EUROPEAN DATA PROTECTION SUPERVISOR

EDPS Comments on the Federal Trade Commission Trade Regulation Rule on Commercial Surveillance and Data Security
Commercial Surveillance ANPR, R 111004

Executive Summary

These public comments are provided having regard to the public consultation on the advance notice of proposed rulemaking ('ANPR') on commercial surveillance and data security practices that harm consumers issued by the Federal Trade Commission ('the FTC') on 11 August 2022.

The EDPS, in his role of EU independent data protection authority pursuant to Regulation (EU) 2018/1725, welcomes this consultation and is available to engage with the FTC on the issues identified in response the questions raised by the FTC. In doing so, the EDPS aims at fostering the fruitful cross-Atlantic dialogue on the enhancement of privacy, data protection and data security. The EDPS also follows with keen interest the developments related to the proposed American Data Privacy and Protection Act ("ADPPA").

These comments are based on the EU data protection legislation, as well as relevant guidance of the European Data Protection Board ('the EDPB'), established by the General Data Protection Regulation (EU) 2016/679 ('the GDPR') of which the EDPS is a member, and draw on the EDPS extensive body of legislative advice and other relevant legislation in force or recently adopted.

The EDPS recalls the concept of personal data, special categories of personal data, data protection principles and conditions for lawful processing of personal data in EU data protection law. We refer in particular to GDPR legal basis for data processing having regard to the provision of online services. We also recall the importance of the security of data processing, not limited to the storage limitation, under the GDPR.

The EDPS wishes to highlight in particular the importance of the principles of purpose limitation and data minimisation enshrined in EU law under both primary (Charter of Fundamental Rights of the European Union) and secondary law (Article 5(1)(b) and (c) GDPR). The principles of data minimisation and purpose limitation are also relevant having regard to the development of AI systems. We recall the importance of the principle of data minimisation also for data security. Due to the risks for the person concerned, the principles of data minimisation and purpose limitation are particularly important in the context of 'Internet of Things' (IoT) and 'Internet of Bodies' (IoB), as well as in the context of the provision of online services.

With reference to the FTC questions on consent, the EDPS first recalls the requirements of consent (freely given, specific, informed and unambiguous), as one of the possible legal grounds for the processing of personal data under the GDPR. We then point out to 'dark

EUROPEAN DATA PROTECTION SUPERVISOR
Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu
Website: edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

patterns' as harmful commercial practices undermining the validity of consent. From a technological viewpoint, we note that providing informed consent in the IoT context is technically possible; although often challenging. We also point to other legal instruments of EU law that might be applicable in this context, including the ePrivacy Directive 2002/58/EC.

Systemic issues of pervasive 'commercial surveillance' and of information and power asymmetries between platform providers and end-users seem to require some clear prohibitions of tracking and profiling of individuals: it is the case of online behavioural advertising. The recently adopted Digital Services Act provides for the prohibition for certain categories of online providers to serve advertising based on profiling using special categories of personal data and personal data related to children. Other recent EU legislative proposals that would provide additional prohibitions on the processing of certain categories of personal data in specific contexts are: the proposal for review of the consumer credit directive, the proposal for a platform work directive. The recently adopted Digital Markets Act (DMA) will also impose additional conditions and limits on the processing of personal data (regarding the combination and cross-use) by "gatekeepers".

The recently proposed AI Act aims, among other objectives, at addressing the issue of "algorithmic harm". The use of artificial intelligence technologies introduces a higher level of complexity into profiling and automated decision-making. In their Joint Opinion on the AI Act, the EDPS and the EDPB recommended specific prohibitions to be included in the AI Act. At the same time, the EDPB and the EDPS recommended in particular the mitigation of bias from the first stages of AI development and at all different stages of the AI life-cycle (design, development and application).

Finally, the EDPS highlights the risks related to the use of (AI-driven) recommender systems in the context of online targeting and brings to the FTC attention, among others, his Opinion 3/2018 on online manipulation and personal data, as well as on the DSA and on the Proposal for a Regulation on the transparency and targeting of political advertising.

1. Introduction

1.1 Introduction and background

1. On 11 August 2022 the Federal Trade Commission ('the FTC') published an advance notice of proposed rulemaking ('ANPR') to seek public comments on commercial surveillance and data security practices that harm consumers[1]. The FTC invites comment on "whether it should implement new trade regulation rules or other regulatory alternatives concerning the ways in which companies (1) collect, aggregate, protect, use, analyse, and retain consumer data, as well as (2) transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive". In particular, it seeks input "about prevalent commercial surveillance practices or lax data security practices that are unfair or deceptive, as well as about efficient, effective, and adaptive regulatory responses"[2].

[1] https://www.ftc.gov/system/files/ftc_gov/pdf/commercial_surveillance_and_data_security_anpr.pdf
[2] Idem, p. 12.

2. The EDPS welcomes this opportunity to provide a contribution based on his role of the EU independent data protection authority responsible under Article 52(2) of Regulation 2018/1725[3] *'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'.*

3. These comments are based on the EU data protection legislation, as well as relevant guidance of the European Data Protection Board ('the EDPB'), established by the General Data Protection Regulation (EU) 2016/679[4] ('the GDPR') of which the EDPS is a member, and draw on the EDPS extensive body of legislative advice and other relevant legislation in force or currently under consideration in the EU.

4. As a general comment, the EDPS welcomes the ANPR and its focus on "commercial surveillance" and data security. The EDPS also follows with keen interest the developments related to the proposed American Data Privacy and Protection Act ("ADPPA"). The EDPS considers that the adoption of a baseline generally applicable data privacy and protection legislation by the US Congress would be welcome and would likely contribute to effectively addressing many of the consumer harms resulting from "commercial surveillance" and lax security practices.

5. The EDPS comments are **structured** according to four 'clusters', which regroup some of the FTC questions. It is important to note in this respect, that many of the questions/answers are **closely intertwined**. On substance, we focussed our attention on:

    - **the principles of purpose limitation and data minimisation**;
    - conditions and limits of data subject's **consent** as ground for processing of personal data and as a safeguard against harmful commercial surveillance;
    - data processing that, due to unacceptable and 'systemic' risks, should be **prohibited** regardless of consent;
    - '**algorithmic harms'**, in particular having regard to **discrimination** and micro-targeting.

[3] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39-98.

[4] 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. 1-88.

For each cluster, we briefly recall the EU data protection principles and rules, accompanied by examples of harmful commercial practices that need to be addressed (including so-called dark patterns and intrusive online behavioural advertising).

1.2 Relevant EU legal framework

6. In the European Union, the rights to privacy and to the protection of personal data are fundamental rights of each and every individual, at 'constitutional level' in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ('the Charter') and Article 16 of the Treaty on the Functioning of the European Union ('TFEU'). They are further implemented by secondary EU laws, including in the commercial domain, by the GDPR and the Directive on privacy and electronic communications ('ePrivacy Directive')[5]. The latter is the main legal instrument of EU law laying down the rules to safeguard the confidentiality of communications, as well as the rules regarding tracking and monitoring including via the use of cookies and similar techniques[6].

7. The EDPS also wishes to draw attention to other recently adopted legislative instruments, as well as to legislative proposals that appear relevant in the present context. These include the recently adopted Digital Markets Act[7] ('the DMA') and

[5] 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. 37–47.

[6] The ePrivacy Directive covers processing of personal data and the protection of privacy including provisions on: the security of networks and services; the confidentiality of communications; access to and storing information on terminal equipment; processing of traffic and location data; calling line identification; public subscriber directories. It also lays down general rules applicable to unsolicited commercial communications ("spam"). Initially, it applied only to publicly available electronic communications services (i.e. internet access provision and telephony services. Since the entry into application of Directive 2018/1972 establishing the European Electronic Communications Code on 20 December 2020, it now applies to all 'interpersonal communications services', i.e. services normally provided for remuneration that enable direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service; this includes also 'number-independent interpersonal communications service' such as instant messaging (apps).

[7] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265, 12.10.2022, p. 1-66. The Regulation will enter into force on the twentieth day following that of its publication in the Official Journal of the European Union and apply from 2 May 2023.

Digital Services Act[8] ('the DSA'), the Proposal for a Regulation on the transparency and targeting of political advertising[9] and the Proposal for AI Act[10] ('the AI Act').

2. Comments

2.1 Concept of personal data; special categories of personal data; data protection principles; conditions for lawful processing of personal data in EU data protection law

8. It is important to highlight that **the concept of personal data** under the GDPR is a broad one[11]. According to Article 4(1) GDPR, personal data means any information relating to an identified or identifiable natural person ("data subject"). This broad definition mirrors the GDPR's aim to protect fundamental rights and freedoms of each individual and in particular their right to the protection of personal data (Article 1(2)). It assumes that no personal data is irrelevant, especially in a commercial surveillance context.

9. **Specific protection** is given in case of information society services[12] directed to a child (Article 8 GDPR) and **special categories** of personal data (as defined in Article 9(1) GDPR)[13]. The processing of special categories of personal data is prohibited in principle. Article 9(2) lays down an exhaustive list of exemptions to this prohibition (i.e. legal grounds for processing that must be met in addition to the legal basis in Article 6, see below).

10. The GDPR provides that the processing of personal data must comply with the principles set out in Article 5. These are the principles of **lawfulness, fairness and transparency**; **purpose limitation**; **data minimisation**; **accuracy**; **storage limitation**; **integrity and confidentiality**; and **accountability**.

---

[8] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, p. 1–102. The Regulation will enter into force on the twentieth day following that of its publication in the Official Journal of the European Union and apply from 17 February 2024.

[9] Proposal for a Regulation of the European Parliament and of the Council on the transparency and targeting of political advertising, COM/2021/731 final.

[10] Proposal for a Regulation of the European Parliament and of the Council of laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM/2021/206 final.

[11] See WP29 Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007.

[12] According to Article 4, point (25) of the GDPR 'information society service' means a service as defined in point (b) of Article 1(1) of Directive 2015/1535 of the European Parliament and of the Council.

[13] "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation". On the notion of special categories of personal data, see the recent judgment of the Court of Justice of 1 August 2022, *Vyriausioji tarnybinės etikos komisija*, C-184/20, ECLI:EU:C:2022:601, paras 117-128.

11. Personal data are processed lawfully only if and to the extent the processing complies with at least one of the **legal basis** listed in Article 6 GDPR[14], and, in case the processing concerns **special categories of personal data**, with the conditions set out in Article 9 GDPR. These requirements apply also when the personal data in question are **publicly available**.

2.2 GDPR legal basis for data processing in the context of the provision of online services

12. The EDPB Guidelines on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of **online services** to data subjects specify that "As a general rule, processing of personal data for **behavioural advertising** is **not necessary** for the **performance of a contract** for online services. Normally, it would be hard to argue that the contract had not been performed because there were no behavioural ads. This is all the more supported by the fact that data subjects have the absolute right under Article 21 to object to processing of their data for direct marketing purposes. Further to this, Article 6(1)(b) cannot provide a lawful basis for online behavioural advertising simply because such advertising indirectly funds the provision of the service. Although such processing may support the delivery of a service, this in itself is not sufficient to establish that it is necessary for the performance of the contract at issue."[15]

---

[14] See WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014, which in fact describes the functioning of all the legal basis. See also EDPB Guidelines on consent under Regulation 2016/679; EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects.

[15] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, issued on 8 October 2019, paras. 52-53.
On the conditions and limits of the possibility to invoke Article 6(1)(b) GDPR as legal basis for the processing of personal data in the context of the provision of online services, see the Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR, adopted on 28 July 2022, paras. 80-99; the same decision is also relevant having regard to the conditions and limits of the possibility to invoke Article 6(1)(f) GDPR, see in particular para. 132: "*Considering the EDPB's conclusion in paragraphs 118-119 and, especially, 131 above, it is the view of the EDPB that Meta IE could not rely on Article 6(1)(f) GDPR for the contact information processing since the processing was either unnecessary or, if it were to be considered necessary, it did not pass the balancing test.*"
On the **legal basis** for the processing of personal data, see also the Binding Decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, adopted on 28 July 2021, para. 59 in particular, in connection with the obligation to provide information where personal data are collected from the data subject pursuant to Article 13 GDPR.
See also the Opinion of the Advocate General Rantos, 20 September 2022, *Meta Platforms Inc., formerly Facebook Inc., Meta Platforms Ireland Limited, formerly Facebook Ireland Ltd., Facebook Deutschland GmbH v Bundeskartellamt*, Case C-252/21, ECLI:EU:C:2022:704, paras. 54-57 (on Article 6(1)(b) GDPR), paras. 58-66 (on Article 6(1)(f) GDPR), and paras. 51 and 52 "[..] *the processing envisaged by the provisions cited is carried out, in the present case, on the basis of the general conditions of contract imposed by the controller, in the absence of the consent of the data subject, or even against his or her will, which, in my opinion, calls for a strict interpretation of the grounds in question, particularly in order to avoid any circumvention of the requirement for consent. 52. Lastly, I would point out that, under Article 5(2) of the GDPR, the controller is responsible for demonstrating that the personal data are processed in accordance with the regulation. Moreover, under Article 13(1)(c) of that regulation,*

13. The EDPB also notes that, in line with ePrivacy requirements, controllers must obtain data subjects' prior consent to place the cookies necessary to engage in behavioural advertising[16].

14. Therefore, a commercial surveillance practice consisting in behavioural advertising whereby the controller relies on Article 6(1)(b) GDPR as legal basis would not be in compliance with the GDPR.

2.3 Security of processing (*reference to FTC question 35)*

15. **Personal data security** is one of the main principles of the GDPR. Lack of appropriate personal data security both at the early stages of design and development of data processing activities, and at the operational stage of the processing, might have adverse impact for the rights and freedoms of individuals[17].

16. It is important to stress that the security of processing under the GDPR is not limited to the storage limitation[18]: appropriate technical and organizational measures must be implemented for the ongoing storage and use of personal data to safeguard the rights and freedoms of the data subject.

17. A **data protection impact assessment**, to be performed by the controller both at the moment of the design of the processing activities and at the time of actual processing[19], to ensure that the risks for the rights and freedoms of individuals have been assessed and properly mitigated, is key.

18. The GDPR indicates encryption and pseudonymisation as important measures to mitigate data security risks. Security of processing is also relevant in the context of transfers of personal data to third countries.

2.4 Purpose limitation and data minimisation

2.4.1 Principle of purpose limitation in EU data protection law (*reference to FTC questions 43-45)*

19. Pursuant to **Article 8(2)** of the Charter, personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. This principle is also laid down in **Article 5(1)(b)** GDPR which stipulates that personal data must be collected for specified,

---

it is for the controller to specify the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing."

[16] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, issued on 8 October 2019, para. 55.

[17] See Article 25 GDPR, Data protection by design and by default; Article 32, Security of processing; recitals 75 and 78. Having regard to the obligations laid down in Article 32 GDPR, see also ISO/IEC 27001 international standard, which addresses the management of information security.

[18] On the 'storage limitation' principle (Article 5(1)(e)), see the recent judgment of the Court of Justice of 20 October 2022, *Digi Távközlési és Szolgáltató Kft.* C-77/21, ECLI:EU:C:2022:805, para. 62.

[19] See Article 35 GDPR, Data protection impact assessment.

explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

20. Purpose limitation plays a key role in the EU data protection law. Honouring data subject's expectations about why their personal data are processed enhances transparency, predictability, legal certainty and, ultimately, contributes to individual**'s trust**. Specifying the purpose of data processing operations is a pre-requisite for applying other **data quality** requirements, including adequacy, relevance, proportionality and accuracy of the data collected and the requirements to ensure that personal data is not retained longer than necessary for the purpose(s) of processing[20].

21. According to **Article 5(1)(b)** GDPR, personal data must be collected for **specified, explicit and legitimate purposes**. *Specified* should be understood as "sufficiently defined to enable the implementation of any necessary data protection safeguards, and to delimit the scope of the processing operation". For the purpose to be *explicit*¸ it "must be sufficiently unambiguous and clearly expressed". Finally, to be *legitimate*, the purpose must be "interpreted within the context of the processing, which determines the 'reasonable expectations' of the data subject." This last requisite also provides a link to the necessity for the processing to be based on a legal ground (Article 6 GDPR) and to broader legal principles such as non-discrimination.[21]

22. **Further processing** of personal data for purposes other than those for which they were initially collected are allowed **only where the processing is compatible with the purposes for which the personal data were initially collected** (Article 5(1)(b) and Recital (50)). Article 5(1)(b) also states that "further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes."

23. In order to determine the compatibility of further processing, **Article 6(4)** GDPR, as specified by Recital (50), presents a **compatibility test**. The controller after having met all the requirements for the lawfulness of the original processing, should take into account, *inter alia*: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations[22].

24. The principle of purpose limitation is one of the basic principles underpinning the GDPR, although certain flexibility has been introduced in Article 6(4), which opens up the possibility to process personal data for a purpose other than that for which it has been collected, under conditions. This approach combines a principled approach with

[20] See Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2 April 2013, p. 4 and 11.
[21] See Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2 April 2013, p. 12.
[22] See the recent judgment of the Court of Justice of 20 October 2022, *Digi Távközlési és Szolgáltató Kft.* C-77/21, ECLI:EU:C:2022:805, paras 24-45.

a degree of flexibility that might be required in today's technological landscape, where it is not always possible to predict with absolute certainty all of the purposes for which personal data could usefully be processed in the future.

2.4.2 **Purpose limitation and data minimisation in the context of development of AI systems** (*reference to FTC question 48*)

25. The EDPS is aware of the claim that full compliance with purpose specification and data minimisation might be not feasible in the context of **artificial intelligence**. The argument is often made that **it is not possible to exactly predict all the purposes for future use** of data.

26. In this regard, the EDPS observes, that, depending on the specific context, there are techniques that organisations might be able to adopt in order to develop AI systems to process **as little personal data as possible**, while still remaining functional (e.g. through **privacy-enhancing technologies including** differential privacy or the use of synthetic data)[23]. Secondly, and more fundamentally, the fact that some data might later in the process be found to be useful for making predictions does not mean its processing is also necessary. For example, the processing of data from social media to assess the health risks or the creditworthiness of individuals is unlikely to be a compatible purpose under EU data protection law[24].

27. Finally, it is important to recall that also in the context of development of AI systems, the processing of personal data must be **lawful, fair and transparent**[25].

2.4.3 **Data minimisation and security of processing** (*reference to FTC questions 47)*

28. The principle of **data minimisation**, laid down in **Article 5(1)(c)**, which provides that personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, is **also crucial for data security**. When companies collect **more personal data than necessary** (often not immediately used, but only kept for future ventures), the chances and severity of potential security incidents increase.

---

[23] On synthetic data, see EDPS IPEN Webinar 2021 - "Synthetic data: what use cases as a privacy enhancing technology?"

[24] See EDPS Opinion 11/2021 on the Proposal for a Directive on consumer credits, 26 August 2021

[25] The EDPS notes with interest that the FTC has recently applied the 'AI disgorgement' remedy (enforcement measure requiring organizations to delete machine learning models and algorithms developed with unlawfully processed data) as response to unfair data processing in the context of the development of AI systems. As part of the settlement with the FTC, Everalbum, Inc. was required to delete the models and algorithms it developed by using the photos and videos uploaded by its users, https://www.ftc.gov/news-events/news/press-releases/2021/05/ftc-finalizes-settlement-photo-app-developer-related-misuse-facial-recognition-technology

29. The EDPB Guidelines on **data protection by design and by default**[26] make this point very clear: controllers should consider both the volume of personal data, as well as the types, categories and level of detail of personal data required for the processing purposes. The design choices related to the data processing should take into account the risks to integrity and confidentiality triggered by the processing of personal data, and the **reduction in risks** when collecting **smaller amounts** and/or **less detailed information** about data subjects.

30. Compliance with data minimization prevents massive collection and processing of personal data, thus decreasing the data security risks (for the rights and freedoms of individuals), in particular in case of personal **data breaches** (e.g. by an insider, by hackers).

31. Pseudonymisation is an important **security control measure**. When assessing cases of personal data breaches, pseudonymisation can contribute to reduce the severity of the impact of the data breach on the person concerned.

2.4.4 Purpose limitation and data minimisation in the context of the 'internet of things' (IoT) and 'internet of bodies' (IoB) (*reference to FTC questions 10 12, 38, in addition to questions 43-47*)

32. A current example of the **importance of data minimisation** is the processing of data related to **connected objects**. The EDPB and the EDPS stressed that, in compliance with the key principle of data minimisation, connected products should be designed in such a way that data subjects are offered the possibility to use devices anonymously and in the least privacy-intrusive way as possible[27]. This is also due to the increased risk of profiling of individuals on the basis of health-related data and biometric data, posed by Internet of Things (IoT) and by Internet of Bodies (IoB).

33. The EDPS also considers, in line with the prohibition of targeted advertising on the basis of special categories of personal data established in the DSA[28], that personal data from IoB (e.g., smartwatches) should not be used for behavioural advertising.

2.4.5 Purpose limitation and data minimisation in the context of the provision of online services

[26] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 20 October 2020, see para. 85 on the security aspects.
See also ENISA publication on "Data Protection Engineering", 27 January 2022. This is the most recent publication from an EU body on data protection engineering and PETs. It illustrates the whole set of available PETs.
[27] EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), 4 May 2022, para. 47.
[28] See at Section 2.6.

34. The EDPB Guidelines on the processing of personal data under Article 6(1)(b)[29] GDPR in the context of the provision of **online services** to data subjects specify that "both **purpose limitation** and **data minimisation** principles are particularly relevant in contracts for online services, which typically are not negotiated on an individual basis. Technological advancements make it possible for controllers to easily collect and process more personal data than ever before. As a result, there is an acute risk that data controllers may seek to include general processing terms in contracts in order to **maximise the possible collection and uses of data**, without adequately specifying those purposes or considering data minimisation obligations."[30] Hence, the assessment on compliance with Article 5(1)(b), providing for the purpose limitation principle, as well as with Article 5(1)(c), providing for data minimisation, are of paramount importance in the context of the provisions of online services.

2.5 Effectiveness of data subject's consent (*reference to FTC questions 73-77*)

2.5.1 Consent as (one of the) legal basis for the processing of personal data under the GDPR

35. As already highlighted above, under Article 6 the GDPR lays down six **legal basis** for processing of personal data[31]. The first basis for a lawful data processing listed in Article 6(1) GDPR is **consent**. Consent is the main materialization, in data protection laws, of individual autonomy and the concept of "informational self-determination". For this reason, consent can only be effective and will only be appropriate if a data subject is offered control and a genuine choice with regard to accepting or declining the terms offered or declining them without detriment[32].

36. Article 4(11) GDPR defines **consent** as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

37. As stated above, the element of "**freely given**" implies that data subjects have a choice and are also allowed to withdraw their consent without detriment at any time (Article 7(3) and recital (42) GDPR). When there is a **clear imbalance** between the data subject and the controller or when consent is not granular enough, for example, it should not be considered valid (recital (43) GDPR) and another appropriate legal basis should be used, if applicable. In the same vein, Article 7(4) GDPR highlights that, when assessing whether consent is freely given, utmost account must be taken of whether,

---

[29] "*processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*". Having regard to Article 6(1)(b), rather than Article 6(1)(a), consent of the data subject, as GDPR legal basis, see Section 2.2.

[30] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, issued on 8 October 2019, para. 16.

[31] See at Section 2.1 of these comments.

[32] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, 4 May 2020, para. 3.

inter alia, consent is "bundled" with the acceptance of a contract, when the processing of the data is not necessary for its performance.

38. The "**specific**" requirement is **closely linked to the purpose limitation principle** and the need for granularity. Consent must always be **related to a specific processing purpose**. This is an important "safeguard against the gradual widening or blurring of purposes for which data is processed, after a data subject has agreed to the initial collection of the data."[33]

39. Consent must also be "**informed**", which means that data subjects must understand what they are agreeing to. Transparency duties by data controllers, laid down in Articles 12-14 GDPR, are essential to provide data subjects with the adequate information to take decisions in relation to their personal data.

40. Finally, consent must be "**unambiguous**", i.e. it should be given by a clear affirmative action, such as by a written statement, including by electronic means, or an oral statement[34].

41. Against this background, the EDPS points out to **commercial surveillance practices that undermine the validity of consent** (the so called "dark patterns") or otherwise, due to the **systemic and pervasive nature of online surveillance** (online behavioural advertising), make data subject's consent not effective and not meaningful, as detailed below.

2.5.2 "Dark patterns" as a harmful commercial practice undermining the validity of consent (freely given, specific, informed, and unambiguous) (*reference to FTC question 73, 75, 76*)

42. It is a matter of concern for the EDPS, that the advertising-driven business model prevailing on the internet allows for an **increasingly opaque and pervasive data collection and processing, including profiling, of individuals**. In this context, consent is often used not as a means to materialize data subject's control, but as a *carte blanche* to legitimise data processing which is not in accordance to the principles and the controller's obligations laid down in the GDPR. In particular, **deceptive practices** such as the use of the so-called **dark patterns** are not aligned with the fairness principle. This is an "overarching principle which requires that personal data should not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data subject"[35].

43. "Dark patterns" may be defined as **interfaces and user experiences that lead data subjects into making unintended, unwilling and potentially harmful decisions regarding the processing of their personal data**. Their aim is to influence users' behaviour, what can hinder their ability to effectively protect their personal data and

[33] *Idem*, para. 56.
[34] Recital (32) GDPR.
[35] EDPB Guidelines 4/20219 on Article 25 Data Protection by Design and by Default, 20 October 2020, para. 69.

make conscious choices.[36] The design of users' interface plays a key role. We also point out to different dark patterns' strategies, such as displaying buttons of different colours/sizes, elements that are difficult to click-on, confusing language, *etc.*

44. "Dark patterns" represent **a violation of the data subject's autonomy** in order to maximise attention and profit, in particular when it comes to children and vulnerable people. Although a topic much discussed in the consumer protection area, the implications they have on the right to data protection are clear. They could **manipulate** people to provide more data than necessary, to give consent when otherwise they would not have given, as well as make it difficult to cancel a registration, etc. The use of dark patterns therefore violates the principles that personal data must be processed fairly and in a transparent manner in relation to the data subject.

45. In addition to being in breach of the GDPR, these practices are also **expressly prohibited** by the DSA[37]. The DSA aims to contribute to the proper functioning of the internal market for intermediary services by setting out harmonised rules for a safe, predictable and trusted online environment. According to Article 25 of the DSA, as specified under recital 67, providers of online platforms must not design, organise or operate their online interfaces in a way that **deceives, manipulates or otherwise materially distorts or impairs** the ability of recipients of their service to make free and informed decisions.

2.5.3 Effectiveness of data subject's consent in the internet of things scenario *(reference to FTC questions 73-74, 84)*

46. The EDPS notes that effective and meaningful consent is challenged by the current internet of things ('IoT') scenario[38]. The concerns expressed by the EDPS on the collection and use of personal data for a purpose that is different from the one of the original collection (for instance, of data from a fitness-app for non-health-related purpose) are hence justified not only by the possible high risks posed by the data processing, but also by the fact that **providing consent in the IoT context is often**

[36] EDPB Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them, 14 March 2022, para. 3. A commercial surveillance practice that is particularly problematic, due to the intrusiveness as well as since it jeopardises the quality of the user's consent, is **cross-device tracking**. In this regard, see EDPB Guidelines 8/2020 on the targeting of social media users, 13 April 2021, para. 27, 56, 77, example no. 8 at p. 24, para 86.

[37] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, p. 1–102.
On the issue of dark patterns, the EDPS welcomes the recent FTC report "Bringing Dark Patterns to Light", September 2022. The Report refers to the term "dark patterns" to describe design practices that trick or manipulate users into making choices they would not otherwise have made. These choices relate to a variety of industries and contexts, including ecommerce. However, section IV of the Report focusses on design elements that obscure or subvert privacy choices (see at pages 15-19). The EDPS considers that a fruitful discussion might take place in this regard to enhance the level of data protection for persons concerned on both sides of the Atlantic.

[38] See Article 29 Data Protection Working Party Opinion 8/2014 on the recent developments on the internet of things, 16 September 2014, Section 2.2, p. 7.

challenging. It is therefore important that data from IoT is only used for **purposes** that are compatible with the original purpose of the processing and that these purposes are all known to the persons concerned.

47. An important requirement for consent, as explained above, is that it must be **informed**. Providing information to users **prior to obtaining their consent** is essential in order to enable them to make informed decisions, understand what they are agreeing to and to exercise their right to withdraw their consent. However, the 'IoT concept' encompasses a wide variety of devices (from doorbell cameras to smart lightbulbs), many of which **not having the graphical interfaces normally found on computers or smartphones**. Hence, users need to retrieve information about the data processing **from other media** (*e.g.* product's website). While this practice might be considered in accordance to Article 12(1) GDPR, which states that "[*t*]*he information shall be provided in writing, or by other means, including, where appropriate, by electronic means"*, it should be taken into account that, and increasingly so, IoT devices are designed to be **seamless** to use, often abstracting the user from the underlying data processing.

48. Nonetheless, the design of **user-friendly and easy to use devices** should not collide with proper, and clear, information about the data processing taking place. Aside from providing information in the product package, manufacturers should make sure that users can access such information if the package is no longer available (for instance, by printing a QR-code in the body of the device with an hyperlink to the privacy policy of the product)[39].

49. Concerning the IoT devices, it is also important to recall that it is not allowed to track users' behaviour and activities without their knowledge and consent. In this context, the EDPS recalls that the ePrivacy Directive seeks to ensure that users' activities are not monitored without their consent. **Article 5(3) of the ePrivacy Directive** is applicable in as much as IoT devices qualify as "terminal equipment" under the ePrivacy Directive. Article 5(3) provides that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is **only allowed on condition that the subscriber or user concerned has given his or her consent**, having been provided with clear and comprehensive information, in accordance with the GDPR, *inter alia*, about the purposes of the processing. However, the consent requirement does not apply in case of technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.[40]

---

[39] See Article 29 Data Protection Working Party, "Guidelines on Transparency under Regulation 2016/679", wp260rev.01, 11 April 2018 (later endorsed by the EDPB), p. 21, on the 'layered approach', 'other types of appropriate measures'.

[40] On the applicability of the ePrivacy Directive in the context of IoT, see: Article 29 Data Protection Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 September 2014, p. 14; EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019, p.13; EDPB

2.6 **Prohibitions** *(reference to FTC questions 41, 42, 25, 75, 76, 73-74, and on personalised advertising to **children**, question 21)*

50. Examples of **commercial surveillance practices** that, in the view of the EDPS, should be prohibited **regardless of end-users' consent**, relate to **online targeted advertising**.

51. The EDPS considers that online **behavioural** advertising should be regulated more strictly in favour of less intrusive forms of advertising that do not require tracking of users' interaction with content, notably **contextual** advertising (*reference to FTC questions 41 and 42*). The DSA is a first step towards this goal, since it lays down **a ban on advertising based on profiling using special categories of data** and **minor's data**[41].

52. This consideration is underpinned, having regard to user's consent, by **systemic issues** of endemic commercial surveillance and power asymmetries **which cannot be addressed by the end-user**, also taking into account the well-known phenomenon of '*consent fatigue*'[42].

53. Moreover, in some cases, for instance having regard to the use of advertising technologies directed to **children**, the harmful effect of commercial surveillance might be considered higher due to the vulnerability of the data subject. Recital (38) of the GDPR specifies that "[c]hildren merit specific protection with regard to their

---

Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0 Adopted on 9 March 2021, p. 7, specifying that "*Since the controller, when seeking consent for the storing or gaining of access to information pursuant to art. 5(3) ePrivacy directive, will have to inform the data subject about all the purposes of the processing – including any processing following the aforementioned operations (meaning the "subsequent processing") – consent under art. 6 GDPR will generally be the most adequate legal basis to cover the processing of personal data following such operations [..]. Hence, consent will likely constitute the legal basis both for the storing and gaining of access to information already stored and the subsequent processing of personal data.*"

[41] See Article 26(3): "*Providers of online platforms shall not present advertising to recipients of services based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using special categories of personal data as referred to in Article 9(1) of Regulation (EU) 2016/679.*"; and, specifically on minors' data, Article 28: *"Online protection of minors:*
1. Providers of online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service.
2. Providers of online platform shall not present advertising on their interface based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor.
3. Compliance with the obligations set out in this Article shall not oblige providers of online platforms to process additional personal data in order to assess whether the recipient of the service is a minor.
4. The Commission, after consulting the Board, may issue guidance to assist providers of online platforms in the application of paragraph 1."
On the DSA in relation to AI-driven recommender systems, see at Section 2.7.3 of these comments.

[42] See EDPB Guidelines 05/2020 on consent under Regulation 2016/679, 4 May 2020, para. 87: "*In the digital context, many services need personal data to function, hence, data subjects receive multiple consent requests that need answers through clicks and swipes every day. This may result in a certain degree of click fatigue: when encountered too many times, the actual warning effect of consent mechanisms is diminishing.*"

personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child." This recital specifies the provisions in Article 8 GDPR on conditions applicable to child's consent in relation to information society services.

54. The EDPB Guidelines on the targeting of social media users also highlights that *"[t]argeting can influence the shaping of children's personal preferences and interests, ultimately affecting their autonomy and their right to development.*"[43] The cost-benefits analysis might, therefore, even be superseded by a presumption of unacceptable negative externalities and the paramount necessity to respect the best interests of the child[44] (*reference to FTC question 28).*

55. In a blogpost issued on 14 March 2022 related to the DSA,[45] the EDPS stated: "*Let me be clear: **transparency is essential but it is not enough**. If we are truly serious about tackling the risks that surround online targeted advertising, we will need more than increased transparency. In our Opinion on the Proposal for a Digital Services Act, we advocated for a prohibition of targeted advertising on the basis of pervasive tracking. Alternative models exist, but we need regulatory incentives to favour less intrusive forms of advertising that do not require tracking of user interaction with content. How do we achieve this? At the very least, we should consider further restricting the categories of personal data that can be processed for targeted advertising purposes. Special categories of data or other data that can be used to exploit vulnerabilities should not be used to target ads. Processing of data from vulnerable groups, such as children, can have unexpected results for an entire generation.*"

56. **Other commercial surveillance practices** would be prohibited under EU law under approval having regard to specific services (*reference to FTC question 76).* We refer here in particular to the Proposal for review of the **consumer credit** directive,[46] and to the Proposal for a **platform work** directive.[47]

57. The Proposal for the review of the **consumer credit** directive offers indications on the types of personal data which should not be used to assess creditworthiness. Having regard to this assessment, referred to in Article 18, the Proposal specifies that [emphasis added] "[p]ersonal data, such as personal data **found on social media**

[43] EDPB Guidelines 8/2020 on the targeting of social media users, 13 April 2021, para. 16.
[44] Article 24(2) of the Charter states that *"[i]n all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration*".
[45] Wiewiórowski, W., "It is time to target targeted advertising", 14 March 2022.
[46] Proposal for a Directive of the European Parliament and of the Council on consumer credits, COM/2021/347 final.
[47] Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work, COM/2021/762 final.

platforms or **health data, including cancer data**, should not be used when conducting a creditworthiness assessment."[48]

58. In his Opinion on this legislative proposal,[49] the EDPS recommended **clearly delineating the categories and sources of personal data** that may be used for the purpose of creditworthiness assessment, in order to promote fair access to credit and data protection. In particular, the EDPS invited the legislator to strive for increased consumer protection and harmonisation by clearly specifying the categories of personal data that should and should not be processed. The EDPS also recommended **explicitly prohibiting the use of any special categories of personal data under Article 9(1) GDPR.** Having regard to **advertising and marketing of credit agreements**, the EDPS recommended specifying in the Proposal that the use of personal data collected and processed **in the context of creditworthiness** assessment should **not be allowed for marketing** purposes[50].

59. The proposal for a **platform work** directive provides that digital labour platforms must not process any personal data concerning platform workers that are not intrinsically connected to and strictly necessary for the performance of the contract between the platform worker and the digital labour platform, and specifies certain categories of personal data which must not be processed, namely: (a) any personal data on the **emotional or the psychological state of the platform worker**; b) any personal data relating to the health of the platform worker, except in cases referred to in Article 9(2), points (b) to (j) GDPR; (c) any personal data in relation to **private conversations, including exchanges with platform workers' representatives**; and (d) any personal data in relation to the moment in time **when the platform worker is not offering or performing platform work**[51].

60. In the consultation on this legislative proposal[52], the EDPS welcomed in particular the prohibition to process any personal data **on the emotional or psychological state of the platform worker**.[53]

---

[48] Recital (47); Article 18(2): "*The assessment of creditworthiness shall be carried out on the basis of relevant and accurate information on the consumer's income and expenses and other financial and economic circumstances which is necessary and proportionate such as evidence of income or other sources of repayment, information on financial assets and liabilities, or information on other financial commitments.*"

[49] EDPS Opinion 11/2021 on the Proposal for a Directive on consumer credits, 26 August 2021, see executive summary, at p. 2, paras 14-19 and 43.

[50] EDPS Opinion 11/2021 on the Proposal for a Directive on consumer credits, 26 August 2021, para. 43.

[51] Article 6(5).

[52] EDPS Formal comments on the Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work, 2 February 2022.

[53] EDPS Formal comments on the Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work, 2 February 2022, p. 3.

61. It is also worth recalling that the recently adopted **Digital Markets Act** (DMA)[54] provides a prohibition for "gatekeepers"[55] to track end-users outside of the gatekeepers' core platform service for the purpose of targeted advertising, without effective consent having been granted[56].

62. In this case, the prohibitions and limitations on the processing of personal data in the context of commercial surveillance are due, at the same time, to **data protection** concerns (the invasiveness of the data processing and of users' profiling), as well as to **competition** concerns (the market power stemming from the availability and cross-use of a potentially wide variety and quantity of personal data by undertakings holding a strong economic position)[57].

2.7 Automated decision-making and "algorithmic harm," including discrimination based on protected categories (*reference to FTC questions 53-72*)

2.7.1 Automated individual decision-making, including profiling

63. Article 22 GDPR lays down rules applicable to automated individual decision-making, including "profiling", understood as "any form of automated processing of personal

---

[54] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265, 12.10.2022, p. 1-66.

[55] The DMA establishes a set of objective criteria for qualifying a large online platform as a so-called "gatekeeper" (under Article 3 DMA, designation of gatekeepers). These criteria will be met if a company has a **strong economic position**, significant impact on the internal market and is active in multiple EU countries; has a strong intermediation position, meaning that it links a large user base to a large number of businesses; has (or is about to have) an entrenched and durable position in the market, meaning that it is stable over time if the company met the two criteria above in each of the last three financial years.

[56] See Article 5(2) DMA (emphasis added): "*The gatekeeper shall not do any of the following:*
(a) process, for the purpose of providing online advertising services, personal data of end users ***using services of third parties*** *that make use of core platform services of the gatekeeper;*
(b) combine personal data from the relevant core platform service with personal data ***from any further core platform services or from any other services provided by the gatekeeper or with personal data from third-party services****;*
(c) cross-use personal data from the relevant core platform service ***in other services provided separately by the gatekeeper****, including other core platform services,* ***and vice-versa****; and*
(d) sign in end users ***to other services of the gatekeeper*** *in order to combine personal data,*
unless the end user has been presented with the specific choice and has given consent within the meaning of Article 4, point (11), and Article 7 of Regulation (EU) 2016/679.
Where the consent given for the purposes of the first subparagraph has been refused or withdrawn by the end user, the gatekeeper shall not repeat its request for consent for the same purpose more than once within a period of one year.
This paragraph is without prejudice to the possibility for the gatekeeper to rely on Article 6(1), points (c), (d) and (e) of Regulation (EU) 2016/679, where applicable."

[57] See EDPS Opinion 2/2021 on the Proposal for a Digital Markets Act, issued on 10 February 2021, para. 23: "*The EDPS welcomes this provision, as it both helps to address competition concerns and further strengthens the protection of the fundamental rights to privacy and to the protection of personal data in relation to gatekeepers.*"; see also para. 12: "*Already in 2014, the EDPS pointed out how competition, consumer protection and data protection law are three inextricably linked policy areas in the context of the online platform economy. The EDPS considers that the relationship between these three areas should be a relationship of complementarity, convergence and coherent application, not a relationship where one area replaces or enters into friction with another.*"

data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements"[58].

64. Pursuant to Article 22(1), GDPR stipulates that the data subject has the right not to be subject to a **decision based solely on automated processing, including profiling**, which produces legal effects or similarly significantly affects him or her.

65. Article 22(2) provides exceptions to the rule, which should be accompanied by safeguards to protect data subject's rights and freedoms and legitimate interests. These safeguards include the right **to obtain human intervention** on the part of the controller, the right for the data subject **to express their point of view** and to **contest the decision** (Article 22(3)), as well as **to obtain an explanation of the decision** reached after such assessment (as specified by Recital (71)).

66. Automated decision-making often involves profiling. According to the WP29's guidelines on automated individual decision-making and profiling "profiling is composed of three elements: it has to be an **automated form of processing;** it has to be **carried out on personal data;** and **the objective of the profiling must be to evaluate personal aspects about a natural person**. [..] Broadly speaking, profiling means gathering information about an individual (or group of individuals) and evaluating their characteristics or behaviour patterns in order to place them into a certain category or group, in particular to analyse and/or make predictions about, for instance, their: ability to perform a task; interests; or likely behaviour."[59] These Guidelines highlight in particular the risk of discrimination stemming from profiling[60].

2.7.2 Risks stemming from the use of Artificial Intelligence technology

67. The use of AI is likely to introduce **a higher level of complexity** into **profiling and automated decision-making practices**. In particular, the "algorithmic error" might become more difficult to discern and the risks for fundamental rights and freedoms may become high or even unacceptable.

---

[58] Article 4, definition (4), of the GDPR.

[59] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 22 August 2018, p. 8. These Guidelines were endorsed by the EDPB (European Data Protection Board, Endorsement of GDPR WP29 guidelines by the EDPB, 25 May 2018).

[60] See for instance at p. 5 "*Profiling can perpetuate existing stereotypes and social segregation. It can also lock a person into a specific category and restrict them to their suggested preferences. This can undermine their freedom to choose, for example, certain products or services such as books, music or newsfeeds. In some cases, profiling can lead to inaccurate predictions. In other cases it can lead to denial of services and goods and unjustified discrimination.*"; see examples provided in the boxes at p. 10.

68. **Artificial Intelligence (AI)**[61] **technologies** present a number of specific challenges, in particular related to **making predictions and taking automated decisions based on inferences**.

69. As these activities are often carried out based on probabilistic analysis and correlations, our ability to provide causal interpretation to outcomes can be affected in a way that transparency, human control, accountability and liability over results will be severely challenged[62].

70. Since personal data are in many cases in the centre of these decisions, AI systems often intrinsically affect data subject's rights to privacy and to the protection of personal data. But not only that. Several other fundamental rights are also affected, such as the right to non-discrimination, freedom of expression, and freedom of movement. In a collective perspective, these systems can help promoting political and ideological polarisation, disinformation and manipulation and, as a result, even democracy can be endangered[63].

71. The **Proposal for AI Act** provides that certain particularly harmful AI practices are **prohibited** as contravening Union values. The prohibition[64] (if adopted) would cover practices that have a significant potential to **manipulate** persons through **subliminal techniques** beyond their consciousness or exploit vulnerabilities of specific vulnerable groups in order to materially distort their behaviour in a manner that is likely to cause them or another person psychological or physical harm.

72. The Proposal for AI Act also prohibits AI-based **social scoring** for general purposes done by public authorities. Finally, **the use of 'real time' remote biometric identification systems in publicly accessible spaces** for the purpose of law enforcement is also prohibited unless certain limited exceptions apply.

73. In the Joint Opinion on the AI Act, the EDPS and the EDPB consider that these prohibitions are too narrow[65].

---

[61] The proposal for the AI Act defines "AI systems" as "*software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with*" (see Article 3, point (1)).

[62] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), issued on 18 June 2021, para. 3.

[63] See Section 2.7.3.

[64] Title II, *Prohibited artificial intelligence practices*, Article 5, of the Proposal for AI Act.

[65] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, para. 28: "*Article 5 of the Proposal risks paying lip service to the "values" and to the prohibition of AI systems in contrast with such values. Indeed, the criteria referred to under Article 5 to "qualify" the AI systems as prohibited limit the scope of the prohibition to such an extent that it could turn out to be meaningless in practice (e.g. "causes or is likely to cause [...] physical or psychological harm" in Article 5 (1) (a) and (b); limitation to public authorities in Article 5(1)(c); vague wording in and points (i) and (ii) under (c); limitation to "real time" remote biometric identification only without any clear definition etc.).*"

74. Moreover, the EDPS and the EDPB consider that the following AI systems **should also be prohibited**:

- **social scoring**, by public authorities or on their behalf, **as well as by private companies**[66];

- any use of AI for automated recognition of human features in publicly accessible spaces, such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals;[67]

- AI systems **categorizing individuals from biometrics** (for instance, from face or voice recognition) **into clusters according to ethnicity, gender, as well as political or sexual orientation, or other grounds for discrimination prohibited under Article 21 of the Charter** (**biometric categorization** systems)[68];

- AI systems inferring "emotions" of natural persons (so-called **emotion categorization systems**), except for well-specified use-cases, namely for health or research purposes with appropriate safeguards in place and subject to all data protection conditions and limits, including purpose limitation[69].

75. Most of these AI systems could indeed be used for or in the context of **commercial surveillance**. Hence, the red-lines highlighted in the Joint Opinion concern **unacceptable (AI-based) commercial surveillance**, also taking into account population(group)-level harms caused by data-driven industries, power imbalances in the data ecosystem, and structural issues (such as 'stereotyping' according to ethnicity, or other grounds for discrimination).

76. Having regard to high-risk AI systems, the Proposal for AI Act provides that these systems should be accompanied by relevant documentation and instructions of use and include concise and clear information, **including in relation to possible risks to fundamental rights and discrimination**, where appropriate.

77. However, the EDPS is aware that **tackling discrimination** is a complex issue that requires in-depth assessment of **all different stages** of the 'AI life-cycle' (design,

---

[66] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, para. 29.

[67] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, para. 32.

[68] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, para. 33.

[69] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, para. 35.
See also EDPS Opinion on the Recommendation for a Council Decision authorising the opening of negotiations on behalf of the European Union for a Council of Europe convention on artificial intelligence, human rights, democracy and the rule of law, 13 October 2022, paras. 34-36.

development and application of AI systems), and strengthening the mitigation of bias **from the first stages** of the AI development process[70].

78. **Audit** in this regard is also essential. In the Joint Opinion on the AI Act, the EDPS recommended *ex ante* and **third party** audit of the high-risk AI systems[71].

2.7.3 Risks related to the use of recommender systems and online micro-targeting

79. The prevailing **advertising-driven business model** makes vast use of online recommender systems - increasingly relying on **artificial intelligence** systems - and has been instrumental in provoking such harms.

80. The EDPS has considered this issue with the utmost attention. In the Opinion on **online manipulation and personal data**[72], the EDPS identified several risks and harms resulting from how personal data is used to determine the online experience. The design of digital services provided by very large online platforms is generally optimised to benefit advertising-driven business models and can cause societal concerns. In particular, the Opinion highlighted how the existing business models behind many online services has contributed to increased political and ideological polarisation, disinformation and manipulation.

81. The DSA aims at ensuring, having regard to the provision of digital services in the internal market, online safety and the protection of fundamental rights, and to set a governance structure for the supervision of providers of intermediary services. To this end, the DSA contains provisions on the exemption of liability of providers of intermediary services; sets out "due diligence obligations", adapted to the type and nature of the intermediary service concerned; and contains provisions concerning implementation and enforcement. The DSA recognises in particular the risks resulting from the use of **algorithmic systems** as regards their potential for amplifying certain

[70] A useful assessment tool is provided by the European Law Institute (ELI) Model Rules on Impact Assessment of Algorithmic Decision-Making Systems Used by Public Administration ('Model Rules'). These Model Rules provide for an impact assessment of those algorithmic decision-making systems used by public authorities which are likely to have significant impacts on the public. Though tailored to public administrations, the Model Rules provide a methodology and a set of questions that are in most cases also applicable in case of use of algorithmic decision-making systems by private entities.

[71] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, para. 37.
See also EPRS, "*Auditing the quality of datasets used in algorithmic decision-making systems*", July 2022.

[72] EDPS Opinion 3/2018 on online manipulation and personal data, issued on 19 March 2018, see at p. 12 on the use of AI in this context: "*Artificial Intelligence is used for fine-grained surveillance, to monitor, filter, and censor messages sent between users of messaging applications. Machine-learning algorithms aim to maximise attention and likes, making media susceptible to manipulation. Social media bots which distort news or foment anger or dissent may be autonomous or controlled by humans. More sophisticated applications of Artificial Intelligence, like deep-fakes, speech simulation and automated news reporting, are likely to increase with its potency in this ecosystem as they become cheaper to deploy, unless countermeasures are deployed successfully.*"

content, including disinformation, and contains provisions, related to **transparency of recommender systems**[73], aiming at reducing such risks.

82. In the Opinion on the Proposal[74], the EDPS welcomed the DSA, since it seeks to promote a transparent and safe online environment. In his Opinion, the EDPS recommends **additional measures** to better protect individuals when it comes to content moderation, online targeted advertising and recommender systems used by online platforms, such as social media and marketplaces.

83. The EDPS highlighted among others that the legislator should consider a ban on online targeted advertising based on pervasive tracking and restrict the categories of data that can be processed for such advertising methods. In accordance with the requirements of data protection by design and by default, **recommender systems** should by default not be based on profiling.

84. The **Proposal for a Regulation on the transparency and targeting of political advertising**[75] provides specific rules on **political** advertising services. Such rules concern, in particular, **transparency obligations** addressed to the various actors involved in political advertising, as well as **a prohibition of targeting or amplification techniques that involve the processing of special categories of personal data**.[76]

85. In the Opinion on the Proposal[77], the EDPS welcomed the overarching aims of the proposed Regulation. Nonetheless, the EDPS recommended to consider **stricter rules** concerning online targeted advertising for political purposes, in addition to the proposed measures to make this type of advertising more transparent.

86. In particular, the EDPS recommended a **full ban on micro-targeting for political purposes**, which consists of targeting an individual or a small group of individuals

---

[73] Article 27, Recommender system transparency:
"*1. Providers of online platforms that use recommender systems shall set out in their terms and conditions, in plain and intelligible language, the main parameters used in their recommender systems, as well as any options for the recipients of the service to modify or influence those main parameters.*
2. The main parameters referred to in paragraph 1 shall explain why certain information is suggested to the recipient of the service. They shall include, at least:
a) the criteria which are most significant in determining the information suggested to the recipient of the service; (b) the reasons for the relative importance of those parameters.
3. Where several options are available pursuant to paragraph 1 for recommender systems that determine the relative order of information presented to recipients of the service, providers of online platforms shall also make available a functionality that allows the recipient of the service to select and to modify at any time their preferred option. That functionality shall be directly and easily accessible from the specific section of the online platform's online interface where the information is being prioritised."
[74] EDPS Opinion 1/2021 on the Proposal for a Digital Services Act, issued on 10 January 2021.
[75] Proposal for a Regulation of the European Parliament and of the Council on the transparency and targeting of political advertising, COM/2021/731 final.
[76] See Article 12(1) on the prohibition of processing of special categories of personal data; see in particular Article 12(3) and Annex II on the transparency requirements (information to be provided in the context of political advertising).
[77] EDPS Opinion 2/2022 on the Proposal for Regulation on the transparency and targeting of political advertising, issued on 20 January 2022.

with political messages according to some of their perceived preferences or interests that their online behaviour may reveal.

87. The EDPS also considered that **further restrictions should be put in place concerning the categories of personal data** that may or may not be processed for the purpose of political advertising, including when political advertising involves the use of targeting and amplification techniques. Specifically, the use of targeted advertising based on pervasive tracking for political purposes should be prohibited.

Brussels, 18 November 2022

[e-signed]
Wojciech Rafał WIEWIÓROWSKI