 final, p. 1.
[6] COM (2020) 825 final, p. 2.
[7] COM(2020) 842 final.
[8] European Data Protection Supervisor, "The EDPS Strategy 2020-2024, Shaping a Safer Digital Future", 30 June 2020, https://edps.europa.eu/press-publications/press-news/press-releases/2020/shaping-safer-digital-future-new-strategy-new_de
[9] COM (2020) 825 final, p. 12 ("*Union citizens and others are exposed to ever-increasing risks and harms online – from the spread of illegal content and activities, to limitations to express themselves and other societal harms").*
[10] Recital (54) of the Proposal.
[11] European Data Protection Supervisor, Opinion 3/2018 on online manipulation and personal data, 19 March 2018, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.
[12] European Data Protection Board, Guidelines 8/2020 on the targeting of social media users, Version 1.0, 2 September 2020, 4-7, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf.
[13] Recital (56) of the Proposal.
[14] Recital (68) of the Proposal.
[15] See in the same vein also the Note from the EU Counter-Terrorism Coordinator, "The role of algorithmic amplification in promoting violent and extremist content and its dissemination on platforms and social media", p. 2, Council of the European Union, 9 December 2020, https://data.consilium.europa.eu/doc/document/ST-12735-2020-INIT/en/pdf ("*This business model drives users automatically to content that is detected by algorithms as being the most engaging. As such, social media companies do not simply offer a platform on which citizens exercise their freedom of expression. They amplify certain content and demote other content, while shielding the mechanisms that regulate this from public scrutiny*").
[16] COM(2020) 842 final.
[17] COM (2020) 825 final, p. 5.
[18] European Data Protection Supervisor, "Formal comments of the EDPS on a Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market", 12 February 2019, p. 6, https://edps.europa.eu/sites/edp/files/publication/18-07-03_edps_formal_comments_copyright_en.pdf.
[19] *Ibid*, p. 2.
[20] OJ L 178, 17.7.2000, p. 1.
[21] See Court of Justice of the European Union, *Judgment in La Quadrature du Net a.o.*, Joined Cases C-511/18, C-512/18 and C-520/18, 6 October 2020, ECLI:EU:C:2020:79, at paragraphs 199-200 ("*199 However, Article 1(5) of Directive 2000/31 provides that that directive* ***is not to apply to questions*** *relating to information society services covered by Directives 95/46 and 97/66. In that regard, it is clear from recitals 14 and 15 of Directive 2000/31 that the protection of the confidentiality of communications and of natural persons with regard to the processing of personal data in the context of information society services are governed only by Directives 95/46 and 97/66, the latter of which prohibits, in Article 5 thereof, all forms of interception or surveillance of communications, in order to protect confidentiality. 200 Questions related to the protection of the confidentiality of communications and personal data must be assessed on the basis of Directive 2002/58 and Regulation 2016/679, which replaced Directive 97/66 and Directive 95/46 respectively, and it should be noted that the protection that Directive 2000/31* ***is intended to ensure cannot, in any event, undermine the requirements under*** *Directive 2002/58 and Regulation 2016/679 (see, to that effect, judgment of 29 January 2008, Promusicae, C-275/06, EU:C:2008:54, paragraph 57).")*
[22] Article 2(g) of the Proposal defines "illegal content" as "*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*".
[23] Article 82 of Regulation (EU) 2016/679.
[24] Recital (28) of the Proposal.
[25] See also COM (2020) 825 final, p. 3.
[26] See also the Letter of the EDPB to Dr. Alexander Dix, 20 October 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/out2020-0111edpb_replydrdixart17.pdf.

[27] See also European Data Protection Supervisor, "Opinion 7/2020 on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online", 10 November 2020, https://edps.europa.eu/sites/edp/files/publication/20-11-10_opinion_combatting_child_abuse_en.pdf.
[28] Certain basic obligations are applicable to all providers of intermediary services. In addition, the Proposal contains further obligations for providers of hosting services and, more specifically, online platforms and very large online platforms.
[29] Article 2(p) of the Proposal.
[30] See Article 29 Data Protection Working Party, "Guidelines on Transparency under Regulation 2016/679", wp260rev.01, 11 April 2018 (later endorsed by the EDPB), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.
[31] See also Article 21 of the Proposal.
[32] See paragraphs 49 and following.
[33] See Article 2(h) of the Proposal.
[34] Article 14(1) of the Proposal.
[35] See article 14(2) of the Proposal.
[36] See Article 14(4) of the Proposal.
[37] See Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, 6 February 2018 (later endorsed by the EDPB), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053
[38] Article 15(2)c of the Proposal.
[39] As currently drafted, the text could be (mis)understood as suggesting that information on the use made of automated means to detect or identify illegal content should only be provided if automated means were also used in taking the decision.
[40] Article 15(4) of the Proposal.
[41] See paragraphs 40-43 above. This is further confirmed by the Explanatory Memorandum of the Proposal, which states that "*the provisions of this Regulation relating to liability should not preclude the development and effective operation, by the different interested parties, of technical systems of protection and identification and of automated recognition made possible by digital technology within the limits laid down by Regulation 2016/679.*"
[42] EDPS, "Formal comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online", 12 February 2019, p. 9, https://edps.europa.eu/sites/edp/files/publication/2018-02-13_edps_formal_comments_online_terrorism_regulation_en.pdf
[43] See also European Data Protection Supervisor, "Necessity toolkit on assessing the necessity of measures that limit the fundamental right to the protection of personal data", 11 April 2017; "Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data", 19 December 2019, https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf
[44] See in the same vein European Data Protection Supervisor, "Formal comments of the EDPS on a Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market", 12 Feburary 2019, p. 5, https://edps.europa.eu/sites/edp/files/publication/18-07-03_edps_formal_comments_copyright_en.pdf.
[45] See also the Letter of the EDPB to Dr. Alexander Dix, 20 October 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/out2020-0111edpb_replydrdixart17.pdf.
[46] EDPS, "Formal comments of the EDPS on a Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market", p. 6.
[47] EDPS, "Formal comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online", p. 6-7.
[48] The Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 include nine criteria. Automated content moderation systems used by online platforms that involve processing of personal data are fulfill at least least the first three (Evaluation or scoring, automated-decision making with legal or similar significant effect and systematic monitoring). Very large online platforms also fulfil the large scale processing criterion.
[49] As indicated previously, the EDPS recommends the co-legislature to further delineate circumstances efforts to combat "illegal content" legitimate processing of personal data. See in partcular paragraphs 26-27.
[50] See also Article 29 Data Protection Working Party, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", wp251rev.01, 6 February 2018 (later endorsedy by the EDPB), p. 28, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 ("*Controllers should carry out frequent assessments on the data sets they process to check for any bias, and develop ways to address any prejudicial elements, including any over-reliance on correlations. Systems that audit algorithms and regular reviews of the accuracy and relevance of automated decision-making including profiling are other useful*

measures. Controllers should introduce appropriate procedures and measures to prevent errors, inaccuracies 43 or discrimination on the basis of special category data. These measures should be used on a cyclical basis; not only at the design stage, but also continuously, as the profiling is applied to individuals").

[51] EDPS, "Formal comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online", p. 8.

[52] See similarly EDPS on CSAM derogation, paragraph 39 https://edps.europa.eu/sites/edp/files/publication/20-11-10_opinion_combatting_child_abuse_en.pdf

[53] EDPS, "Formal comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online", p. 9-10.

[54] See also COM (2020) 825 final, p. 5 ("*This proposal is without prejudice to the Regulation (EU) 2016/679 (the General Data Protection Regulation) and other Union rules on protection of personal data and privacy of communications. For example, the measures concerning advertising on online platforms complement but do not amend existing rules on consent and the right to object to processing of personal data. They impose transparency obligations towards users of online platforms, and this information will also enable them to make use of their rights as data subjects. They also enable scrutiny by authorities and vetted researchers on how advertisements are displayed and how they are targeted.*")

[55] Estrada-Jiménez, José & Parra-Arnau, Javier & Rodríguez-Hoyos, Ana & Forné, Jordi. (2019). On the regulation of personal data distribution in online advertising platforms. Engineering Applications of Artificial Intelligence. 82. 13-29. 10.1016/j.engappai.2019.03.013.

[56] See also European Parliament, "European Parliament resolution of 20 October 2020 with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL))", https://www.europarl.europa.eu/doceo/document/TA-9-2020-0273_EN.html paragraph 18. In relation to Article 22 of the Proposal, the EDPS also considers it should be further clarified why there is a difference in treatment of natural persons, as opposed to legal persons, when it comes to the communication of the bank account details (letter c) to ensure the traceability of the trader.

[57] Recital (63) of the Proposal itself mentions "*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.*"

[58] European Parliament, "European Parliament resolution of 20 October 2020 with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online" (2020/2019(INL)), paragraph 15.

[59] European Parliament, "European Parliament resolution of 20 October 2020 with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL))", paragraph 17. At the minimum, the co-legislature should consider the introduction of an explicit requirement, in the same vein as suggested by the Annex to another European Parliament Resolution, ensuring that individuals by default shall not be tracked or micro-targeted and to require an opt-in for the use of behavioural data for advertising purposes, as well as a separate opt-in option for political advertising. See European Parliament, "European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market, (2020/2018(INL))", p. 27 https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272_EN.pdf

[60] Recital (62) of the Proposal.

[61] See European Data Protection Supervisor, "Opinion 3/2018 EDPS Opinion on online manipulation and personal data", 19 March 2018, p. 9, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf ("*Manipulation also takes the form of microtargeted, managed content display which is presented as being most 'relevant' for the individual but which is determined in order to maximise revenue for the platform. This is akin to the 'secret menus' used to steer users of ecommerce sites and the 'dark patterns' used to dissuade decisions less desirable from the platform's perspective (such as declining to add additional items, like insurance, to a shopping cart).*"

[62] See also paragraph 67 above (in relation to online advertising).

[63] Article 31 of the Proposal.

[64] European Data Protection Supervisor, "A Preliminary Opinion on data protection and scientific research", 6 January 2020, https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

[65] European Data Protection Supervisor, "A Preliminary Opinion on data protection and scientific research", 6 January 2020, https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

[66] See also J. Crémer, Y.-A. de Montjoye and H. Schweitzer, "Competition Policy for the digital era", 2019, p. 58 and following, at: https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf . See also the EDPS Opinion on the Digital Markets Act.

[67] The European Commission should ask the European Standardisation Organisations in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC,

95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council. *OJ L 316, 14.11.2012, p. 12–33*

[68] See https://www.digitalclearinghouse.org. The Digital Clearinghouse serves a forum for discussion among data protection, consumer protection, competition authorities which contributed to shifting the analysis of the interaction among the three policy areas from the more academic level to the policy-making and regulatory context. The Digital Clearinghouse was established by the EDPS in 2016 with the Opinion on coherent enforcement of fundamental rights in the age of Big Data, 23 September 2016, more info available at https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en