European Commission

EDPB European Data Protection Board

Joint Guidelines

on the

Interplay between the Digital Markets Act and the General Data Protection Regulation

Version for public consultation

Executive summary

The Digital Markets Act (DMA) and the General Data Protection Regulation (GDPR) pursue different purposes and objectives and have different scopes. While the GDPR aims to protect natural persons with regard to the processing of personal data and ensure the free flow of personal data in the Union covering all data controllers and processors, the DMA aims to tackle unfair practices, and their potential harmful effects for business users, by laying down harmonised rules applicable to gatekeepers ensuring, for all businesses, contestable and fair markets in the digital sector across the Union, to the benefit of both business users and end users.

The DMA and GDPR are complementary in terms of goals and in terms of the protections provided to individuals. Compliance with obligations under the GDPR goes together with the objective of addressing gatekeepers' data-driven advantages that the DMA, among other objectives, aims to tackle.

On 10 September 2024, the European Data Protection Board and the European Commission announced that they would work on joint guidance on the interplay between the DMA and the GDPR, which they would adopt pursuant to their respective legal bases under the GDPR and the DMA. This initiative is aligned with Pillar 3 of the EDPB Strategy 2024-2027, 'Safeguarding data protection in the developing digital and cross-regulatory landscape', in which the EDPB committed to promote consistency and cooperation with competent authorities in fields other than Union data protection law.

These Guidelines on the interplay between the DMA and the GDPR aim to ensure that the DMA and the GDPR are interpreted and applied in a compatible manner, enabling a coherent application that achieves their respective objectives, in line with relevant CJEU case law. A consistent and coherent interpretation of the DMA and the GDPR should mutually reinforce and maximise the achievement of the respective objectives of the two frameworks, while fully respecting the protection of the fundamental right to data protection as enshrined in Union law.

The Guidelines do not aim to exhaustively address all instances where issues of GDPR application may arise in the context of the implementation of the DMA by gatekeepers. Instead, the Guidelines focus on those provisions of the DMA in relation to which there are significant overlaps with substantive rules stemming from the GDPR that merit clarification and a common interpretation among the authorities that are competent to supervise each framework.

Article 5(2) DMA prohibits gatekeepers from carrying out certain processing operations without end users' valid consent, within the meaning of the GDPR. The Guidelines explain the elements that gatekeepers should consider in order to comply with the requirements of specific choice and valid consent under Article 5(2) DMA and the GDPR. The Guidelines also describe circumstances where consent may not be required by either the GDPR or the DMA and under which conditions other legal bases can be relied upon (e.g. the possibility of relying on Article 6(1), point (c) GDPR when processing personal data for security purposes, provided certain conditions are met).

Article 6(4) DMA requires gatekeepers providing operating system CPS to (inter alia) allow and technically enable the installation and effective use of third-party software applications or software application stores on their operating system. The Guidelines recall that gatekeepers should ensure that the measures they implement in compliance with Article 6(4) DMA also comply with applicable laws, including the GDPR and the ePrivacy Directive. However, when selecting appropriate measures to comply with obligations stemming from the GDPR, gatekeepers should select the measures that less adversely affect the pursuit of the objectives of

DRAFT

Article 6(4) DMA, provided that they remain effective in ensuring compliance with the GDPR, also taking into account that operating system providers are generally considered separate and independent controllers from the providers of apps or app stores. The Guidelines provide examples of measures that gatekeepers are expected to take to comply with their own GDPR obligations in the context of Article 6(4) DMA.

Article 6(9) DMA creates a right to data portability at the request of end users or third parties authorised by end users. The Guidelines explain how this right complements Article 20 GDPR, given its broad scope, and elaborates on key GDPR requirements applicable to DMA portability requests. The principal areas examined relate to the portability of personal data of individuals other than the end user, the authentication of end users and verification of the authorisation obtained by third parties, and transfers of personal data to third parties that are in non-EEA countries without an adequacy decision.

Article 6(10) DMA creates a right of data access for business users and authorised third parties, including to personal data of end users engaging with the products or services provided by those business users through the gatekeeper's core platform service. The Guidelines explain the practical implications of business users having to collect end users' consent for such access, how gatekeepers should facilitate the collection and withdrawal of such consent, as well as inform end users about the separate controllers to whom their personal data is shared with pursuant to Article 6(10) DMA.

Article 6(11) DMA establishes an obligation for gatekeepers to provide to any third-party undertaking providing online search engines with access to ranking, query, click and view data in relation to search generated by end users on its online search engines. The shared data that constitutes personal data has to be anonymised. The Guidelines clarify the objective of Article 6(11) DMA to foster contestability in the online search engine market and how to achieve effective anonymisation of shared search data while taking into account such objectives.

Article 7 DMA requires gatekeepers designated in relation to their number-independent interpersonal communications services to offer interoperability to alternative service providers requesting it. The Guidelines elaborate on the requirements of Article 7 that are relevant from the perspective of privacy and data protection law. Most notably, they recall that gatekeepers should comply with data minimisation and other GDPR principles when making their services interoperable, and mention necessary, proportionate, and justified measures that a gatekeeper may apply to ensure that third-party service providers requesting interoperability do not endanger the integrity, security and privacy of its services.

The Guidelines also pronounce on coordination, cooperation and consultation between the European Commission as sole enforcer of the DMA and competent data protection supervisory authorities as enforcers of the GDPR. The Guidelines recall, with reference to relevant CJEU case law concerning the principle of sincere cooperation and *ne bis in idem*, that cooperation and coordination between the European Commission and data protection supervisory authorities is essential to ensure a consistent, effective and complementary application of the DMA and EU data protection law.

DRAFT

Table of Contents

1 Objective, addressees and scope of the Guidelines 5
2 End-user choice and consent (Article 5(2) DMA) 8
2.1 Specific choice and the requirement for a less personalised but equivalent alternative service under the DMA 10
2.2 Consent within the meaning of the GDPR 11
2.2.1 General conditions 11
2.2.2 Special categories of personal data 12
2.3 Ensuring user-friendly choices and consent designs 13
2.4 Limits to repeating consent requests 15
2.5 Processing activities covered by Article 5(2) DMA 16
2.5.1 Article 5(2), point (a) DMA 16
2.5.2 Article 5(2), point (b) DMA 17
2.5.3 Article 5(2), point (c) DMA 18
2.5.4 Article 5(2), point (d) DMA 18
2.6 Processing not requiring consent under Article 5(2) DMA 19
2.6.1 Cross-use of personal data between gatekeeper services provided together with or in support of each other 19
2.6.2 Processing activities which lawfully rely on Article 6(1), points (c), (d) and (e) GDPR 22
3 Distribution of software application stores and software applications (Article 6(4) DMA) 23
3.1 Measures to ensure compliance with the GDPR principle of integrity and confidentiality in relation to personal data 25
3.2 Other measures gatekeepers should take to comply with the GDPR and facilitate compliance of Article 6(4) DMA beneficiaries with the GDPR 26
4 Right to data portability of end users and third parties authorised by end users (Article 6(9) DMA) 27
4.1 Data categories to which the right to portability under Article 6(9) DMA applies 28
4.2 Portability of other data subjects' personal data 29
4.3 Granularity and duration of portability 30
4.4 Real-time and continuous data access 31
4.5 Online choice architecture 32
4.6 Authorised third parties 32
4.7 Right to portability and international transfers of personal data 34
5 Right to data access of business users and authorised third parties (Article 6(10) DMA) 34

DRAFT

5.1 Categories of beneficiaries of the right to data access 35
5.2 Data categories to which Article 6(10) DMA applies 36
5.3 Granularity of data access under Article 6(10) DMA 37
5.4 Mechanism(s) enabling access to end-user's personal data 38
5.5 Continuous and real-time data access 40
5.6 Online choice architecture 40
6 Access to anonymised ranking, query, click and view data (Article 6(11) DMA) 41
7 Interoperability of number-independent interpersonal communication services (Article 7 DMA) 45
7.1 Categories of personal data necessary to ensure interoperability 47
7.2 Personal data processing to preserve the level of security across interoperable services 48
7.3 Other situations where personal data processing may occur 49
7.3.1 Geographical limitations 49
7.3.2 Measures pursuant to Article 7(9) DMA 50
8 Coordination, cooperation and consultation 51

DRAFT

The European Commission

Having regard to Article 47 of 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, ("DMA")[1],

The European Data Protection Board

Having regard to Article 70(1), point(e) of Regulation 2016/679/EU 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, ("GDPR")[2],

Having regard to the European Economic Area ('EEA Agreement')[3] and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 12 and Article 22 of the Rules of Procedure of the European Data Protection Board,

HAVE ADOPTED THE FOLLOWING GUIDELINES

1 Objective, addressees and scope of the Guidelines

1. The Digital Markets Act (DMA) applies to core platform services (CPSs)[4] provided by specific undertakings designated by the European Commission which serve as important gateways between business users[5] and end users[6] ('gatekeepers').[7]

2. Undertakings that are designated by the European Commission as gatekeepers in accordance with Article 3 DMA may qualify as controllers[8] or processors[9] under the

[1] 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, ELI: http://data.europa.eu/eli/reg/2022/1925/oj).

[2] 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

[3] References to "Member States" made throughout this document should be understood as references to "EEA Member States".

[4] According to Article 2(2) DMA, a 'core platform service' means any of the following: online intermediation services; online search engines; online social networking services; video-sharing platform services; number-independent interpersonal communications services; operating systems; web browsers; virtual assistants; cloud computing services; online advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by an undertaking that provides any of the aforementioned CPS.

[5] Article 2(21) DMA, 'business user' means "*any natural or legal person acting in a commercial or professional capacity using core platform services for the purpose of or in the course of providing goods or services to end users*."

[6] Article 2(20) DMA, 'end user' means "*any natural or legal person using core platform services other than a business user*".

[7] European Commission, *Gatekeepers.*

[8] Article 4(7) GDPR, 'controller' means "*any natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of the personal data; where the purposes and means are determined by Union or Member Stat law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."*

[9] Article 4(8) GDPR, 'processor' means "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*".

DRAFT

GDPR[10] or may have within their corporate structure controllers or processors that process personal data[11] under the GDPR.[12] As a result, both the DMA and the GDPR may cover processing activities carried out by or within the same entities.[13]

3. The DMA and the GDPR pursue different purposes and objectives and have different scopes. While the GDPR aims to protect natural persons with regard to the processing of personal data and ensure the free flow of personal data in the Union covering all data controllers and processors,[14] the DMA aims to tackle the potential harmful effects for business users of unfair practices by laying down harmonised rules applicable to gatekeepers ensuring, for all businesses, contestable and fair markets in the digital sector across the Union, to the benefit of business users and end users.[15] In this context, the DMA acknowledges and seeks to address gatekeepers' data-driven advantages, which include their privileged access to large amounts of end users' personal data.[16]

4. The DMA and GDPR are complementary in terms of goals and in terms of the protections provided, including to the rights of end users who are also 'data subjects' under the GDPR.[17] Greater fairness in and contestability of digital markets lead to more choice for individuals, which in turn should increase incentives for gatekeepers and their business users to develop and implement data protection and privacy features, in line with data protection by design and by default.[18] At the same time, compliance with obligations under the GDPR complements the objective to address gatekeepers' data-driven advantages that the DMA, among others objectives, aims to tackle.

5. Article 8(1) DMA states that gatekeepers have to ensure that the implementation of measures to ensure compliance with their obligations under the DMA also comply with applicable law, including the GDPR and Directive 2002/58/EC of the European Parliament and of the Council ("the ePrivacy Directive").[19] Recital 12 DMA adds that

---

[10] See also EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.1, Adopted on 7 July 2021. The determination of the role of a relevant entity covered by the DMA – be it a gatekeeper, a business user, or a third party – under EU data protection law requires a case-by-case assessment.

[11] Article 4(1) GDPR, 'personal data' means "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*."

[12] By virtue of either Article 3(1) or 3(2) GDPR.

[13] The CJEU has established that an "undertaking", is the single economic entity that "*encompasses every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed*". See judgment of the Court of Justice of 23 April 1991, *Höfner and Elser v Macrotron GmbH*, C-41/90, ECLI:EU:C:1991:161, paragraph 21. Processing activities that are regulated by the GDPR may therefore, in some circumstances, be carried out by data controllers that constitute part of an undertaking that has been designated as a gatekeeper for the purposes of the DMA.

[14] Article 1(1) GDPR.

[15] Article 1(1) DMA and recitals (2) to (6).

[16] Recital (2) DMA. See also the EDPB Statement on privacy implications of mergers, Adopted on 19 February 2020, which acknowledges the "*concerns that the possible further combination and accumulation of sensitive personal data regarding people in Europe by a major tech company could entail a high level of risk to the fundamental rights to privacy and to the protection of personal data*."

[17] In this regard, it should be noted that Article 2(20) DMA defines an 'end user' as "*any natural **or legal** person using core platform services other than as a business user*". See also Recital 14 DMA: "*the notion of end users should encompass users that are traditionally considered business users*". However, the present guidelines cover primarily scenarios where they are 'data subjects' and not controllers or processors.

[18] Article 25 GDPR.

[19] 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, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

DRAFT

the DMA applies "*without prejudice to the rules resulting from other acts of Union law regulating certain aspects of the provision of services covered by this Regulation*" – in particular the GDPR and the ePrivacy Directive, "*as well as national rules aimed at enforcing or implementing those Union legal acts*."[20]

6. The DMA and the GDPR should be interpreted in a compatible manner, enabling a coherent application that achieves their respective objectives.[21] This is particularly relevant in relation to those provisions of the DMA that explicitly refer to definitions and concepts under the GDPR or impact the processing of personal data by gatekeepers. In that context, a consistent and coherent interpretation of the DMA and the GDPR should mutually reinforce and maximise achievement of the respective objectives of the two frameworks, while fully respecting the protection of the fundamental rights to data protection as enshrined in Union law.[22] It should also avoid risks that gatekeepers, controllers and processors instrumentalize their compliance with the GDPR with a view to make their compliance with the DMA less effective, and vice-versa.

7. The objective of these Guidelines is to provide guidance for the coherent and consistent interpretation and application of both the DMA and of the GDPR, in relation to some provisions of the DMA that concern or may entail the processing of personal data by gatekeepers or include references to GDPR concepts and definitions.

8. These Guidelines are primarily addressed to gatekeepers designated under the DMA, which may be acting as, or may have within their corporate structure, controllers or processors of personal data in the context of the provision of their services, but also to gatekeepers' business users, as well as to end users who may be data subjects within the meaning of the GDPR.

9. The Commission, in accordance with Article 47 DMA, issues these Guidelines to facilitate the effective implementation and enforcement of the DMA and is solely responsible for the interpretation of the provisions of the DMA covered by these guidelines.

10. The EDPB, in accordance with Article 70(1), point (e) GDPR, issues these Guidelines to examine questions covered by the GDPR and to encourage a consistent application and enforcement of the GDPR, and is solely responsible for the interpretation provided for in the present guidelines of the provisions of the GDPR, including those referred to in the DMA.

---

[20] For example, where processing of personal data required or covered by the DMA involves storing information or gaining access to information already stored in the terminal equipment of an end user, gatekeepers must take into account that such processing activities may require consent under Article 5(3) of the ePrivacy Directive.

[21] See, by analogy, Judgment of the General Court of 3 May 2018, *Malta v Commission*, T-653/16, ECLI:EU:T:2018:241, paragraph 137: "*No provision of Regulations Nos 1049/2001 and 1224/2009 expressly gives one regulation priority over the other. Accordingly, it is appropriate to ensure that each of those regulations is applied in a manner compatible with the other and which enables a coherent application of them (see, by analogy, judgments of 29 June 2010, Commission v Bavarian Lager, C-28/08 P, EU:C:2010:378, paragraph 56, and of 28 June 2012, Commission v Éditions Odile Jacob, C-404/10 P, EU:C:2012:393, paragraph 110)*." Paragraphs 139 and 140 of the judgment also state that, even if "*Article 113(2) and (3) of Regulation No 1224/2009 is not, as such, lex specialis derogating from the general rules on public access to documents laid down in Regulation No 1049/2001*, (...) *the fact remains that, as has been stated in paragraph 137 above, both Regulation No 1049/2001 and Regulation No 1224/2009 should be applied consistently*."

[22] Recital 109 DMA and judgment of the Court of Justice of 21 June 2022, *Ligue des droits humains v Conseil des ministres*, C-817/19, ECLI:EU:C:2022:491, paragraph 86.

DRAFT

11. These Guidelines are without prejudice to the respective powers of the Commission and of the EDPB to issue, within the framework of their respective competences, any further guidance on any provisions of the DMA or the GDPR respectively, and to the case law of the Union courts on DMA and GDPR.

2 End-user choice and consent (Article 5(2) DMA)

12. Gatekeepers collect vast amounts of personal data whilst providing CPSs and other digital services to business and end users. Gatekeepers also process personal data from a significantly larger number of third parties than other undertakings.[23] Access to personal data has increasingly become a parameter of contestability, taking into account the use of personal data to develop, create, and improve highly targeted services. Such access and subsequent processing have to comply with applicable laws, including the GDPR.

13. With its requirement to present end users with a specific choice and to obtain valid consent from them, Article 5(2) DMA seeks to address the enhanced access to personal data that provides gatekeepers with potential advantages in terms of data accumulation, which in turn raises entry barriers and hinders contestability in digital markets.[24]

14. Under Article 5(2) DMA, gatekeepers are forbidden to 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 CPSs of the gatekeeper;

    b. combine personal data from the relevant CPS with personal data from any further CPS 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 CPS in other services provided separately by the gatekeeper, including other CPSs, and vice versa; and

    d. sign in end users to other services of the gatekeeper in order to combine personal data.

15. The prohibitions laid down in Article 5(2) DMA of processing for the purpose of providing online advertising services, combining, cross-using or signing-in end users in order to combine personal data of end users do not apply, where two cumulative conditions are satisfied:

    i. First, the gatekeeper has presented the end user with the *specific choice* of whether to allow the processing, combination, or cross-use of their personal data by the gatekeeper across its CPSs and distinct services. In particular, end users have to be able to make a choice between the service provided to users who grant consent to the processing operations listed under Article 5(2) DMA, and a less personalised but equivalent alternative service provided to users that do not grant such consent (see section 2.1).

    ii. Second, the end user has given valid *consent* within the meaning of Articles 4(11) and 7 GDPR to the processing, combination, or cross-use of personal data described in Article 5(2)(a) to (d) DMA (see section 2.2).

[23] Recital 36 DMA.
[24] Recital 36 DMA.

DRAFT

16. Article 5(2) DMA further provides that where the consent given for the purposes of the processing activities covered by Article 5(2)(a) to (d) DMA has been refused or withdrawn by the end user, the gatekeeper is prohibited from repeating its request for consent for the same purpose more than once within a period of one year (see section 2.4).

17. Finally, Article 5(2) DMA is without prejudice to the possibility for the gatekeeper to process personal data without end users' consent when it is necessary for the gatekeeper's compliance with a legal obligation, to protect the vital interests of the end user (as a data subject) or another natural person, or to perform a task in the public interest or in the exercise of official authority in line with Article 6(1), points (c), (d) or (e) GDPR. (see section 2.6).

18. All processing activities covered by Article 5(2) DMA qualify as processing operations within the meaning of Article 4(2) GDPR.[25] A controller is always required to have an appropriate lawful ground for the processing of personal data, with consent of the data subject being one of the available lawful grounds stated in Article 6(1) GDPR.[26] Article 5(2) DMA however limits the lawful grounds under which the CPSs and other services of gatekeepers, as controllers, may carry out certain processing of personal data of end users, given that gatekeepers cannot rely on the performance of a contract, or on the gatekeepers' or a third parties' legitimate interests for processing activities within the scope of Article 5(2), points (a) to (d) DMA (see section 2.5).[27]

19. Gatekeepers should ensure user-friendly choices and consent designs, notably by streamlining consent requests into a single consent flow if and to the extent that the processing operations requiring consent under the GDPR pursue the same specific purposes as the processing operations that also require consent under Article 5(2) DMA (see section 2.3).

20. While pursing different objectives (see Introduction), Article 5(2) DMA complements the GDPR and fosters end users' control and choices over the processing of their personal data by restricting gatekeepers' ability to determine the lawful ground for certain processing operations and imposing that they rely on end user's consent as defined in Article 4(11) GDPR or one of the other specific lawful grounds under Article 6(1) GDPR mentioned in Article 5(2) DMA, thereby ensuring a high level of protection of personal data.

21. Processing activities other than the ones listed under Article 5(2), points (a) to (d) DMA fall outside the scope of that provision (see section 2.6). An example is the processing of personal data that a gatekeeper's CPS or other gatekeeper service obtains directly from interactions with a specific end user, without processing any personal data from any other service of that gatekeeper or from third parties.

22. Gatekeepers are responsible for ensuring that processing operations covered by Article 5(2) DMA at all times comply with the principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation,

[25] Article 4(2) GDPR defines 'processing' as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".
[26] Article 6(1) GDPR.
[27] Recital 36 DMA.

DRAFT

integrity and confidentiality and accountability enshrined in Article 5 of the GDPR and with the remaining provisions of the GDPR.

2.1 Specific choice and the requirement for a less personalised but equivalent alternative service under the DMA

23. As regards the first condition of specific choice, Article 5(2) DMA read together with recitals 36 and 37 DMA explains that gatekeepers should enable end users to freely choose to opt-in to the data processing and sign-in practices covered by Article 5(2) DMA. This should be achieved by offering a less personalised but equivalent alternative, and without making the use of the CPS or certain functionalities of the CPS conditional upon the end user's consent.[28] This is a means to address the accumulation of personal data by gatekeepers and the correlated erosion of market contestability as underscored by both recitals, which also provide further guidance on the specific choice that has to be presented to end users when seeking their consent for the processing of personal data.

24. It follows that a specific choice entails the gatekeeper offering a less personalised, but equivalent alternative service of the relevant CPS to its end users who refuse consent to the processing, combination or cross-use of personal data covered by Article 5(2) DMA, instead of leaving end users only with the option of not using the service at all.

25. Recital 37 DMA, as it relates to Article 5(2), clarifies that this less personalised but equivalent alternative version of the service should not be different or of degraded quality compared to the version provided to the end users who has consented to such processing for the purpose of providing online advertising services, combination, cross-use or signing-in of end users in order to combine personal data (meaning that the service should remain unchanged, with no suppressed functionalities), unless a degradation of quality is a direct consequence of the gatekeeper not being able to process such personal data or sign in end users to a service. The gatekeeper should inform the end user about this fact at the time of requesting their consent under Article 5(2) DMA.

26. To ensure equivalence, the alternative service should not differ, in terms of performance, experience and conditions of access[29] compared to the service offered to consenting end users.

27. Overall, the less personalised but otherwise equivalent version of the service for non-consenting users is not to include any processing activities that would require consent under Article 5(2) of the DMA. Where the gatekeeper intends to process personal data across services while providing the less personalised alternative, such processing should qualify either as:

    a. cross-use of personal data between services not provided separately (which is not subject to the consent requirement under 5(2), point (c) DMA); or

[28] Recital 36 DMA. This should be without prejudice to the gatekeeper processing personal data or signing in end users to a service, relying on the lawful grounds under Article 6(1)(c), (d) and (e) GDPR, but not on Article 6(1)(b) and (f) GDPR. On these possibilities, see Section 2.6.2 below.

[29] For instance, in decision *relating to Case DMA.100055 - Meta (Article 5(2))* (23 April 2025) C(2025) 2091, OJ C/2025/3466, the Commission found that when the service for consenting users is offered by a gatekeeper free of monetary charge, the alternative service offered to non-consenting end users should also then, in principle, be provided free of monetary charge.

DRAFT

b. be able to rely on Article 6(1), points (c), (d) or (e) GDPR which remain available as processing grounds under Article 5(2) DMA (see section 2.6).

28. Although processing activities in the less personalised but otherwise equivalent alternative service do not require consent under Article 5(2) DMA, such processing still should rely on a valid GDPR lawful ground and remains subject to all other requirements of the GDPR.[30]

2.2 Consent within the meaning of the GDPR

2.2.1 General conditions

29. The second condition for compliance with Article 5(2) DMA concerns a valid consent to the processing, combination, or cross-use of personal data within the meaning of Articles 4(11) and 7 of the GDPR. Consent should be given by a clear affirmative action or statement establishing a freely given, specific, informed and unambiguous indication of agreement by the end user, as stated in Article 4(11) GDPR. To be valid, the consent also has to meet the requirements set out in Article 7 GDPR.[31]

30. The requirements of 'specific' and 'free' consent determine the need for granularity of consent choices provided to end users.[32] In particular, gatekeepers are required to specify the intended purpose of the processing of personal data when seeking end users' consent for the processing of personal data covered by Articles 5(2), points (a) to (d) DMA.[33]

31. Consequently, where gatekeepers seek consent for processing personal data covered by Article 5(2) DMA for various purposes, they should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes.[34] Purposes such as personalisation of content, personalisation of advertisements, and service development, are distinct purposes for which separate consents should be obtained if the gatekeeper wishes to combine or cross-use personal data in the manner described in Article 5(2), points (b) to (d) DMA. Consent requests should describe processing purposes without vagueness or ambiguity as to their meaning or intent, thereby allowing the identification of the precise remit for which consent is granted or refused by end users.[35]

---

[30] For example, for the situations described in sections 2.6.1, the appropriate GDPR lawful ground may be consent under Article 6(1), point (a) GDPR, depending on the specific characteristics of the processing.

[31] Article 5(2) DMA.

[32] EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020, paragraph 44: "*If the controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom. This granularity is closely related to the need of consent to be specific* (...). *When data processing is done in pursuit of several purposes, the solution to comply with the conditions for valid consent lies in granularity, i.e. the separation of these purposes and obtaining consent for each purpose*."

[33] When a service involves "*multiple processing operations for more than one purpose*", "*data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes*"- see EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020, paragraph 42.

[34] EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020, paragraphs 56 and 60: "*obtaining valid consent is always preceded by the determination of a specific, explicit and legitimate purpose for the intended processing activity.* (...) *a controller that seeks consent for various purposes should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes*."

[35] Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation (WP 203), Adopted on 2 April 2013, page 17.

DRAFT

32. When requesting consent, gatekeepers should provide end users with a clearly identifiable option allowing them to refuse consent. The refusal may be expressed by a positive action, by which users select an equally accessible option that allows them to unambiguously indicate their refusal. Acceptance and refusal options should be presented in equal terms, without nudging end users towards consenting.[36]

33. Furthermore, such processing has to be conducted in compliance with the principles enshrined in Article 5 of the GDPR[37] and with the remaining provisions of the GDPR.

34. In scenarios where gatekeepers are controllers under the GDPR, the consequences for data subjects who decide not to consent to the processing of their personal data may amount to detriment and conditionality that would impinge on the freedom (and hence the validity) of consent.[38] Examples of detriment are deception, intimidation, coercion or significant negative consequences if a data subject does not consent.[39] The possibility to refuse or withdraw consent without detriment needs to be demonstrated by the controller.[40]

35. The imbalance of power that may exist between controllers who are gatekeepers and end users (data subjects) may also affect the freedom (and hence the validity) of consent expressed by end users. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will.[41] This may be the case where the controller's position in the market, by itself or in combination with other factors, leads the data subjects to note that there are no other realistic alternative services available to them.[42]

2.2.2 Special categories of personal data

36. In all instances, gatekeepers remain obliged to consider whether the processing activities they carry out would involve categories of personal data captured by Article 9(1) GDPR (so-called 'special categories of personal data').[43] To process such data,

---

[36] See recital 37 DMA: "*Gatekeepers should not design, organise or operate their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of end users to freely give consent*".

[37] EDPB Guidelines 8/2020 on the targeting of social media users, paragraph 58: "*Consent (Article 6(1)(a) GDPR) could be envisaged, provided that all the requirements for valid consent are met. The EDPB recalls that obtaining consent also does not negate or in any way diminish the controller's obligations to observe the principles of processing enshrined in the GDPR, especially Article 5 with regard to fairness, necessity and proportionality, as well as data quality. Even if the processing of personal data is based on consent of the data subject, this would not legitimize targeting which is disproportionate or unfai*r". See also Judgment of the Court of Justice of 4 October 2024, *Maximilian Schrems v Meta Platforms Ireland Ltd*, C-446/21, ECLI:EU:C:2024:834, paragraph 59.

[38] EDPB Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms Adopted on 17 April 2024, paragraph 116. The notion of large online platforms, as defined in this Opinion, may cover gatekeepers as defined under the DMA.

[39] EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020, paragraph 47.

[40] Article 5(2) GDPR.

[41] EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020, paragraph 24.

[42] See also, by analogy, EDPB Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms Adopted on 17 April 2024, paragraphs 105, 109, 110, and 111.

[43] As clarified by the CJEU, the scope of Article 9(1) GDPR is particularly broad, encompassing data that allows information falling within one of the categories described in Article 9(1) GDPR to be revealed, regardless of whether the information is correct and of whether the controller is acting with the aim of obtaining information that falls under Article 9(1) GDPR. See Judgment of the Court of Justice of 1 August 2022, *OT v Vyriausioji tarnybinės etikos komisija*, C-184/20 ECLI:EU:C:2022:601, paragraph 123, which states that Article 9(1) GDPR encompasses "*processing not only of inherently sensitive data, but also of data revealing information of that nature*

the gatekeeper has to secure a permissible and adequate lawful ground under Article 6(1) GDPR, and has also to be able to validly rely on one of the derogations from the prohibition on processing special categories of personal data provided under Article 9(2) GDPR.

37. If gatekeepers are required to rely on consent under Article 9(2), point (a) GDPR – for instance, where processing special categories of personal data for advertising purposes – consent should be explicit. In the context of Article 5(2) DMA, gatekeepers should allow data subjects to issue a statement expressing their consent by filling in an electronic form, or by selecting 'Yes' or 'No' check boxes in an electronic consent interface, provided that the text of the request is sufficiently clear.[44]

38. However, where gatekeepers are also qualified as providers of 'online platforms' under Regulation (EU) 2022/2065 of the European Parliament and of the Council[45] ('DSA'), and to the extent they intend to seek consent for the processing, combination or cross-use of personal data for the purpose of presenting advertisements to end users, they are prohibited from presenting advertisements based on profiling[46] using special categories of personal data.[47]

39. Similarly, in accordance with Article 18(1), point (c) of Regulation (EU) 2024/900 of the European Parliament and of the Council,[48] if gatekeepers conduct processing of personal data in the manner described under Article 5(2) DMA in the context of targeting techniques or ad-delivery techniques for online political advertising, such techniques cannot involve profiling using special categories of personal data.

2.3 Ensuring user-friendly choices and consent designs

40. When the gatekeeper requests consent under Article 5(2) DMA, it should proactively present a user-friendly solution to the end user to provide, modify or withdraw consent in an explicit, clear and straightforward way,[49] also accessible to persons with disabilities.[50]

DRAFT

---

indirectly, following an intellectual operation involving deduction or cross-referencing, the preposition 'concerning' seems, on the other hand, to signify the existence of a more direct and immediate link between the processing and the data concerned, viewed inherently". See also Judgment of the Court of Justice of 4 July 2023, *Meta Platforms and others (Conditions générales d'utilisation d'un réseau social)*, C-252/21, ECLI:EU:C:2023:537, paragraphs 68 and 69.

[44] EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1, Adopted on 4 May 2020, paragraphs 93, 94 and 96.

[45] 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, ELI: http://data.europa.eu/eli/reg/2022/2065/oj).

[46] Article 4(4) GDPR: "*'profiling' means any form of automated processing of personal 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*".

[47] Article 26(3) of the DSA.

[48] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising (OJ L, 2024/900, 20.3.2024, ELI: http://data.europa.eu/eli/reg/2024/900/oj).

[49] Recital 37 DMA. This requirement is similar to Article 7(2) GDPR: "*If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language*."

[50] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (Text with EEA relevance)

41. The fact that gatekeepers are obliged to offer granular choices to end users in relation to the purposes for which they intend to combine or cross-use personal data as described in Article 5(2) DMA should be combined with the requirement for gatekeepers to present end users with user-friendly choices and consent designs. An appropriate consent flow that respects the principles of fairness, transparency and accountability is key to ensure compliance with Article 5(2) DMA and its consent requirements.[51]

42. In order to ensure user-friendly choices and consent designs, and in particular to avoid overburdening end users, gatekeepers should streamline consent requests for the same specific purposes into a single consent flow if and to the extent that the processing operations requiring consent under Article 6(1) GDPR include processing operations falling under Article 5(2) DMA (i.e. where the processing operations for which consent is requested under Article 6(1) GDPR also requires consent under Article 5(2) DMA).[52]

43. A user interface consent flow should allow end users to express a valid consent according to GDPR requirements, otherwise it will be in breach of Article 5(2) DMA. For example, the use of pre-ticked boxes in consent requests (which do not constitute valid consent within the meaning of the GDPR[53]) is therefore not compliant with Article 5(2) DMA.

44. Moreover, Article 13(6) DMA provides that gatekeepers cannot make the exercise of end users' rights or choices under Articles 5 to 7 DMA – including granting, refusing or withdrawing consent to the processing of their personal data – unduly difficult, notably by offering choices to the end-user in a non-neutral manner, or by subverting end users' autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a user interface or a part thereof.[54]

45. Consequently, a user interface consent flow should be presented in a factually and visually neutral way. The design choices of user interface consent flow such as for example use of colours and contrasts of buttons, fonts, pictures, or other design choices that may mislead or nudge end users into providing unintended and thus invalid consent according to Article 4(11) GDPR fall short of effective compliance with Article 5(2) DMA.[55] A user interface consent flow should not be designed in a way that leads end users to forget, not understand, or not think about all or some of the implications of providing their consent. The design of the interface should not be

[51] See Article 5 GDPR and EDPB Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, Adopted on 14 February 2023, paragraphs 9 and 10.

[52] See, by analogy, 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, footnote 17: "*Consent required by art. 5(3) of the "ePrivacy" directive and consent needed as a legal basis for the processing of data (art. 6 GDPR) for the same specific purpose can be collected at the same time (for example, by checking a box clearly indicating what the data subject is consenting to)*."

[53] Judgment of the Court of Justice of 1 October 2019 Planet49 GmbH, C-673/17, ECLI:EU:C:2019:801, paragraph 63: "*the consent referred to in Article 2(f) and in Article 5(3) of Directive 2002/58, read in conjunction with Article 4(11) and Article 6(1)(a) of Regulation 2016/679, is not validly constituted if the storage of information, or access to information already stored in the website user's terminal equipment, is permitted by way of a pre-ticked checkbox which the user must deselect to refuse his or her consent*".

[54] Recital 37 specifies that "*Gatekeepers should not design, organise or operate their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of end users to freely give consent*." See also recital 70 DMA.

[55] See EDPB Report of the work undertaken by the Cookie Banner Taskforce, Adopted on 17 January 2023; See also EDPB Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, Adopted on 14 February 2023.

DRAFT

inconsistent and unclear, making it hard for the end user to navigate the consent request and to understand the purpose of the processing they are consenting to.[56] The interface or user journey should also not be designed in a way that hides information or consent controls. Therefore, the choice presented to end users should not leave them unsure of how their data is processed or as to the degree of control they might have over their personal data under Article 5(2) DMA and the data protection rights conferred by the GDPR.

2.4 Limits to repeating consent requests

46. Article 5(2) DMA provides that consent requests presented to an end user cannot be repeated to the same user for the same purpose more than once within a year.[57] This obligation is reinforced by the requirement to ensure that consent is not requested in a manner that leads to 'choice fatigue' when implementing Article 5(2) DMA.[58]

47. To comply with Article 5(2) DMA and the DMA's broader anti-circumvention rule,[59] gatekeepers should refrain from presenting slightly modified consent requests (e.g. consent requests with a different wording) within the same year, that seek to obtain consent for the same processing operations and for essentially the same purposes.[60]

48. The requirement not to repeat consent requests more than once within a year should apply from the date on which end users make a choice by actively granting or refusing consent. End users who dismiss or abandon the consent request have not given their consent in line with Article 5(2) of DMA and therefore the respective personal data of end users cannot be used by the gatekeepers until such consent is given. In that case, the gatekeeper is entitled to repeat the consent request to those end users, while complying with their obligations under Union consumer protection law,[61] until end users make a choice by granting or refusing consent.

49. In practical terms, compliance with the requirement of Article 5(2) DMA may involve the processing of a limited amount of personal data of the end user by the gatekeeper to record the fact that a consent has been refused or withdrawn by a given end user. In

---

[56] See also EDPB Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, Adopted on 14 February 2023.

[57] Article 5(2) DMA.

[58] See Article 7(2) GDPR: "*the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language*." The EDPB has also clarified that 'continuous prompting' – i.e., "*pushing users to provide more personal data than necessary for the purpose of processing or to agree with another use of their data by repeatedly asking users to provide data or to consent to a new purpose of processing*" – breaches "freedom" and "specificity" consent requirements. See EDPB Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, p. 65.

[59] Article 13(4) DMA.

[60] See also paragraph 31 of these Guidelines.

[61] This means that gatekeepers should allow end users to defer their choice, if appropriate (i.e., not force them to make an immediate choice), and gatekeepers should not engage in behaviour that unduly influences an end user's decision to provide or withhold consent (e.g., by designing the consent interface in a certain way). Such practices may amount to a breach of professional diligence requirements, misleading or aggressive practices under Articles 5 to 9 of Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), OJ L 149, 11.6.2005, p. 22–39, depending on the specific circumstances of the case. See Section 4.2.7 of Commission Notice – Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, C/2021/9320, OJ C 526, 29.12.2021, p. 1–129.

DRAFT

many scenarios of the provision of a CPS to end users, gatekeepers are likely to prompt end users and record their preferences via signed-in end users' account settings, which allows gatekeepers to honour end users' choices in any devices they use to access the CPS.

50. In scenarios where gatekeepers prompt non-signed-in end users and record their preferences, it may be harder or technically impossible for gatekeepers to honour end users' preferences in devices other than the one through which they have expressed their preferences. In line with the data minimisation principle under Article 5(1), point (c) GDPR, personal data used to record end users' preferences should in principle not contain a unique identifier, but should rather contain generic information (e.g., a cookie with a flag or code) which is common to all end users who have refused consent.[62]

51. If such personal data is deleted by an end user or deleted due to a change of technical settings, within the one-year period, gatekeepers may prompt the end user with a new consent request. The same applies to a scenario where the end user accesses the non-signed-in CPS through a device other than the one through which they refused or withdrew consent.

2.5 Processing activities covered by Article 5(2) DMA

52. All data related activities covered by Article 5(2) DMA also qualify as data processing activities within the meaning of the GDPR.

2.5.1 Article 5(2), point (a) DMA

53. Gatekeepers often directly collect personal data of end users for the purpose of providing online advertising services when end users use third-party websites and software applications that make use of the gatekeeper's online advertising services.[63] Tracking technology embedded into websites or software applications of third parties, such as cookies, plug-ins and pixels, are often used to collect personal data for advertising purposes. Gatekeepers may also operate advertising networks of publishers and/or advertisers that collect significant amounts of personal data from millions of end users. Third parties additionally provide gatekeepers with personal data of their end users in order to make use of certain services provided by the gatekeepers in the context of their CPSs, such as custom audiences.[64]

54. Article 5(2), point (a) DMA prohibits gatekeepers from processing, for the purpose of providing online advertising services, personal data of end users using services of third parties that make use of CPSs of the gatekeeper. This prevents gatekeepers from, for example processing the personal data of end users of third-party services that rely on the gatekeepers' online advertising services in order to serve ads on the gatekeeper's

DRAFT

[62] EDPB reply to the Commission's Initiative for a voluntary business pledge to simplify the management by consumers of cookies and personalised advertising choices, p. 8 of the Annex: "*The EDPB agrees that to make the refusal to, or withdrawal of, consent effective, it may be necessary to record the decision of the user for a certain period, in order to reduce the frequency of consent request a user receives*. (...). *In particular, the EDPB recommend clarifying that the record of the "negative consent" relying on cookies should not contain a unique identifier, but should rather contain generic information, a flag or code, which is common to all users who have refused consent*."

[63] Recital 36 DMA.

[64] Custom Audiences are a targeting tool that allows advertisers to upload customer data (e.g. emails, phone numbers) to match with CPS's end users and deliver tailored ads to those end users. See also recital 36 DMA.

own services or on other third parties' services, unless the end user has been presented with a specific choice and granted their valid consent.

55. Where an end user directly interacts with a third-party website, service or software application making use of the gatekeeper's CPS, the nature of Article 5(2), point (a) DMA obligation requires gatekeepers to obtain consent from end users through that third-party website, service or software application.[65]

56. Appropriate and secure technical solutions, such as consent management platforms, may be used by third parties, as long as they ensure that the consent obtained from end users through those means is fully informed and compliant with the requirements of valid consent within the meaning of the GDPR. The gatekeeper remains responsible to ensure that the consent obtained by the relevant third party is fully compliant with the requirements of Article 4(11) and Article 7 GDPR before it processes the personal data obtained via the third party to provide online advertising services. No information should be communicated to the gatekeeper or its services where no consent has been provided by the end user. Failure by the gatekeeper to ensure that end users validly consented through third-party services to the processing of their personal for online advertising services constitutes a violation of Article 5(2), point (a) DMA and of Article 6(1), point (a) GDPR.

2.5.2 Article 5(2), point (b) DMA

57. Under Article 5(2), point (b) DMA, a gatekeeper has to obtain end users' consent to combine[66] personal data from a CPS with personal data from any other CPSs or services provided by the gatekeeper or third parties.

58. In line with the requirements of 'specific' and 'free' consent, and the need for granularity (see paragraph 31), when seeking the consent of end users to combine personal data between a CPS and other gatekeeper or third-party services, the gatekeeper always has to indicate the specific purpose or purposes for which it intends to combine the end user's personal data in order to obtain a valid consent.

59. Examples of the combination of personal data between a CPS and other gatekeeper or third-party services include the use of an end user's personal data, such as interests, obtained from different gatekeeper services, or the use of end user behaviour on third-party websites in combination with personal data obtained from gatekeeper services, in order to provide personalised content. In cases where end users directly interact with the services of a gatekeeper, and the gatekeeper intends to combine personal data obtained from such interactions with personal data from third-party services, the

[65] This is in line with the judgment of the Court of Justice of 29 July 2019, *Fashion ID v Verbraucherzentrale NRW eV*, C-40/17, ECLI:EU:C:2019:629, paragraph 102. Recital 37 DMA provides that "*Exceptionally, if consent cannot be given directly to the gatekeeper's core platform service, end users should be able to give consent through each third-party service that makes use of that core platform service, to allow the gatekeeper to process personal data for the purposes of providing online advertising services*."

[66] Combination is one operation that falls within the notion of processing defined in Article 2(2) GDPR as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

DRAFT

gatekeeper should directly obtain the consent of the end users interacting with its own services.[67]

60. Where the gatekeeper does not present complete and intelligible information to the end user to obtain a valid consent for the combination of an end user's personal data the gatekeeper may not only be in breach of Article 5(2) DMA, but could also be in breach of the principles of lawfulness, fairness, transparency, and purpose limitation under Articles 5(1), points (a) and (b) GDPR, respectively.

2.5.3 Article 5(2), point (c) DMA

61. Article 5(2), point (c) DMA prohibits a gatekeeper from cross-using personal data from a relevant CPS in other services that it provides separately, including other CPSs, and vice versa, without the end user's valid consent. In contrast, Article 5(2), point (c) DMA does not require gatekeepers to obtain consent in instances of cross-use of personal data between a CPS and gatekeeper services that are provided together with or in support of a CPS (see section 2.6.1 of these Guidelines, paragraphs 67 to 71), or for the cross-use of personal data with third party services. However, gatekeepers still have to be able to rely on an appropriate lawful ground for such processing under the GDPR, (section 2.6.1, paragraphs 72 to 77).

62. An example of the cross-use of personal data that requires end user consent is the one-time use of end user information or observed behaviour in a gatekeeper CPS (such as likes, viewed content or session time) by the gatekeeper in another of its services. Whether this cross-use falls within the exemption to consent foreseen under Article 5(2), point (c) DMA depends on whether the two services concerned are provided together or separately (see section 2.6.1).

63. Similarly to Article 5(2), point (b) DMA, the gatekeeper also has to, among other elements, inform end users about the specific purpose for which it intends to cross-use their personal data when requesting their consent to ensure such consent is valid under Article 4(11) and Article 7 GDPR.

2.5.4 Article 5(2), point (d) DMA

64. Article 5(2), point (d) DMA addresses situations where gatekeepers intend to sign in end users to other services of the gatekeeper in order to combine their personal data. Article 5(2), point (d) DMA requires gatekeepers to seek consent not only before any actual data combination, but prior to the moment of signing in of the end user. The consent sought has to comply with the requirements for valid consent as spelled out in Article 4(11) and 7 GDPR, including the requirements of specificity and freely given consent.

65. An example of signing in end users to other services of the gatekeeper in order to combine their personal data, is a situation where a gatekeeper providing an operating system CPS automatically logs in end users to other software applications ("apps") or services of the gatekeeper that are installed on the operating system.

[67] This is also in line with the judgment of the Court of Justice of 4 July 2023, *Meta Platforms and others (Conditions générales d'utilisation d'un réseau social)*, C-252/21, ECLI:EU:C:2023:537, paragraph 151, where the Court confirmed that separate consent must be given for the processing of personal data of end users collected from individuals whilst actively using the service ('on-platform data') and personal data obtained from other sources ('off-platform data').

DRAFT

66. The gatekeeper has to comply fully with the other provisions of the GDPR, notably Article 5(1), point (c) on data minimisation and Article 25 on data protection by design and by default when designing and deploying sign-in mechanisms.[68]

2.6 Processing not requiring consent under Article 5(2) DMA

2.6.1 Cross-use of personal data between gatekeeper services provided together with or in support of each other

DMA perspective

67. As already mentioned in paragraph 61 above, the DMA does not require gatekeepers to obtain consent in instances of cross-use of personal data between a CPS and gatekeeper services that are provided together with or in support of a CPS.[69] This ensures that Article 5(2), point (c) DMA does not inhibit cross-use of personal data that is required to offer the essential functionalities of certain services.

68. In order for a relevant service to be qualified as provided together with, or in support of another as referred to in Article 5(2), point (c) DMA read in conjunction with recital 36 DMA, that service should have a close functional interconnection with the CPS or other gatekeeper service, such as identification or payment services.[70] Under the DMA, online advertising services can, in principle, also be considered as services provided together with, or in support of, the gatekeeper's relevant CPS on which ads are displayed.[71]

69. Only personal data that is strictly necessary to provide such interconnected functionality, in line with end users' reasonable expectations, can be used without triggering the requirement to gather consent under Article 5(2) DMA. The material and temporal scope of the personal data that is cross-used should therefore be limited to what is strictly necessary to offer the interconnected functionalities to cross-use personal data without consent. As a consequence, the retention of personal data that has been cross-used by the gatekeeper should be limited to the time required to carry out the relevant functionality.

70. An example of where personal data may be cross-used without end user consent in compliance with Article 5(2), point (c) DMA is when the identification details of an end user are cross-used by a delivery service or a payment service provided by the gatekeeper together with, or in support of, a specific CPS, in order to proceed with the expected delivery or specific payment by an end user. Similarly, in the context of a gatekeeper's online search engine CPS, the cross-use of a single search query by the gatekeeper's online advertising service may be considered strictly necessary in order to display an ad on the online search engine. In that case, the search query can therefore be cross-used without end user consent under Article 5(2) DMA in order to provide an ad result, alongside non-ads results on the gatekeeper's online search engine CPS.

---

[68] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0, Adopted on 20 October 2020, paragraph 76.

[69] Recital 36 DMA.

[70] See also recital 43 DMA.

[71] This is also supported by the delineation of CPS established in the Commission Decisions C(2023) 6101 final, C(2023) 6104 final, C(2023) 6105 final, designating respectively Alphabet, Amazon and Meta as gatekeepers pursuant to Article 3(4) DMA, where the Commission found that the display of advertisements can be considered part of both the online advertising CPS and the other CPS on which the advertisement is displayed. This is without prejudice to the requirement of securing an appropriate lawful ground under the GDPR, as explained in section 2.6.1, paragraphs 72 to 77.

DRAFT

71. As recalled in paragraph 61, even in instances of cross-use of personal data that do not require consent under Article 5(2) DMA, the gatekeeper remains responsible for ensuring full compliance with the GDPR, including the requirement of having a valid lawful ground under Article 6(1) GDPR for the processing of personal data.

GDPR perspective

72. Provided that their respective conditions are effectively complied with, the lawful grounds of Article 6(1), point (b) or (f) GDPR may be appropriate lawful grounds for the cross-use of personal data between a CPS and another gatekeeper service without end user consent, where both services are provided together with or in support of each other.

73. The cross-use of personal data by the gatekeeper between services provided together or in support of each other, in situations where the processing is objectively necessary for performing the contract or taking pre-contractual steps at the end users' request can, subject to a case-by-case assessment by the controller, lawfully rely on Article 6(1), point (b) GDPR.[72] For example, cross-using the end user's personal data collected in a CPS in a payment service also provided by the gatekeeper to process a payment could rely on Article 6(1), point (b) GDPR as a lawful ground.[73] In contrast, it should be recalled that processing for online advertising services cannot be seen as strictly necessary, under the GDPR, to perform the contract entered into by end users with gatekeepers for the provision of a CPS.[74]

74. If the cross-use of personal data cannot be deemed strictly necessary for the gatekeeper to provide the CPS, or another service provided together or in support of the CPS, pursuant to the contract with the end user under Article 6(1), point (b) GDPR, there may be circumstances where the gatekeeper may be able to rely on Article 6(1), point (f) GDPR to carry out such processing activities. For processing to be based on the legitimate interest lawful ground, the three following cumulative conditions have to be fulfilled:

    a. the pursuit of a legitimate interest by the controller or by a third-party;

    b. the need to process personal data for the purposes of the legitimate interest(s) pursued (i.e., the processing of personal data is "necessary" for those purposes); and,

    c. the interests or fundamental freedoms and rights of the concerned data subjects do not take precedence over the legitimate interest(s) of the controller or of a third party.[75]

75. For example, depending on the characteristics of the processing, the cross-use of on-platform personal data (i.e., collected in the gatekeeper's CPS) in an advertising service of the gatekeeper that is provided together or, in support of the CPS where such

[72] This can only occur when the processing is objectively indispensable for a purpose that is integral to the main subject matter of the contract; it is not sufficient if such processing is merely useful for the performance of that contract. See Judgment of the Court of Justice of 9 January 2025, *Mousse v Commission nationale de l'informatique et des libertés*, C-394/23, ECLI:EU:C:2025:2, paragraphs 33 and 34.

[73] 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, paragraph 30 and Example 1.

[74] 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, paragraphs 25, 30 and 52.

[75] Judgment of the Court of Justice of 4 July 2023, *Meta Platforms and others (Conditions générales d'utilisation d'un réseau social)*, C-252/21, ECLI:EU:C:2023:537, paragraph 106; Judgment of the Court of Justice of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/1, ECLI:EU:C:2019:1064, paragraph 40.

DRAFT

data is collected, may be regarded as carried out for a legitimate interest of the gatekeeper. In particular, processing a limited set of on-platform personal data, such as geography (as opposed to precise location), language and content, as well as topics of interest as actively provided by the end user, might not require consent. If processing operations do not involve intrusive measures, such as profiling and tracking, and do not go beyond the reasonable expectations of the end users, it may be possible to rely on Article 6(1), point (f) of the GDPR.

76. Processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest of the controller.[76] In relation to the other two conditions, controllers need to demonstrate in particular that the legitimate interests pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental right to data protection,[77] and pay particular attention to whether the processing would be reasonably expected by data subjects,[78] in particular if they include children.[79] In any case, end users retain the unconditional right, under Article 21(3) GDPR, to object to the processing of their personal data for direct marketing purposes.

77. Moreover, certain cross-uses of on-platform data in a supporting advertising service of the gatekeeper may require the latter to obtain consent under the GDPR. This may be the case where such cross-use entails the processing of high volumes and a large variety of types of personal data or involves personal data that allows information falling within Article 9(1) GDPR to be revealed about end users,[80] in a manner that

DRAFT

[76] See Recital 47 GDPR and Judgment of the Court of Justice of 4 July 2023, *Meta Platforms and others (Conditions générales d'utilisation d'un réseau social)*, C-252/21, ECLI:EU:C:2023:537, paragraph 115. Regarding the notion of direct marketing, see Judgment of the Court of Justice of 25 November 2021, *StWL Städtische Werke Lauf a.d. Pegnitz v eprimo GmbH*, C-102/20, ECLI:EU:C:2021:954, paragraph 47. See also EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0, Adopted on 8 October 2024, paragraph 109.

[77] Judgment of the Court of Justice of 4 July 2023, *Meta Platforms and others (Conditions générales d'utilisation d'un réseau social)*, C-252/21, ECLI:EU:C:2023:537, paragraphs 108 and 109. See also Judgment of the Court of Justice of 4 October 2024, *Koninklijke Nederlandse Lawn Tennisbond v Autoriteit Persoonsgegevens*, C-621/22, ECLI:EU:C:2024:857, paragraphs 51-53.

[78] Judgment of the Court of Justice of 4 July 2023, *Meta Platforms and others (Conditions générales d'utilisation d'un réseau social)*, C-252/21, ECLI:EU:C:2023:537, paragraph 112. Paragraph 117 of the judgment adds that "*the user of* [Facebook] *cannot reasonably expect that the operator of the social network will process that user's personal data, without his or her consent, for the purposes of personalised advertising. In those circumstances, it must be held that the interests and fundamental rights of such a user override the interest of that operator in such personalised advertising by which it finances its activity, with the result that the processing by that operator for such purposes cannot fall within the scope of point (f) of the first subparagraph of Article 6(1) of the GDPR*". See also Judgment of the Court of Justice of 4 October 2024, *Koninklijke Nederlandse Lawn Tennisbond v Autoriteit Persoonsgegevens*, C-621/22, ECLI:EU:C:2024:857, paragraphs 55 and 56.

[79] Recital 38 GDPR. See also Judgment of the Court of Justice of 4 July 2023, *Meta Platforms and others (Conditions générales d'utilisation d'un réseau social)*, C-252/21, ECLI:EU:C:2023:537, paragraphs 111 and 123.

[80] Judgment of the Court of Justice of 4 July 2023, *Meta Platforms and others (Conditions générales d'utilisation d'un réseau social)*, C-252/21, ECLI:EU:C:2023:537, paragraph 68: "*For the purposes of applying Article 9(1) of the GDPR, it is important to determine, where personal data is processed by the operator of an online social network, if those data allow information falling within one of the categories referred to in that provision to be revealed, irrespective of whether that information concerns a user of that network or any other natural person. If so, then such processing of personal data is prohibited, subject to the derogations provided for in Article 9(2) of the GDPR.*"

goes beyond their reasonable expectations[81] or that may otherwise have a significant impact on their rights and freedoms.[82]

2.6.2 Processing activities which lawfully rely on Article 6(1), points (c), (d) and (e) GDPR

78. Under Article 5(2) DMA, gatekeepers may engage in processing operations listed under Article 5(2) DMA without obtaining end user consent, provided they fulfil the requirements to rely on the lawful grounds for processing personal data articulated in Article 6(1), points (c), (d) or (e) GDPR.

79. For Article 6(1), points (c) and (e) GDPR to serve as lawful grounds for the processing of personal data, the basis for the processing must be laid down in Union law or in Member State law to which the controller is subject, pursuant to Article 6(3) GDPR.[83] In line with the principle of accountability, gatekeepers should ascertain the extent to which they have to carry out processing activities covered by Article 5(2) DMA under their legal obligations. For example, a gatekeeper may be subject to a legal obligation requiring the processing operations of combining or cross-using personal data for the purpose of network security or service integrity or fraud detection.[84]

80. Article 6(1), point (d) and 6(1), point (e) GDPR, respectively, enable a controller to process personal data, where doing so is necessary to protect the vital interests of a data subject or of another natural person, or where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the relevant controller. When relying on either Article 6(1), points (d) or (e) GDPR, gatekeepers should take into account that reliance on vital interests and public interest tasks to justify processing operations covered by Article 5(2) DMA is possible only in very limited scenarios, in light of gatekeepers' types of activities and their essentially economic and commercial nature.

81. Gatekeepers should implement technical and organisational measures that would prevent reuse of personal data that has been processed on Article 6(1), points (c), (d) and (e) GDPR for further purposes (e.g., through the segregation of personal data in separate filing systems). The processing would also need to comply with the principles under Article 5 GDPR and the remaining provisions of the GDPR.

82. Even where processing operations fall outside of the scope of application of Article 5(2) DMA, they remain subject to all requirements of the GDPR, including the principle of lawfulness. This means that, depending on the characteristics of the processing operations carried out by the gatekeeper, the lawful grounds of Article 6(1),

---

[81] Factors to consider in this context include the data subjects' interests, fundamental rights and freedoms, the impact of the processing on data subjects, the reasonable expectations of the data subject and the final balancing of opposing rights and interests, including the possibility of further mitigating measures. See EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0, Adopted on 8 October 2024, paragraphs 31-60. With regard to the impact of the processing, which includes the context of the processing, a gatekeeper may, for instance, have more resources and negotiating power than the individual data subject, and therefore, may be in a better position to impose on the data subject what it believes is in its 'legitimate interest'.

[82] Judgment of the Court of Justice of 4 July 2023, *Meta Platforms and others (Conditions générales d'utilisation d'un réseau social)*, C-252/21, ECLI:EU:C:2023:537, paragraph 116.

[83] Recital 41 GDPR, in relation to Article 6(3) GDPR, clarifies that such a legal basis should be clear and precise and its application should be foreseeable to persons subject to it. This complements the requirements of Article 7 and 8 of the Charter, as interpreted by the CJEU, according to which any interference must be provided for by law which is clear, precise and foreseeable.

[84] EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1), point (f) GDPR, paragraphs 107 and para 128.

DRAFT

points (b) or (f) GDPR or consent under Article 6(1), point (a) GDPR could be appropriate for processing operations where such operations fall outside the scope of application of Article 5(2) DMA.[85] The Commission, the EDPB and the supervisory authorities of the EDPB commit to cooperate closely to assess whether the circumstances of concrete processing operations fall in scope of Article 5(2) DMA consent requirements or only fall in scope of the GDPR.

3 Distribution of software application stores and software applications (Article 6(4) DMA)

83. Article 6(4) DMA requires gatekeepers to:

a. allow and technically enable the installation and effective use of third-party apps or software application stores ("app stores") using, or interoperating with, its operating system and allow those apps or app stores to be accessed by means other than the relevant CPS of that gatekeeper;

b. not prevent such installed apps or app stores from prompting end users to decide whether they want to set that downloaded app or app stores as their default; and

c. technically enable end users who decide to set that downloaded app or app store as their default to carry out such a change in an easy manner.

84. Enabling the installation and effective use of apps or app stores may entail risks for the integrity of the hardware or operating system as well as the security of end users. In the case of third-party apps or app stores, Article 6(4) DMA allows gatekeepers to:

a. take, to the extent that they are strictly necessary and proportionate, measures to ensure that third-party apps or app stores do not endanger the integrity of the hardware or operating system provided by the gatekeeper, provided that such measures are duly justified by the gatekeeper; and

b. apply, to the extent that they are strictly necessary and proportionate, measures and settings other than default settings, enabling end users to effectively protect security in relation to third-party apps or app stores, provided that such measures and settings other than default settings are duly justified by the gatekeeper.

85. Recital 50 of the DMA, referring to Article 6(4) DMA, also clarifies in this respect that measures implemented by gatekeepers to protect the integrity of the hardware or operating system should include "*any design options that need to be implemented and maintained in order for the hardware or the operating system to be protected against unauthorised access, by ensuring that security controls specified for the hardware, or the operating system concerned cannot be compromised*." Regarding the measures and settings other than default settings that gatekeepers are allowed to apply, Article 6(4) read in conjunction with recital 50 of the DMA adds that these should aim to "*ensure that third-party software applications or software application stores do not undermine end users' security"* as well as to enable *"end users to effectively protect security in relation to third-party software applications or software application stores*".

86. Article 6(4) DMA as informed by recital 50 of the DMA makes clear that it is the responsibility of the gatekeeper to demonstrate that the measures it implements to protect the integrity of the hardware or operating system are "*necessary and justified*

[85] For further guidance on the ability on the conditions to rely on the lawful basis of legitimate interest, including for fraud detection and information security purposes, see EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1), point (f) GDPR, paragraphs 100-108 and paragraphs 126-128 respectively.

DRAFT

and that there are no less-restrictive means to safeguard the integrity of the hardware or operating system"[86] and that the measures it implements to enable end users to effectively protect security in relation to third party apps or app stores are "*strictly necessary and justified and that there are no less-restrictive means to achieve that goal*".[87]

87. In order to comply with their obligations under Article 6(4) DMA, gatekeepers have to allow and technically enable the installation and effective use of third-party apps or app stores. When allowing this, gatekeepers may only take restrictive measures covered by the strictly defined safeguards set out in the second and third subparagraphs of Article 6(4) DMA or are required to comply with other existing laws as provided for in Article 8(1) DMA.

88. Pursuant to Article 8(1) DMA, gatekeepers have to ensure that the implementation of the measures taken to comply with the DMA also comply with applicable laws, including the GDPR and national legislation implementing the ePrivacy Directive. This means that, when taking measures in accordance with Article 6(4) DMA, gatekeepers should ensure that they are also in compliance with their obligations under any other applicable legislation, such as the GDPR and the ePrivacy Directive.

89. At the same time, gatekeepers should not seek to instrumentalize their compliance with other applicable laws with a view to make their compliance with Article 6(4) DMA less effective. When selecting among several possible appropriate measures to comply with obligations stemming from other applicable laws, gatekeepers should select the measures that less adversely affect the pursuit of the objectives of Article 6(4) DMA, provided that they remain effective in ensuring compliance with those other applicable laws.

90. In order to enable effective supervision of the compliance with the obligation under Article 6(4) DMA, and in line with their obligations under Article 8(1) DMA, gatekeepers should be able to demonstrate compliance with their respective obligations under the DMA by keeping an exhaustive and comprehensive list of the measures they put in place and, for each of these measures, their corresponding specific applicable provisions of Union law, including the GDPR, and the rationale justifying why there are no other effective means to comply with those other legal requirements that would less adversely affect the attainment of the goals of Article 6(4) DMA.

91. Insofar as compliance with the GDPR is concerned, a controller is responsible, pursuant to Article 4(7), Article 5(2) and Article 24(1) of that Regulation, for the processing of personal data where it defines the means and purposes of such processing.

92. Gatekeepers, as providers of operating systems, and app developers, should generally be considered as separate controllers under the GDPR since they define, independently of each other, the means and purposes of processing of personal data in relation to the respective operating system, app or app store. Article 6(4) DMA does not intend to establish any joint controllership or controller-processor relationship between a gatekeeper and an app developer as a beneficiary of that provision.

93. Gatekeepers should take account of the division of responsibility and liability between themselves and third parties providing apps and app stores, and ensure that they do not

[86] Recital 50 DMA.
[87] Idem

DRAFT

implement measures that would undermine or circumvent effective compliance with Article 6(4) of the DMA. Gatekeepers should pay particular attention to any technical or contractual measures they seek to impose which may be intended to prescribe the way a third party, such as an app developer, complies with the GDPR. In this regard, as a separate and independent controller, the third party remains responsible and liable for its own processing and should therefore be free to choose how it ensures that such processing complies with the GDPR.

3.1 Measures to ensure compliance with the GDPR principle of integrity and confidentiality in relation to personal data

94. Gatekeepers' measures designed to safeguard the integrity of the gatekeeper's hardware or operating system and/or applied to enable end users to protect their security from being undermined in accordance with Article 6(4) DMA are consistent with the gatekeepers' obligation under Article 32 of the GDPR to ensure a level of security of personal data appropriate to the risk.

95. For example, Article 6(4) of the DMA allows measures to prevent the transmission of malicious code that may compromise an end user's security or disrupt the functioning of the operating system or the hardware, or to impede software which disables or alters the normal functioning of the operating system or the hardware. Similarly, gatekeepers may enable end users to decide whether they allow beneficiaries under Article 6(4) of the DMA, such as third-party app and app store providers ("Article 6(4) DMA beneficiaries"), to gain access to certain sensitive information such as location, photos, or contacts. When doing so, gatekeepers may offer end users the possibility to limit access to such sensitive information (e.g., once, while using the app, or not to allow such access altogether) provided that gatekeepers also offer those possibilities to end users of their own services, and that they do not impose more restrictive measures on third-party app or app store providers than they apply to their own services.

96. In addition, measures such as requiring the encryption of network connections, which may not be strictly related to protecting the integrity of the device or its operating system, or to enabling end users to protect their security, may be necessary for the gatekeeper's compliance with its obligations under Article 32 of the GDPR and therefore in line with Article 8(1) DMA.

97. Gatekeepers may also need to take additional appropriate measures, alone or jointly with developers of third-party apps or app stores, to comply with their obligations stemming from the GDPR, while ensuring that those measures do not contradict or unjustifiably frustrate the effective implementation of Article 6(4) of the DMA or other DMA provisions. Appropriate measures may, in particular, include targeted technical and organisational measures enabling the effective handling, alone or jointly with relevant Article 6(4) DMA beneficiaries, of personal data breaches to ensure compliance with Articles 33 and 34 of the GDPR. These targeted measures include, inter alia, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident and should be appropriate to comply with the GDPR and other legal requirements including, but not limited to, legal requirements stemming from the Cyber Resilience Act.[88]

[88] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), OJ L, 2024/2847, 20.11.2024.

DRAFT

98. Data processing by the gatekeeper has to have due regard for requirements stemming from Article 5(3) of the ePrivacy Directive. This means that the gatekeeper has to obtain the end user's consent for storing information or gaining access to information already stored in terminal equipment, unless the processing is strictly necessary to provide an information society service explicitly requested by the end user. This exemption to the consent rule under Article 5(3) of the ePrivacy Directive may for instance be relied upon for storing information or for gaining access to information stored in the terminal equipment of end users if these operations are strictly necessary for maintaining the security of the operating system and are user-centric (e.g., setting of a cross-side request forgery token on the user's device).[89] By contrast, when storing information or gaining access to information stored in the terminal equipment does not pursue well-specified security-related purposes (e.g., combatting ad fraud), they cannot reasonably be considered to meet the criterion of the exemption.

3.2 Other measures gatekeepers should take to comply with the GDPR and facilitate compliance of Article 6(4) DMA beneficiaries with the GDPR

99. Gatekeepers are required to adopt other appropriate technical and organisational measures to ensure and demonstrate compliance with their obligations under Article 5(1), point (f) and 5(2), Article 24, Article 25 and Article 32 of the GDPR. For example, gatekeepers should offer access to data, sensors and services on a granular basis to ensure that the beneficiaries of Article 6(4) of the DMA can selectively access only the parts of the operating system and the data that are necessary for the distribution and functioning of the respective apps or app stores. Such measure should ensure that Article 6(4) DMA beneficiaries, can have sufficiently granular control in the application programming interface ('API") of the gatekeeper so that they may limit their access to only that data which they deem necessary for the functioning of their respective app or app store.[90]

100. Gatekeepers should also implement certain additional measures to demonstrate their compliance with the GDPR and to enable Article 6(4) DMA beneficiaries to comply with their obligations under the GDPR, such as:

a. enabling providers of apps or app stores to seek valid consent to process data stored on the device of the end-user by enabling them to present interfaces with consent prompts in the operating system of the gatekeeper. In this context, the gatekeeper should not impose any requirement on providers of apps or app stores related to whether to seek consent and the format of the interfaces for seeking end users' consent. Where gatekeepers make defaults available to facilitate app developers' own compliance with the GDPR, such formats should not make collection of consent more burdensome than for the gatekeeper's own services, and should allow app developers to configure the interface to ensure consent is informed and complies with all GDPR requirements;[91]

[89] Article 29 Data Protection Working Party Opinion 04/2012 on Cookie Consent Exemption, adopted on 7 June 2012, Section 3.3.

[90] While gatekeepers are required to make available an API which allows for granular access by third party beneficiaries, such as developers, it is the responsibility of the app developers to only seek access to data which is necessary for the functioning of their respective app.

[91] It should be noted that in cases where joint controllership does arise (e.g., where app developers decide to rely on an advertising identifier provided by the gatekeeper), the gatekeeper providing this identifier and third-party beneficiary may need to reach an agreement on the content and format of the consent request.

DRAFT

b. providing additional protections from malware, such as by making available a secure storage space dedicated to the local storage of data, and making available state-of-the-art encryption functionalities to applications; and

c. enabling app developers to deliver adequate information about the app and app store, including the types of data the app or app store is able to process and for what purposes.

101. When offering these features, gatekeepers should refrain from imposing, either technically or contractually, how Article 6(4) DMA beneficiaries comply with the GDPR as independent controllers. In particular, gatekeepers should not in any way prescribe whether, how, and when Article 6(4) DMA beneficiaries are to seek consent for the collection of data, restrict the further processing of data that was collected for a specific purpose, nor limit the types of processing which beneficiaries may carry out as separate and independent controllers.[92] Article 6(4) DMA beneficiaries should, as separate and independent controllers, remain free to opt for gatekeepers' measures made available to them (such as the ones listed in paragraph 100) as optional features or to differentiate their offering based on enhanced privacy measures.

4 Right to data portability of end users and third parties authorised by end users (Article 6(9) DMA)

102. Article 6(9) DMA requires gatekeepers to "*provide end users and third parties authorised by an end user, at their request and free of charge, with effective portability of data provided by the end user or generated through the activity of the end user in the context of the use of the relevant core platform service, including by providing, free of charge, tools to facilitate the effective exercise of such data portability, and including by the provision of continuous and real-time access to such data*".

103. Article 6(9) DMA enshrines the right to data portability for end users of CPSs listed in the designation decisions for gatekeepers pursuant to Article 3(9) DMA. As part of this right, the end user can also authorise third parties to access and port data that the end user provided or generated through the use of a designated CPS. Recital 59 DMA further explains that Article 6(9) DMA is not only an enabler for effective switching and multihoming, but also an enabler for innovation in the digital sector, for instance by giving rise to new business models or encouraging the evolution of existing models, which both serve the overarching DMA objective to promote contestability in the digital sector.[93]

104. Article 6(9) DMA complements the data portability right established by Article 20 GDPR,[94] insofar as the requesting end user under Article 6(9) DMA is also a data subject as defined by the GDPR. The data portability right enshrined in Article 20 GDPR applies to personal data that has been processed by automated means on the

[92] In cases where joint controllership does arise, however, the gatekeeper and third-party beneficiary will need to put in place an arrangement which determines their respective responsibilities for compliance with the obligations under the GDPR in accordance with Article 26 GDPR. See also EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, adopted on 7 July 2021, paragraphs 161-170.

[93] Recital 59 DMA: "[…] *To ensure that gatekeepers do not undermine the contestability of core platform services, or the innovation potential of the dynamic digital sector, by restricting switching or multi-homing, end users, as well as third parties authorised by an end user, should be granted effective and immediate access to the data they provided or that was generated through their activity on the relevant core platform services of the gatekeeper. Facilitating switching or multi-homing should lead, in turn, to an increased choice for end users and acts as an incentive for gatekeepers and business users to innovate*".

[94] Recital 59 DMA.

DRAFT

basis of the data subject's consent,[95] or in order to perform a contract entered into by the data subject.[96] Article 6(9) DMA differs from Article 20 GDPR because among others it applies irrespective of the lawful ground under which data has been processed by the gatekeeper under the GDPR and requires gatekeepers to enable continuous and real-time data portability to end users or third parties authorised by them. Portability under Article 6(9) DMA should also be enabled by gatekeepers at no additional cost to end users or authorised third parties.

105. Given that Article 6(9) DMA establishes a clear legal obligation for gatekeepers to enable data portability, the applicable lawful ground for gatekeepers to port personal data that falls in the scope of Article 6(9) DMA to end users, or third parties authorised by end users, is Article 6(1), point (c) GDPR.

106. As with Article 20 GDPR data portability requests, and while gatekeepers are likely to be qualified as controllers in relation to the porting of personal data under Article 6(9) DMA, gatekeepers fulfilling data portability requests under the conditions set forth in Article 6(9) DMA are not responsible for the subsequent processing of data by the end user or authorised third party receiving the data.[97] Authorised third parties act upon request of the end user and are likely separate controllers of the end user's data in relation to such subsequent processing (where end users are data subjects), notably when the data of the end user is directly transmitted to the third party. Where an end user qualifies as a controller in relation to the subsequent processing, any third party that they authorise to access the personal data may act as a processor on behalf of the end user. In such a situation, the end user and the authorised third party are required to enter into a contract in accordance with Article 28(3) GDPR.[98] The gatekeeper is therefore not responsible for compliance of the authorised third party or the end user with data protection legislation.

4.1 Data categories to which the right to portability under Article 6(9) DMA applies

107. Article 6(9) DMA applies to a broad range of data, covering both data that is actively provided by the end user (e.g., identification data provided when signing up for the CPS) and data that is generated through the activity of the end user in the context of the use of the relevant CPS, which includes data created by the end user through their use of the CPS or at the request of the end user of a CPS (e.g. playlists saved by the end user) and data that is observed by the gatekeeper from the end user's behaviour, such as user engagement with the CPS. However, Article 6(9) DMA does not cover data that gatekeepers create on the basis of the data provided by the end user or based on the end user's activities on the CPS (i.e., derived or inferred data).

108. Data within the scope of Article 6(9) DMA also covers data that is processed (including automatically) by the gatekeeper CPS, such as the IP address, location and device settings of an end user, as well as data that is exclusively processed on device.[99] As indicated in paragraph 105 above, personal data categories to which the right to

[95] Articles 6(1)(a) and 9(2)(a) GDPR.
[96] Article 6(1)(b) GDPR.
[97] See also Article 29 Working Party Guidelines on the right to data portability (WP242 rev.01), as last revised and adopted on 5 April 2017, p. 6.
[98] E.g., where end users port and then re-use personal data for their own business purposes and engage the authorised third party to provide services that entail the processing of such personal data on their behalf. See also recital 14 DMA.
[99] Data that has been provided or generated in the context of digital services is increasingly being processed and stored on the devices of end users. This development is particularly relevant to certain categories of CPSs and may be driven by the use of new processing technologies, such as artificial intelligence.

DRAFT

portability under Article 6(9) DMA applies can lawfully be ported by the gatekeeper on the basis of Article 6(1), point (c) GDPR.

109. On-device data that is provided or generated in the context of the use of a CPS falls within the scope of Article 6(9) DMA, irrespective of whether the gatekeeper makes use of such on-device data. To ensure compliance with Article 6(9) DMA, gatekeepers have to enable the portability of such data at the request of end users or authorised third parties, such as third-party services or apps installed on a device. Appropriate technical solutions will enable end users, or third parties authorised by them, to access data directly on device for data porting, which may also include wired or wireless device-to-device transfer, where appropriate. In line with the GDPR principles of data minimisation and purpose limitation, enabling device-to-device portability should not result in further access to on-device data by a gatekeeper.

110. In line with the objectives of Article 6(9) DMA, data portability solutions should enable immediate and effective access to on-device data by the end users, or third-party authorised by the end user, and should be capable of supporting multi-homing and switching of services and devices by the end user. However, and also since access to on-device data would likely qualify as access to information stored in the terminal equipment of the end user under Article 5(3) ePrivacy Directive, access to the data by the gatekeeper for the purposes of porting it to the end user or an authorised third party should only take place after the request of the end user or a duly authorised third party. In that manner, the access would be considered as "*strictly necessary in order to provide an information society service explicitly requested by the* (...) *user*" within the meaning of Article 5(3) ePrivacy Directive.

111. In the context of their obligation to ensure and demonstrate compliance with Article 6(9) DMA, gatekeepers should keep an internal list of all categories of data that can be ported under that provision.

4.2 Portability of other data subjects' personal data

112. The obligation in Article 6(9) DMA also applies to personal data of data subjects other than the end user of the relevant CPS, where the dataset whose portability is requested by the end user or an authorised third party also contains such personal data. Unlike Article 20 GDPR, data within the scope of Article 6(9) DMA are not limited to personal data concerning the data subject/end user, but also include personal data concerning other data subjects, as long as such data is provided by the end user or generated through the activity of the end user in the context of the use of the relevant CPS. This means that gatekeepers are also legally obliged, within the meaning of Article 6(1), point (c) GDPR, to give access to personal data of individuals other than the end user upon a request of the end user or of an authorised third party, if there is personal data concerning those other individuals in the relevant dataset.

113. While gatekeepers are not responsible for the subsequent processing of the ported data, the gatekeeper nevertheless has to ensure appropriate information about the recipients of the ported data in line with the transparency obligations enshrined in the GDPR.[100] In addition to providing information about the categories of recipients who may obtain personal data as a result of a portability request under Article 6(9) DMA (e.g., via a privacy notice), data subjects other than the end user requesting portability (as long as

[100] Articles 13(1)(e) and 14(1)(e) GDPR requires controllers to inform data subjects about the recipients or categories of recipients of their personal data.

DRAFT

the gatekeeper has previously identified them)[101] should also be provided with a link to a dashboard listing the specific recipients to whom their personal data has been disclosed.[102] A hyperlink to this dashboard may be included in the CPS's privacy notice.

114. To help ensure that the exercise of the right to data portability by an end user under Article 6(9) DMA does not disproportionately affect the rights and freedoms of data subjects concerned by the portability request other than the end user, gatekeepers should also make available to the end user or the authorised third party relevant tools to exclude from the dataset to be ported parts of the dataset that contain personal data of individuals other than the end user,[103] while warning the end user or the authorised third party that they are responsible for the processing of the personal data of other individuals that they are requesting.

115. In relation to the subsequent processing of the ported data, end users or authorised third parties that do not process the personal data of those other individuals for a purely personal or household activity[104] are bound by the GDPR and have to comply with its requirements in relation to the personal data of those other individuals. This includes the requirements of informing data subjects about the processing of their personal data and of relying on an appropriate lawful ground for such processing.[105]

116. To facilitate compliance by the end user or the authorised third party with the GDPR, while there is no legal obligation to do so, the gatekeeper may also make available tools to enable requesting end users or authorised third parties, on a voluntary and optional basis, to establish contact with individuals other than the end user, notably where gatekeepers are in a position to identify those individuals in the dataset to be ported. If the gatekeeper has not yet identified other data subjects within the dataset, the gatekeeper does not need to take active measures to identify those other data subjects for the sole purpose of enabling the end user or the authorised third party to establish contact with individuals other than the end user. In that case, it is the responsibility of the end user or the authorised third party, as a separate controller, to ensure compliance with the GDPR for portability requests involving the indirect collection of other individuals' personal data, including the GDPR principles of transparency and lawfulness of processing.

4.3 Granularity and duration of portability

117. In order to ensure end users have and keep control of their personal data,[106] gatekeepers should ensure that requesting end users and third parties authorised by end users have

---

[101] Article 11(1) GDPR.

[102] See case Judgment of the Court of Justice of 12 January 2023, *RW v Österreichische Post AG*, C-154/21, ECLI:EU:C:2023:3, paragraph 46, and Article 29 Working Party Guidelines on transparency under Regulation 2016/679 (WP260 rev.01), as last revised and adopted on 11 April 2018, p. 37: "*The actual (named) recipients of the personal data, or the categories of recipients, must be provided. In accordance with the principle of fairness, controllers must provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers opt to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipients (i.e. by reference to the activities it carries out), the industry, sector and sub sector and the location of the recipients*."

[103] See, by analogy, Article 29 Working Party Guidelines on the right to data portability (WP242 rev.01), as last revised and adopted on 5 April 2017, p. 11.

[104] See Article 2(2)(c) GDPR.

[105] See Articles 13, 14, and 6(1) GDPR.

[106] Recital 7 GDPR.

DRAFT

clarity and control over the precise datasets that they wish to port, including the frequency and duration of such porting.

118. Data portability should be enabled for specific subsets of end user data, both in terms of the kind (e.g., messages, photos, videos or documents) and formats of data to be ported. Data that is ported under Article 6(9) DMA should be received in a format that can be immediately and effectively accessed and used by the end user or the relevant third party authorised by the end user to which the data is ported.[107]

119. End users should also be able to select the applicable timeframe within which the data to be ported was provided or generated, taking into account appropriate time ranges for the specific data and use cases at stake, and including both past and future timeframes.

4.4 Real-time and continuous data access

120. Whilst many data requests may concern one time data transfers or downloads, the obligation for gatekeepers to enable continuous and real-time access to data requires the porting of data from, or through a CPS, to a third-party service or product on an uninterrupted basis. Such data portability is particularly essential to the DMA's objectives of facilitating multihoming and switching of services by end users and enabling the creation of innovative services. Real time and continuous data portability is also crucial to fostering innovation of third-party services, by addressing data accumulation by gatekeepers and providing a stable source of data for the improvement and creation of new services across various sectors.

121. The obligation to enable real time and continuous data access requires gatekeepers to ensure that the data within the scope of Article 6(9) DMA is consistently updated, as soon as possible after such information has been provided or generated within the context of the use of a CPS to enable synchronisation between their personal data on the CPS and on any external services they choose to transfer it to. It should be possible for an end user, or a third party authorised by an end user, to simultaneously request both the porting of historic data provided or generated up until the porting request, as well as continuous and real-time data access for the future.

122. End users and authorised third parties should be able to request real time and continuous data portability for meaningful periods of time, including indefinitely (i.e., while the contractual relationship between the end user and the gatekeeper lasts). This does not preclude the gatekeeper from providing end users with additional options for data porting, to ensure end users have control of their personal data. Gatekeepers have to ensure the security of personal data when providing continuous and real-time access, including protection against unauthorised processing.[108]

123. In principle, and unless explicitly requested by the end user, reminders of ongoing data portability should only be sent by the gatekeeper at the end of the requested period, and before expiry of such a period so that the end user may renew the data porting concerned. However, it may be reasonable for gatekeepers to implement periodic reminders to end users, in order to ensure that they remain in control of their personal data portability choices. Periodic reminders will be particularly appropriate where an end user has requested portability for 12 months or longer, and in all cases, should not be sent more often than every 3 months. Particular care should be taken to avoid overwhelming end users with information, for example by providing the option of a

[107] Recital 59 DMA.
[108] See Articles 5(1)(f) and 32 GDPR.

DRAFT

digest, which summarises all ongoing data portability flows, in place of individual reminders for each ongoing flow. In any case, end users should remain in control and be able to customise how often they want to be reminded about their portability choices, and to disable reminders from the gatekeeper if so desired.

124. Taking into account the state of the art of available technical solutions for each CPS, the gatekeeper is required to use appropriate and high-quality technical measures, such as application programming interfaces (APIs)[109] that are capable of enabling access to consistently updated data by end users and authorised third parties. Such technical measures should be made easily accessible to end users and authorised third parties and the data should be provided in a format that allows end users or authorised third parties to immediately and effectively access and use it. In order to ensure that portability solutions made available by gatekeepers are as effective as possible, gatekeepers should ensure appropriate visibility and accessibility of the data portability solutions, including by having dedicated and easily accessible data portability online interfaces, and by providing end users and interested third parties with comprehensive documentation for accessing the tools, such as any rules of access and use, the application process, a data scheme, technical solutions, and timescales.

4.5 Online choice architecture

125. To request data portability from a CPS, end users will inevitably interact with consent screens and other interfaces designed by gatekeepers. Gatekeepers should not engage in behaviours that would undermine the effectiveness of the DMA's obligations, including the design used by the gatekeeper, the presentation of end-user choices in a non-neutral manner, or using the structure, function or manner of operation of a user interface or a part thereof to subvert or impair user autonomy, decision-making, or choice.[110] As a general rule, gatekeepers should be prohibited from engaging in any behaviour that would undermine effective compliance with the DMA's obligations,[111] regardless of whether that behaviour is of a contractual, commercial, technical or of any other nature, or consists in the use of behavioural techniques or interface design.[112]

126. Gatekeepers should therefore ensure that the design of data portability interfaces and the user journey for requesting and consequently carrying out data portability are sufficiently clear and user-friendly. Furthermore, portability options and the wording used to describe them should be provided in a neutral and objective manner and should not nudge end users towards a specific choice. These considerations apply equally to the interfaces on which the end user initially makes a data portability request, authorises third parties to port data, as well as subsequent reminders and authorisation renewals presented by the gatekeeper to the end user.

127. Similarly, documentation and data portability interfaces made accessible by gatekeepers to third parties should not undermine the effectiveness of Article 6(9) DMA, including by the use of incomplete or misleading information about the rights of authorised third parties under Article 6(9) DMA.

4.6 Authorised third parties

128. The role of authorised third parties under Article 6(9) DMA is a key factor in enabling effective data portability and innovation in the digital sector. Gatekeepers can therefore

[109] Recital 59 DMA.
[110] Recital 70 DMA.
[111] See Article 8(1) DMA.
[112] Article 13(4) DMA.

DRAFT

not restrict, in any way, the data portability use cases and business purposes that authorised third parties can pursue with the data they receive under Article 6(9) DMA.

129. Article 8(1) DMA provides that DMA compliance is without prejudice to compliance with other legal obligations, including the GDPR, which provides for the principle of integrity and confidentiality under Article 5(1), point (f) GDPR and the requirement to ensure security of processing in Article 32 GDPR. In particular, gatekeepers are required to implement appropriate technical and organisational measures to prevent unauthorised or unlawful disclosure of personal data to unauthorised third parties.

130. As far as organisational measures are concerned, the gatekeeper, within the framework of its onboarding processes,[113] can request third parties' identity details and information on whether, and to what extent, the data to be ported will involve the transfer of personal data outside the EEA to a third country that has not been recognised as providing an adequate level of protection by the Commission (see paragraphs 136 to 138).

131. However, gatekeepers should not make data portability conditional upon the business use case or purpose for which the ported data will be used by the authorised third party. Gatekeepers should also not gather information pertaining to the authorised third party's compliance measures under the GDPR, including potential administrative or judicial proceedings the third party has undergone in relation to compliance with the GDPR, or whether the third party has suffered breaches of data security in the past. Such information would not necessarily be an indicator of future compliance or the security of an application or related processing, and as such is not strictly necessary to comply with the gatekeeper's own responsibility under the GDPR.

132. As far as technical measures are concerned, the gatekeeper should establish authentication procedures to ensure that the gatekeeper only processes data portability requests where the end user or a third party duly authorised by the end user are the ones making such requests. Without proper authentication procedures (including to verify the authorisation granted by end users to a requesting third party), there is a risk of disclosure of personal data to unauthorised third persons and thus of processing that breaches Articles 5(1), point (a) GDPR and other provisions of the GDPR, including Article 5(1), point (f), Article 24(1) and Article 32(1) GDPR.

133. The GDPR does not specify exact methods for authenticating data subjects. Authentication of the requesting end user will be presumed to have occurred in instances where the end user is already signed in to a user account associated with the relevant CPS or where the end user signs into the CPS as part of an authorisation procedure prompted by the authorised third party. In the same vein, when gatekeepers accept an end user's identity in daily operations (e.g., where an end user of a CPS that does not require a login is uniquely identified by the gatekeeper via other means) then no additional information should be requested from that end user when receiving a portability request. However, where there are reasonable doubts about a data subject's identity, Article 12(6) GDPR states that the controller can ask the data subject to provide additional information. In such cases, the gatekeeper, when acting as a

[113] Gatekeepers have implemented different processes and systems that enable authorised third parties to receive data under Article 6(9) DMA. Depending on the specific processes or systems implemented by a gatekeeper, third parties may either be onboarded onto these systems *prior to* receiving end user authorisation, or *after* authorisation by end users.

DRAFT

controller, has to observe Article 5(2) of the GDPR and be able to justify its doubts, as required by the principle of accountability.

134. Gatekeepers should keep proof of the authorisation obtained from end users by third parties as well as the duration of the authorisation.

135. The gatekeeper is also responsible for taking all the security measures needed to ensure that personal data is securely transmitted (by the use of end-to-end or data encryption).[114] However, the gatekeeper should not require authorised third parties to meet other security or data protection standards following the transmission of the data, including those of the gatekeeper.

4.7 Right to portability and international transfers of personal data

136. In certain circumstances, compliance by the gatekeeper with the portability requests initiated by end users or third parties authorised by them may involve international transfers of personal data, triggering the application of the rules provided in Chapter V GDPR.

137. In line with Article 45 GDPR, gatekeepers should not restrict in any way portability requests involving the transfer of personal data outside the EEA to a third country offering an adequate level of protection as recognised by a Commission decision.[115]

138. If and when portability requests (initiated by end users or authorised third parties) involve the transfer of personal data outside the EEA to a third country that does not benefit from a Commission adequacy decision, the gatekeeper should seek, in line with the derogation provided in Article 49(1), point (a) GDPR, the end user's explicit and specific consent to the envisaged transfer, after having informed him or her of the possible risks of such transfers due to the absence of an adequacy decision and appropriate safeguards.[116] Such consent, for the purposes of enabling data portability under Article 6(9) DMA, has to comply with all requirements stemming from Article 4(11) and Article 7 GDPR in relation to the envisaged transfer.

5 Right to data access of business users and authorised third parties (Article 6(10) DMA)

139. In order to increase contestability and fairness in the digital sector, Article 6(10) DMA requires gatekeepers "*to provide business users and third parties authorised by a business user, at their request, free of charge, with effective, high-quality, continuous and real-time access to, and use of aggregated and non-aggregated data, including personal data, that is provided for or generated in the context of the use of the relevant CPSs or services provided together with, or in support of, the relevant CPSs by those business users and the end users engaging with the products or services provided by those business users. With regard to personal data, the gatekeeper shall provide for such access to, and use of, personal data only where the data are directly connected with the use effectuated by the end users in respect of the products or services offered*

[114] See also Article 29 Working Party Guidelines on the right to data portability (WP242 rev.01), as last revised and adopted on 5 April 2017, p. 19.

[115] The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, the United States (commercial organisations participating in the EU-US Data Privacy Framework) and Uruguay as providing adequate protection.

[116] EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, Adopted on 25 May 2018, p. 7 and 8.

DRAFT

by the relevant business user through the CPS, and when the end users opt-in to such sharing by giving their consent."

140. The data access obligation laid down in Article 6(10) DMA applies to data provided for or generated in the context of the use of CPSs that are listed in a designation decision addressed to a gatekeeper by the Commission, as well as other services of the gatekeeper, including services provided together with, or in support of, relevant CPSs (examples of such services include payment and identification services), where the data associated with these additional services is inextricably linked to the relevant data access request.[117] Business users of these relevant CPSs, or services provided together with, or in support, of such relevant CPSs, as well as end users of such business users, provide and generate a vast amount of data in the context of their use of the gatekeepers' relevant CPS.[118]

141. Whereas gatekeepers may already enable access to, and use of, some of this data in the context of contractual relationships with business users making use of a gatekeeper's relevant CPS, or services provided together with, or in support, of such relevant CPSs, the extent and granularity of such data access and use may be insufficient to enable business users to take full advantage of such data. Taking into account the general requirement of lawfulness for gatekeepers to process personal data under the GDPR,[119] Article 6(10) DMA clarifies that the sharing of end user personal data under that provision may only take place when business users obtain end users' prior consent,[120] without prejudice to compliance with other rules and principles of the GDPR.

142. The gatekeeper has to provide such data upon request by a business user or a third party authorised by them (i.e. a data processor acting for a business user),[121] free of charge.

5.1 Categories of beneficiaries of the right to data access

143. As defined in Article 2(21) DMA, "business user" refers to any individual or organisation, whether natural or legal, operating in a commercial or professional capacity. Business users of a relevant CPS or services provided together with, or in support, of a relevant CPS, as well as third parties authorised by such business users, are the beneficiaries of the right of access and use of data under Article 6(10) DMA.

144. In the case of third parties directly requesting data on a business user's behalf, gatekeepers may request additional, strictly necessary and justified information, in order to verify the identity of the third party and confirm that the third party is effectively authorised to act on behalf of the business user, particularly where personal data are concerned. Recital 60 DMA clarifies that data access under Article 6(10) DMA may only be granted to third parties acting as processors on behalf of the business user. Where business users authorise third parties to process personal data on their behalf, they can only use processors providing sufficient guarantees that processing will meet the requirements of the GDPR,[122] and both parties are required to enter into a contract in accordance with Article 28 GDPR.

---

[117] Recital 60 DMA.
[118] Recital 60 DMA.
[119] Article 6(1) GDPR.
[120] In the meaning of Article 4(11) GDPR and in compliance with all requirements from that provision and Article 7 GDPR.
[121] Recital 60 DMA.
[122] See Article 28(1) and recital 81 GDPR. See also EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, Adopted on 07 July 2021, paragraphs 93-160.

DRAFT

145. The gatekeeper should establish effective and user-friendly authentication and authorisation procedures, in order to ensure that the gatekeeper only processes data access requests from a business user or a third party duly authorised by the business user. Authentication of a requesting business user may take place via sign in to the relevant CPS and should be presumed to have occurred in instances where the business user is already signed in to a business account associated with the relevant CPS.

146. Where possible, gatekeepers should make technical means available to third parties which allow business users to authorise them to access data under Article 6(10) DMA. For example, APIs which enable the third party to prompt a business user to sign in to the business user account associated with the relevant CPS and confirm that the third party is indeed acting on the business user's behalf.

5.2 Data categories to which Article 6(10) DMA applies

147. Article 6(10) DMA covers a broad scope of data that includes data actively provided by business users (e.g., identification data, product or service data and customer data that has been lawfully obtained) and data that is generated through the activity of the business user and of the business user's end users in the context of the use of the relevant CPS, or services provided together with, or in support, of such relevant CPSs.

148. Generated data will include data created at the request of the business user or through the business user's use of a CPS or services provided together with, or in support of the relevant CPS, as well as data that is observed by the gatekeeper from the business user's use of those services, and the behaviour of end users engaging with the products or services provided by those business users. The scope of data covered by Article 6(10) DMA also extends to other data that is processed (including automatically) by a relevant CPS, or services provided together with, or in support, of relevant CPSs, such as IP address and location data.

149. Whereas business users may be satisfied with access to non-personal data, there are use cases where access to personal data will be deemed relevant by a business user, for example where a business user wants to synchronise or personalise services that it offers to individual end users across various platforms or services, or when a business user wants to access performance data (e.g., crash data) for providing an end user with customer support.[123]

150. In order to ensure that business users have access to the relevant data for their business activities, Article 6(10) DMA extends to end user data that is directly connected with the use made by the end users in respect of the products or services offered by the requesting business user through the relevant CPS, or services provided together with, or in support, of such relevant CPSs, including personal data. However, Article 6(10) DMA does not cover data that gatekeepers create on the basis of the data provided by the end user and/or observed based on the end user's activities on the CPS (i.e., derived or inferred data). To comply with the data minimisation principle under Article 5(1), point (c) GDPR, the gatekeeper only has to make available to the requesting business user or authorised third party personal data of end users that is covered by the scope of Article 6(10) DMA.

151. When access to personal data is deemed relevant by business users, and at their request, gatekeepers should only enable the sharing of personal data if the end users whose

[123] Recital 60 DMA, which contains illustrative examples.

DRAFT

personal data is requested have opted-in to such sharing by giving their consent within the meaning of the GDPR.[124]

152. The data access right in Article 6(10) DMA additionally applies to both aggregated and non-aggregated data. Gatekeepers will have to provide business users, and third parties authorised by business users, with aggregated data that is provided or generated in the context of the use of a relevant CPS, or services provided together with, or in support, of such relevant CPSs. On their end, pursuant to their own obligation under Article 5(1), point (c) GDPR, business users should consider whether the personal data that they request under Article 6(10) DMA is adequate and limited to what is necessary in relation to the purposes for which they will process them (which is not for the gatekeeper to assess before giving access to the data).

153. Gatekeepers will also be required to provide access to data falling within the scope of Article 6(10) DMA that is exclusively processed on a device.[125] To ensure compliance with Article 6(10) DMA, gatekeepers should enable effective, high-quality, continuous and real-time access to on-device data at the request of business users or their authorised third parties. Where personal data is concerned, and in line with the GDPR principles of data minimisation and purpose limitation, enabling business user or authorised third party access to such data under Article 6(10) DMA should not result in further access to on-device data by a gatekeeper itself.

154. In the context of their obligation to ensure and demonstrate compliance with Article 6(10) DMA, gatekeepers are encouraged to keep a record of all categories of data, including personal data, that are provided or generated by business users and end users of business users, in the context of the use of each designated CPS and where relevant, additional services of the gatekeeper, including those provided together with or in support of the relevant CPS.[126]

5.3 Granularity of data access under Article 6(10) DMA

155. Gatekeepers should ensure that requesting business users and their authorised third parties have clarity and control over the precise datasets that they wish to access and make use of, including end user personal data that is directly connected with the use of products or services offered by the relevant business user through the relevant CPS and services provided together with, or in support of, the relevant CPS.

156. At the same time, gatekeepers have to comply with the transparency principle of the GDPR and related transparency obligations before they process personal data access requests by business users or third parties authorised by business users.[127] Gatekeepers should inform end users, through the relevant CPS privacy policies, about the right of business users and third parties under Article 6(10) DMA to request such access to the end user's personal data, subject to the end user's consent. In addition, gatekeepers should inform end users about specific recipients of their personal data pursuant to

[124] See Article 2(32) DMA: "'*consent means consent as defined in Article 4, point (11), of Regulation (EU) 2016/679*" and Article 6(1), point (a) GDPR.

[125] Data that has been provided or generated in the context of digital services is increasingly being processed and stored on the devices of users. This development is particularly driven by the use of new processing technologies, such as artificial intelligence.

[126] Such a record is without prejudice to the record-keeping obligations of gatekeepers pursuant to Article 30 GDPR.

[127] Article 5(1), point (a), Article 12, Article 13 and Article 14 GDPR.

DRAFT

Article 6(10) DMA via a dedicated dashboard[128] (a link to which may be included in the CPS's privacy policy). This is particularly important given that the interface where end users consent to provide access to a business user, or a third party authorised by the business user, will generally be offered by the gatekeeper and not the business user.

157. Data access should be enabled for any business user data and end user data that is within scope of the obligation laid down in Article 6(10) DMA. For example, this includes business performance data, end user engagement data, end user payment history, etc. Data should be made available at a level of granularity that provides the most utility to business users and third parties authorised by business users, in light of the DMA's objective of facilitating access to effective and high-quality data (including personal data) through Article 6(10) DMA. Where a business user requests data relating to its end users but does not require personal data, the gatekeeper should provide access to a suitably granular aggregated dataset that does not contain personal data.[129]

158. Business users and third parties authorised by business users should also be able to select the applicable timeframe within which the data to be accessed or used was provided or generated. It should be possible to customise the timeframe of a data access request.

5.4 Mechanism(s) enabling access to end-user's personal data

159. The applicable lawful ground for gatekeepers to grant access to end users' personal data under the scope of Article 6(10) DMA to business users or third parties authorised by business users, is Article 6(1), point (c) GDPR, since a legal obligation to share personal data is established by the DMA for the gatekeeper. At the same time, this legal obligation is only triggered for gatekeepers if the personal data is directly connected with the use made by end users in respect of products or services offered by business users in the context of the use of relevant CPS, or services provided together with, or in support, of such relevant CPSs, and once the business user has obtained consent within the meaning of the GDPR.[130]

160. The gatekeeper's core obligation in this regard is therefore to provide mechanism(s) "*to enable business users to obtain consent of their end users for such access and retrieval*" under Article 6(10) DMA, in line with recital 60 DMA and Article 13(5) DMA.[131]

161. Through this mechanism, business users should be given an effective possibility to obtain consent for access to an end user's personal data. This can be achieved through a dedicated online interface via the gatekeeper's CPS, which should enable business users to obtain consent fulfilling all the requirements of Article 4(11) and Article 7 GDPR. To ensure that end users' consent is informed, gatekeepers should give business users the opportunity to configure the interface to appropriately reflect the necessary elements of information, notably concerning the data that is requested and

[128] See Article 13(1), point (e) and Article 14(1), point (e) GDPR, Judgment of the Court of Justice of 12 January 2023, *RW v Österreichische Post AG*, C-154/21, ECLI:EU:C:2023:3, paragraph 46, and Article 29 Working Party Guidelines on transparency under Regulation 2016/679 (WP260 rev.01), as last revised and adopted on 11 April 2018, p. 37.

[129] Recital 26 GDPR.

[130] See Article 2(32) DMA: "'*consent means consent as defined in Article 4, point (11), of Regulation (EU) 2016/679*" and Article 6(1)(a) GDPR.

[131] Article 13(5) DMA requires gatekeepers to take the necessary steps to enable business users to directly obtain end users' consent to their processing, where that consent is required under the GDPR or the ePrivacy Directive.

DRAFT

the purpose of its intended use.[132] In order to make such a consent mechanism effective, gatekeepers should also ensure that business users' request to access personal data is sufficiently visible to end users. Gatekeepers also have to ensure that obtaining consent for business users is not more burdensome than obtaining consent from the end users for their own services.[133] They cannot impose additional obstacles or requirements on business users when obtaining consent, compared to what they require for their own services.[134] Gatekeepers should also make available a dedicated online interface through which end users are able to withdraw their consent for access to personal data by specific business users, thereby enabling business users to comply with Article 7(3) GDPR.[135] Where an end user withdraws their consent through the gatekeeper's interface, the gatekeeper should cease to provide access to the end user's personal data to the specific business user concerned, and inform the business user that the end user has withdrawn their consent.[136]

162. Gatekeepers should allow business users to record end users' consent for sharing their personal data with specific business users, in line with the accountability principle under Article 5(2) GDPR.

163. Gatekeepers need to verify that all conditions set under Article 6(10) DMA are fulfilled before granting access to data to a business user or a third party authorised by a business user. In relation to personal data, this entails verifying whether end users have consented to the sharing of their personal data with business users or third-party processors authorised by business users. Thus, gatekeepers should keep a record of end users' consent for sharing their personal data with specific business users. However, gatekeepers are not responsible for ensuring the validity of end users' consent and should therefore not assess or verify whether the consent obtained by business users complies with the requirements of the GDPR, which is the responsibility of the businesses users and is to be monitored by the competent data protection supervisory authorities.

164. Reminders about ongoing data access under Article 6(10) DMA should be sent just before the expiry of the data access period consented to by the end user, so that the end user may renew the data access concerned or withdraw its consent. It may however be reasonable for gatekeepers to implement periodic reminders to end users having consented to the use of their personal data by business users, or third parties authorised by the business users, for 12 months or longer, in order to ensure that end users remain in control of their choices concerning data access. Such reminders should not be sent more often than every 3 months. It may also be appropriate to implement options such as ongoing data consent summaries or digests in place of individual reminders for each instance of data access by specific business users, to avoid overwhelming the end user with reminders if they have consented to sharing personal data with a large number of business users. In any case, end users should remain in control and be able to customise how often they want to be reminded about their data access choices, and to disable reminders from the gatekeeper if so desired.

---

[132] See, for the minimum requirements for consent to be considered 'informed' under Article 4(11) GDPR, EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1, Adopted on 4 May 2020, paragraph 64.
[133] Article 13(5) DMA.
[134] Recital 60 DMA.
[135] EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1, Adopted on 4 May 2020, paragraph 114.
[136] See, by analogy, Judgment of the Court of Justice of 27 October 2022, *Proximus NV v Gegevensbeschermingsautoriteit*, C-129/21, ECLI:EU:C:2022:833, paragraph 85.

DRAFT

5.5 Continuous and real-time data access

165. The obligation on gatekeepers to enable continuous and real-time access to data under Article 6(10) DMA requires access to data on an uninterrupted basis. It should also be possible for a business user or authorised third party to simultaneously request both access to historic data provided or generated up until the access request, as well as continuous and real-time data access for the future, including where the personal data of end users is concerned, where end users have given valid consent.

166. By requiring continuous and real-time access to data, including the personal data of end users, Article 6(10) DMA aims to ensure that business users and authorised third parties can access up-to-date information and maintain synchronisation between their data on the platform and any external services they choose to transfer it to as long as third party service providers process data only on their behalf.

167. In line with Article 6(10) DMA read in light of recital 60 DMA, gatekeepers should ensure, by means of appropriate and high-quality technical measures, such as application programming interfaces (APIs) or integrated tools for small volume business users, that business users or third parties authorised by business users are provided free and effective access to the data continuously and in real time. APIs should be made easily accessible to business users and authorised third parties and the data should be provided in a format that allows business users or authorised third parties to immediately and effectively access and use it.

168. Gatekeepers should endeavour, taking into account the state of the art of available technical solutions for each CPS, to implement data access solutions that meet the continuous and real time access objective set forth in the DMA. In providing such technical solutions, gatekeepers should implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including protection against unauthorised processing.

169. Business users and authorised third parties should be able to request real time and continuous data access for meaningful periods of time, including indefinitely (i.e., for the duration of the contractual relationship between the business user and the gatekeeper). This does not preclude the gatekeeper from providing business users or authorised third parties with additional options for data access.

170. In order to ensure that access solutions made available by gatekeepers are as optimal and effective as possible, gatekeepers should ensure appropriate visibility and accessibility of those solutions, including by having dedicated and easily accessible business user data access portals, and by providing interested business users and third parties with comprehensive documentation for accessing the tools, such as any rules of access and use, the application process, a data scheme, technical solutions, and timescales.

5.6 Online choice architecture

171. Under Article 6(10) DMA, business users, authorised third parties and end users will inevitably interact with consent screens and other online interfaces designed by gatekeepers. As a general rule, gatekeepers should not engage in behaviours that would undermine the effectiveness of the DMA's obligations, including the design used by the gatekeeper, the presentation of end-user choices in a non-neutral manner, or using

DRAFT

the structure, function or manner of operation of a user interface or a part thereof to subvert or impair user autonomy, decision-making, or choice.[137]

172. Gatekeepers should avoid risks of consent fatigue and strive to enable the most user-friendly consent mechanisms, taking into account the specific characteristics and user-facing interfaces of the relevant CPS, or service provided together with or in support of the CPS. Gatekeepers should endeavour to integrate business user consent requests seamlessly into the end user journey on the user-facing interface (e.g., on the dedicated webpage or product listing of a specific business user, or at the moment of booking or purchase of a business user's service or product). In cases where a potentially high number of business users may request access to data under Article 6(10) DMA and will therefore need to obtain end users' consent before being granted access to personal data of the end users by the gatekeeper, end users should not be overwhelmed with consent requests, in particular where requests are repetitive or disruptive of the end user's experience. Several solutions should be explored by gatekeepers in this regard while maintaining their interfaces user-friendly, such as displaying layered and intuitive consent interfaces to end users where end users can give, review, or modify their consent choices.

173. Furthermore, data access and consent options, including the wording used to describe them, should be provided in a neutral manner and should not nudge users towards a specific choice. These considerations apply equally to the interfaces on which the business user initially makes a data access request, authorises a third party to access data on their behalf, or facilitates the consent of an end user, as well as subsequent reminders and authorisation renewals presented by the gatekeeper to any party in the context of Article 6(10) DMA.

174. Similarly, documentation and online interfaces presented to business users and third parties should not undermine the effectiveness of Article 6(10) DMA, including by the use of incomplete or misleading information about the rights of third parties under Article 6(10) DMA.

6 Access to anonymised ranking, query, click and view data (Article 6(11) DMA)

175. Article 6(11) DMA establishes an obligation for gatekeepers "*to provide to any third-parti undertaking providing online search engines, at its request, with access on fair, reasonable and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on its online search engines. Any such query, click, and view data that constitutes personal data shall be anonymised*".

176. The goal of Article 6(11) DMA is to achieve contestability and fairness for the provision of online search engine services. Article 6(11) DMA aims to level the playing field as regards the data available to undertakings providing online search engines. Third-party undertakings providing online search engines only see a small amount of the queries and user interactions compared to the vast amount seen by gatekeepers providing online search engines designated as CPS, and therefore lack scale in search data that is critical for maintaining and improving search quality. The data sharing obligation under Article 6(11) DMA, as informed by recital 61 DMA, is limited to online search engines operated by gatekeepers designated under the DMA on the one hand, and a specific type of data receivers, namely third-party undertakings

[137] Recital 70 DMA.

DRAFT

providing online search engines or the third parties with whom they have contracted in order to process this data on their behalf as processors, on the other.

177. Article 6(11) DMA read in the light of recital 61 DMA explains that "*a gatekeeper should ensure the protection of the personal data of end users, including against possible re-identification risks, by appropriate means, such as anonymisation of such personal data*[138]" and that this should be done "*without substantially degrading the quality or usefulness of the data*".

178. According to recital 26 of the GDPR relating to the definition of personal data, "*To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments*." The same recital further provides that "*the principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data that has been rendered anonymous in such a manner that the data subject is not or no longer identifiable*" with means reasonably likely to be used. Information relates to an identified or identifiable natural person where, by reason of its content, purpose or effect, it is linked to an identifiable person.[139]

179. Moreover, according to the CJEU, "*pseudonymisation may, depending on the circumstances of the case, effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable*"[140], with the result that the data is not personal for them.[141] However, that presupposes, firstly, that the recipient of the pseudonymised data "*is not in a position to lift* [the technical and organisational] *measures* [implementing the pseudonymisation]" "*during any processing of the* [pseudonymised data] *which is carried out under its control*"[142]. Secondly, it also presupposes that "*those measures must in fact be as such as to prevent* [the recipient] *from attributing those* [pseudonymised data] *to the data subject including by recourse to other means of identification such as cross-checking with other factors, in such a way that, for the* [the recipient], *the person concerned is not or no longer identifiable*".[143] Moreover, "*in the context, inter alia, of a potential subsequent transfer of those data to third parties*" and "*in so far as it cannot be ruled out that those third parties have means reasonably allowing them to attribute pseudonymised data to the data subject, such as cross-checking with other data at their disposal*, *the data subject must be regarded as identifiable as regards both that transfer and any subsequent processing of those data*

[138] Article 4(1) GDPR defines personal data as any information relating to an identified or identifiable natural person.
[139] Judgment of the Court of Justice of 4 September 2025, *EDPS v. SRB*, C-413/23 P, ECLI:EU:C:2025-645, paragraph 55 and case law cited.
[140] *Ibid.*, paragraphs 86 and 87.
[141] *Ibid*., paragraph 75.
[142] *Ibid.,* paragraph 77.
[143] *Ibid.,* paragraph84.

DRAFT

by those third parties. In such circumstances, pseudonymised data should be considered to be personal in nature.[144]

180. When selecting among various possible ways of achieving anonymisation of data of end users shared under Article 6(11) DMA, gatekeepers should select the one that preserves the most quality and usefulness of the data for the third party undertaking requesting access to it, while also ensuring that the shared data of end users is anonymised taking into account all the means reasonably likely to be used by the third party undertaking providing online search engine or by another person to identify end users directly or indirectly.

181. Anonymisation techniques inherently reduce the usefulness of the data for the data receiver. To maximise the level of data quality and usefulness for requesting third-party undertakings providing online search engines in line with the goals of Article 6(11) DMA while ensuring shared data is effectively anonymised in line with Article 4(1) read in conjunction with recital 26 GDPR, anonymisation should be achieved by appropriate technical measures for alteration of the data, complemented by organisational, administrative and contractual measures to mitigate residual likelihood of identification.[145] In this regard, the use of appropriate technical measures that result in the alteration of the data to be provided is indispensable. Organisational, administrative, and contractual measures, when they derive from legally binding requirements imposed on the gatekeeper, in particular through a Commission implementing act (see paragraphs 187 to 189 below), can complement technical measures in order to mitigate residual likelihood of identification, in the specific context of Article 6(11) DMA.[146] For end users' data not to be considered personal data for the requesting third-party undertaking providing an online search engine, the likelihood of identification should be insignificant, taking into account all the means reasonably likely to be used to identify end users. An implementing act under Article 8(2) DMA can, depending on the requirements imposed, have an impact on the means reasonably likely to be used to identify end users and on residual likelihood of identification in the context of Article 6(11) DMA. The effects of the implementing act should be both durable (meaning that the measures cannot be changed at will) and verifiable (meaning that compliance is subject to appropriate monitoring and verification).

182. Taking into account the requirements and considerations in paragraphs 175-181 above, to fulfil the requirements of Article 6(11) DMA, gatekeepers should consider the issues set out in the following two points.

183. First, the gatekeeper needs to evaluate the extent to which the initial dataset (i.e. the ranking, query, click and view data generated by end users) contains personal data of end users. Recital 61 DMA, referring to Article 6(11) DMA, clarifies that what needs to be anonymised is the personal data of the end user generating the data, and not the personal data of other individuals that might be identifiable via ranking, query, click and view data (e.g., a person mentioned in a query). However, the GDPR remains applicable to the sharing of personal data of other individuals that might be identifiable via ranking, query, click and view data by gatekeepers pursuant to their legal

[144] *Ibid.,* paragraph 85.

[145] Recital 61 DMA states that "[t]*he relevant data is anonymised if personal data is irreversibly altered in such a way that information does not relate to an identified or identifiable natural person or where personal data is rendered anonymous in such a manner that the data subject is not or is no longer identifiable*".

[146] In other words, measures other than technical measures for the alteration of data are not sufficient, on their own, to render the likelihood of identification insignificant.

DRAFT

obligation under Article 6(11) DMA and the re-use of the data by the requesting third-party undertakings providing online search engines.

184. When complying with Article 6(11) DMA, gatekeepers should consider both possibilities of direct and indirect identification to determine whether the dataset contains personal data before sharing the dataset with a requesting third party to determine whether appropriate measures should be put in place to anonymise the data of the end user.

185. Particular attention should be given to the means that the requesting third-party undertakings providing online search engine and other persons that would reasonably be considered to be able to gain access or process the data (including unintended third parties) would reasonably likely use to identify the end user generating the data.[147] For information to qualify as personal data, it is not required that all the information enabling the identification of the data subject must be in the hands of one person,[148] in particular the requesting third party undertaking providing an online search engine and receiving Article 6(11) DMA data. Moreover, the assessment of anonymity of end users' shared data should take into account the availability of additional information relating to the end users generating the data via use of the gatekeeper's search engine.[149]

186. Second, the anonymisation approach selected by the gatekeeper should be appropriate to achieve effective anonymisation. There are different measures available to achieve anonymisation. Gatekeepers subject to Article 6(11) DMA should carefully assess the most recent developments in the field of anonymisation and identification when selecting such measures.

187. In this context, account should be taken of the specific regulatory framework of the DMA under which data sharing pursuant to Article 6(11) DMA takes place. This includes, in particular, the fact that such data sharing has a clearly defined scope, which only includes gatekeepers and third-party undertakings providing online search engines or the third parties with whom they have contracted in order to process this data on their behalf as processors. Moreover, the exercise of the Commission's legal powers to regulate data sharing under Article 6(11) DMA via an implementing act pursuant to Article 8(2) DMA should be taken into consideration.

188. Through an implementing act under Article 8(2) DMA, the Commission may specify legally binding measures on gatekeepers to ensure effective anonymisation and on the eligibility of third parties to receive data under Article 6(11) DMA.[150] Such legally binding measures may prescribe conditions and safeguards under which a gatekeeper must share data with eligible third parties under Article 6(11) DMA. This may include the specification of technical measures that result in the alteration of the data to be provided, as well as administrative, organisational, and contractual measures to be

[147] See recital 26 GDPR.

[148] Judgment of the Court of Justice of 19 October 2016, *Breyer v. Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779, paragraph 43. See also Judgment of the Court of Justice of 9 November 2023, *Gesamtverband Autoteile-Handel eV v Scania CV AB*, C-319/22, ECLI:EU:C:2023:837, paragraph 45; Judgment of the Court of Justice of 7 March 2024, *IAB Europe v Gegevensbeschermingsautoriteit*, C-604/22, ECLI:EU:C:2024:214, paragraph 40.

[149] For example, third party undertakings providing online search engines receiving the data may be able to have access to additional information through advertising networks that might enable them to link the data in question to specific individuals.

[150] The Commission may specify via an implementing act the ineligibility of potential third party recipients under Article 6(11) DMA.

DRAFT

adopted by the gatekeeper before sharing data under Article 6(11) DMA. In relation to measures for the alteration of data, these may include the removal of data liable to be used for the identification of the end user generating the search data (e.g., precise location of the end user, queries with words searched below a specific low number of times, and precise time and sequence of click data).[151]

189. In relation to other measures to complement the alteration of data by the gatekeeper to mitigate residual likelihood of identification, the implementing act may specify, for example, measures that restrict data usage (including a prohibition to attempt to re-identify end users), access controls, data retention/storage, general and incident reporting, internal monitoring and supervision, and independent auditing. The implementing act may include an obligation for gatekeepers to contractually impose measures, where appropriate, on eligible third-party undertakings as a condition to access the data. Contractual requirements may, among others, limit onward sharing of the data received by eligible third-party undertakings. The implementing act may also impose specific monitoring obligations on the gatekeeper and also specify appropriate measures that gatekeepers must take in case of an established violation by third-party undertakings providing online search engines of requirements set out in the contract. Such measures may include requiring the gatekeeper to notify the competent data protection supervisory authority in case of an alleged breach of the GDPR,[152] cease sharing data with the third-party undertaking providing an online search engine, and providing it with the contractual right to order the third party to delete any data it received from the gatekeeper.[153] Specific consideration is warranted to ensure that the measures imposed by the implementing act would remain enforceable even after a change of legal and factual circumstances, such as a merger of the third party undertaking providing an online search engine with another company or the third party undertaking providing an online search engine going out of business.

190. Gatekeepers should ensure that access to the dataset is granted on fair, reasonable and non-discriminatory terms in line with Article 6(11) DMA read together with recital 61 DMA. Therefore, measures imposed on third-party undertakings providing online search engines should not constitute a disproportionate burden for the recipients including in terms of cost and processes should be timely, transparent and objective.

7 Interoperability of number-independent interpersonal communication services (Article 7 DMA)

191. The lack of interoperability allows gatekeepers that provide number-independent interpersonal communications services[154] ("NIICS") to benefit from strong network effects, which contributes to the weakening of contestability.[155] Furthermore, gatekeepers often provide NIICS as part of their platform ecosystem, and this further

[151] Other technical measures may include, depending on the context, the application of noise addition or perturbation such as differential privacy techniques, and the use of aggregation methods.
[152] Such notification would appear warranted where there is evidence that the third-party undertaking providing an online search engine receiving data under Article 6(11) DMA has sought to relate the data received to the end users generating the data, in which case the data may no longer be considered anonymous and might lack a legal basis for processing under Article 6(1) GDPR.
[153] In this regard, it is also relevant to note that the gatekeeper and the third-party undertaking providing an online search engine have conflicting interests in relation to the search data sharing under Article 6(11) DMA and that thus the gatekeeper has strong incentives to closely monitor compliance by the third party with the contractual terms.
[154] For the definition of NIICS, see Article 2(9) DMA, referring to the definition contained in Article 2(7) of Directive (EU) 2018/1972.
[155] Recital 64.

DRAFT

exacerbates entry barriers for alternative providers of such services and increases costs for end users to switch.

192. Article 7(1) DMA therefore requires gatekeepers designated in relation to their NIICS to offer interoperability.[156] Interoperability should be provided, at no costs and upon request, for basic functionalities listed in Article 7(2) DMA, to third-party providers of NIICS that offer or intend to offer their NIICS to end users in the Union. By enabling the sharing of network effects, interoperability would ensure increased contestability in relation to the provision of NIICS such as messaging services.

193. To facilitate the practical implementation of Article 7(1) DMA, the gatekeeper concerned is required to publish a reference offer laying down the technical details and general terms and conditions of interoperability with its NIICS.[157] It is possible for the Commission, if applicable, to consult the Body of European Regulators for Electronic Communications, in order to determine whether the technical details and the general terms and conditions published in the reference offer that the gatekeeper intends to implement or has implemented ensures compliance with this obligation.[158]

194. Several clauses in Article 7 DMA contain obligations that are also relevant from the perspective of Union data protection law. Article 7(3) DMA specifies that *"The level of security, including the end-to-end encryption, where applicable, that the gatekeeper provides to its own end users shall be preserved across the interoperable services."* Article 7(8) DMA provides that *"The gatekeeper shall collect and exchange with the provider of number-independent interpersonal communications services that makes a request for interoperability only the personal data of end users that is strictly necessary to provide effective interoperability. Any such collection and exchange of the personal data of end users shall fully comply with Regulation (EU) 2016/679 and Directive 2002/58/EC."* Lastly, Article 7(9) DMA provides that "*The gatekeeper shall not be prevented from taking measures to ensure that third-party providers of NIICS requesting interoperability do not endanger the integrity, security and privacy of its services, provided that such measures are strictly necessary and proportionate and are duly justified*."

195. To establish interoperability, the duties and responsibilities of two parties – i.e., the gatekeeper and the NIICS provider requesting interoperability – should be considered.

196. On the side of the NIICS provider requesting interoperability, the provider will need to comply and implement the technical details and general terms and conditions for interoperability set out by the reference offer of the gatekeeper, including in what concerns personal data processing that is necessary to enable interoperability. From the moment in which interoperability is established, the NIICS provider requesting interoperability is responsible for complying with Union data protection law in relation to the personal data it accesses (e.g., when providing the NIICS to the end user that decides to make use of the interoperable basic functionalities).

197. Pursuant to Article 7(4) DMA, the gatekeeper is required to draft and publish a reference offer with technical details, general terms and conditions on interoperability. The Reference Offer should ensure effective interoperability with the basic

[156] According to Article 2(29) DMA, "'*interoperability' means the ability to exchange information and mutually use the information which has been exchanged through interfaces or other solutions, so that all elements of hardware or software work with other hardware and software and with users in all the ways in which they are intended to function*."
[157] Article 7(4) DMA.
[158] Recital 64 DMA.

DRAFT

functionalities listed in Article 7(2) DMA. Such reference offer and more broadly the gatekeeper's measures to ensure compliance with Article 7 DMA should ensure full compliance with Union data protection law,[159] including that only personal data that is strictly necessary for provision of effective interoperability is processed in compliance with Article 5(1), point (c) GDPR.

198. The implementation of interoperability by the gatekeeper under Article 7 DMA is very likely to fulfil the criteria for the requirement to carry out a data protection impact assessment under Article 35 GDPR[160] which includes an assessment of possible risks to the rights and freedoms of data subjects arising from data exchange that is needed for the purpose of ensuring interoperability, as well as appropriate, timely and effective measures to tackle the risks identified.

199. Under Article 7(8) DMA, the gatekeeper has to ensure full compliance with Union data protection legislation when sharing personal data with providers of NIICS requesting interoperability. In particular, the gatekeeper is obliged to collect and share only personal data that is strictly necessary to provide effective interoperability and so in line with GDPR and the ePrivacy Directive. In line with Article 5(1), point (c) GDPR, controllers should consider if the purpose of the processing requires use of personal data or if anonymised data can be used and using the latter where possible. This data minimisation principle is particularly relevant in the case where gatekeepers need to collect additional personal data from end users that the gatekeeper does not use itself when providing its own communication service, for the sole purpose of providing effective interoperability, while meeting all requirements of Article 7 DMA and Union data protection law, in particular to maintain the level of security across interoperable services.

200. The other parts of this section look at the interplay between Union data protection law and the DMA, in relation to the categories of personal data that are necessary for the provision of interoperability (cf. section 7.1), personal data processing to preserve the level of security across interoperable services (section 7.2) and other situations where personal data processing may take place in the context of Article 7 interoperability (section 7.3).

7.1 Categories of personal data necessary to ensure interoperability

201. Personal data needed to ensure interoperability can be separated in the following three major categories:

a. the message content themselves that would be exchanged between servers of the gatekeeper and those of the other providers.

b. the personal data that is needed to ensure technical aspects of interoperability between the NIICS of the gatekeeper and of the provider requesting interoperability, including to ensure that end users of the different NIICS can address each other and communicate.

[159] Article 8(1) DMA.

[160] See Article 29 Data Protection Working Party 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 (WP 248 rev.01), As last Revised and Adopted on 4 October 2017, p. 10. Interoperability under article 7 DMA is likely to satisfy more than two of the criteria mentioned, i.e. it relates to data of a highly personal nature (electronic communications whose confidentiality should be protected), is large scale, and relies on innovative technical processes.

DRAFT

c. personal data that gatekeepers may process to ensure that the level of security they provide to their own end users is preserved across the interoperable services, in line with Article 7(3) DMA.

202. In relation to point b. in paragraph 201, gatekeepers need to decide how to resolve identities across the different NIICS. Users of a NIICS may obtain the identity of a user of another NIICS "out of band" (i.e. via a separate, independent communication channel, such as by email or verbally). Gatekeepers should then ensure that their end users have requested to use interoperable features from specific alternative NIICS before enabling end users of those NIICS to communicate with their end users. Furthermore, in light of Article 7(7) DMA, it is important that gatekeepers raise their end users' awareness by informing them about the possibility to communicate across NIICS, including whenever a third party NIICS becomes interoperable with the gatekeeper's NIICS.

203. In line with Article 7(7) DMA, end users of the gatekeepers' NIICS and of the third party NIICS need to remain free to decide whether to make use of the interoperable basic functionalities that may be provided by the gatekeeper pursuant to Article 7(1) DMA. This means that end users should be free to decide whether to engage in conversations and be discoverable by users of third-party NIICS, including through automated discovery mechanisms that might entail the sharing of data that is not strictly required to ensure interoperability between the gatekeeper and the alternative NIICS provider where applicable. End users should remain free to opt-in to those mechanisms.

204. It is also relevant that the interoperability requests displayed to users specify the NIICS providers (i.e., the new controllers) that would gain access to some necessary end users' personal data. If the number of providers of NIICS achieving interoperability becomes very significant, gatekeepers may want to avoid 'choice fatigue' by requesting end users to make their choices in parallel to "moments of discontinuity" in their relationship with end users (e.g. the moment of subscription, of a software update or during a communication campaign), or when the end user of an interoperable NIICS tries to initiate a communication. They may also implement simple interoperability management systems where end users can give, review, or modify their interoperability choices across multiple providers at once (while keeping the possibility to go granular if the user wishes to), thereby reducing repetitive requests. If end users accept the exchange of identity data between the gatekeepers and providers of other NIICS requesting interoperability, and the gatekeeper and the provider requesting interoperability establish a common naming convention, exchanging only the information defined in the convention (including the end user's identifier in each of the NIICS) might be considered "strictly necessary" in accordance with Article 5(1), point (c) GDPR.

7.2 Personal data processing to preserve the level of security across interoperable services

205. Under Article 7(3) DMA, gatekeepers are required to preserve the level of security across interoperable services. In cases where the gatekeeper offers end-to-end-encryption to its end users of its NIICS, such encryption should be preserved across the interoperable services. End-to-end-encryption ("E2EE") is generally understood as a technology that encrypts the content data on the end device of the sending party and decrypts it on the end device of the addressed recipient in such a way that only the sender and the recipient, at the exclusion of any third party, including the carrier or the

DRAFT

chain of involved carriers, can access and control the content data of the communication.[161] Maintaining trustworthy E2EE through the process of interoperability is key to ensure that the standard of security remains the same for end users in all services.

206. Ensuring E2EE across interoperable NIICS is a task that requires both the gatekeeper and the NIICS provider requesting interoperability to actively cooperate. In that context, the implemented libraries and software solution should be well defined.

207. From a data protection point of view, implementing a well-defined protocol for managing the exchange and certification of cryptographic keys between gatekeepers and providers of NIICS requesting interoperability would greatly contribute to a secure foundation for a reliable implementation of E2EE. From the perspective of the purpose limitation principle under Article 5(1), point (b) GDPR, gatekeepers should also consider appropriate measures to ensure that the different service providers can only use the keys as well as any other corresponding content exchanged for key agreement received from the gatekeeper for the intended purpose of enabling interoperability of the NIICS.

208. Another example of measures that gatekeepers should implement to maintain the level of security under Article 7(3) DMA having data protection implications are measures to protect the metadata of the communication between end users and use the minimum amount of metadata for effective encryption key management. Another possible measure is to cryptographically verify the authenticity of the communication channel for the end users of their NIICS, thereby allowing such end users to trigger a challenge-response protocol that ensures both parties are communicating with the intended communication partner.

7.3 Other situations where personal data processing may occur

7.3.1 Geographical limitations

209. In addition, considering the limits in the territorial scope of the DMA,[162] gatekeepers should ensure that any geographical limitations they impose, and the measures introduced to enforce them, do not unduly restrict the activities of interoperable NIICS providers nor the enjoyment of interoperable functionalities by end users. Moreover, the question of what types of data collection and processing gatekeepers and third parties should be permitted to conduct in this context is important. In this respect, it would be important that the Reference Offer clarifies the respective responsibilities of the gatekeeper and of the third-party provider, including when it comes to verifying geographical restrictions.

DRAFT

[161] EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, Adopted on 28 July 2022, paragraph 97: "*In the context of interpersonal communications, end-to-end encryption ('E2EE') is a crucial tool for ensuring the confidentiality of electronic communications, as it provides strong technical safeguards against access to the content of the communications by anyone other than the sender and the recipient(s), including by the provider*". See also Article 29 Data Protection Working Party, Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU, Adopted on 11 April 2018: "*Encryption is therefore absolutely necessary and irreplaceable for guaranteeing strong confidentiality and integrity when data are transferred across open networks like the Internet, or stored in mobile devices like smartphones. This encryption should ideally always cover the entire communication, from the device of the sender to that of the recipient (end-to-end-encryption)*."

[162] See Article 1(2) DMA.

210. In any case, the gatekeeper end users and third-party end users should be adequately informed of the information that is collected and processed for the purpose of verifying and enforcing geographical limitations. In that respect, the Commission and the EDPB consider that depending on the characteristics of the service, end users should be able to benefit from interoperability whenever there are objective indications that the service is usually used in the Union, e.g. when end users regularly use a phone number belonging to a numbering plan of a Member State. Where such information is unavailable, or where there are objective reasons to suspect that the geographic limitations specified in the reference offer are often circumvented,[163] information that allows to estimate the general location of end users, such as an obfuscated IP address indicating the country, would in principle be sufficient for verifying and enforcing geographical limitations and collecting more precise location data would go beyond what is necessary in the context of enabling interoperability. Additionally, to comply with Article 5(1), point (c) GDPR on data minimisation, gatekeepers should not continuously monitor the end user's location, but only verify their location at appropriate intervals, and gatekeepers should generally only record whether the end user is "in" or "out" of the territorial scope of the DMA, without recording the precise country where they are in each verification. Moreover, data that is processed by gatekeepers in the context of these verifications should be stored only for a very limited period of time and should not be re-used for other purposes. Finally, gatekeepers need to take into account any restrictions that may apply under the ePrivacy Directive to the processing of data for the verification of end users' location.[164]

7.3.2 Measures pursuant to Article 7(9) DMA

211. Lastly, and in addition to the measures that gatekeepers are required to take pursuant to Article 7(3) DMA, Article 7(9) DMA allows gatekeepers to take strictly necessary, proportionate, and justified measures to ensure that third-party providers of NIICS requesting interoperability do not endanger the integrity, security and privacy of its services.

212. A possible example of measures that could be adopted by gatekeepers under Article 7(9) DMA is the adoption of blocking functionalities for the end users of their NIICS, thereby allowing such end users to technically prevent certain end users of the other providers' NIICS from sending them messages. This may, for instance, require blocking multiple identities associated to a single individual registered across various platforms to prevent cross-platform attacks with multiple pseudonyms (also called Sybil). With interoperable NIICS, each of them needs to be able to analyse the message or behaviour (e.g., to identify spam or abuse) of an end user that the end user in the other NIICS has requested to be blocked, to decide what action to take on its own servers and regarding its own users. This may also entail an exchange of information (including personal data) between the gatekeeper and the provider of the NIICS requesting interoperability under Article 7 DMA.

213. In the context of ensuring security, including in connection with relevant legal requirements,[165] gatekeepers should ascertain whether and to what extent the envisaged processing is actually necessary to ensure the integrity, security and privacy

[163] E.g., where the third party NIICS provider offers interoperability with the gatekeeper's NIICS globally.
[164] See, in particular, and depending on the characteristic of the processing, Articles 5(3), 6 and 9 ePrivacy Directive.
[165] See e.g. Article 32 GDPR; Article 7(3) DMA; Article 4(1)-(1a) ePrivacy Directive; and Article 21 Directive (EU) 2022/2555.

DRAFT

of the gatekeeper's services, and whether the objectives pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental freedoms and rights of end users (in particular, means that do not involve or use less intrusive forms of profiling of end-users).[166]

8 Coordination, cooperation and consultation

214. The DMA lays down a centralised monitoring and enforcement system, with the Commission empowered as the sole authority to implement and enforce the DMA.[167] At the same time, recital 37, relating to Article 5(2) of the DMA, says that the DMA "*is without prejudice to*" the GDPR, "*including its enforcement framework, which remains fully applicable with respect to any claims by data subjects relating to an infringement of their rights under*" the GDPR.[168]

215. Cooperation and coordination between the Commission, the EDPB and national data protection supervisory authorities within the remit of their respective powers and competences is required by the principle of sincere cooperation enshrined in Article 4(3) of the Treaty on European Union (TEU).[169] The DMA also provides for a duty of cooperation and coordination between the Commission and Member States, as well as the explicit possibility for the Commission to consult national authorities (including data protection supervisory authorities) where appropriate, on any matter relating to the application of the DMA.[170] Such cooperation and coordination between the Commission and data protection supervisory authorities is essential to ensure a consistent, effective and complementary application of the DMA and Union data protection law.[171] This includes not only the GDPR, but also the ePrivacy Directive, where relevant, in the context of the DMA. This will not only benefit end users, but also gatekeepers, business users and beneficiaries of DMA obligations by improving legal certainty of how the DMA, on the one hand, and Union data protection law, on the other, are applied.

---

[166] If they still opt for measures entailing profiling techniques, gatekeepers and providers requesting interoperability should pay due regard to the level of detail and the comprehensiveness of the profile, the impact of the profiling, and the safeguards aimed at ensuring fairness, non-discrimination and accuracy in the profiling process. See Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01), As last Revised and Adopted on 6 February 2018, page 14.

[167] Recital 91 of the DMA.

[168] See also recital 12 of the DMA.

[169] Judgment of the Court of Justice of 4 July 2023, *Meta Platforms and others (Conditions générales d'utilisation d'un réseau social)*, C-252/21, ECLI:EU:C:2023:537, paragraphs 53 and 54: "*Under that principle, (…) in areas covered by EU law, Member States, including their administrative authorities, must assist each other, in full mutual respect, in carrying out tasks which flow from the Treaties, take any appropriate measure to ensure fulfilment of the obligations arising from, inter alia, the acts of the institutions of the European Union and refrain from any measure which could jeopardise the attainment of the European Union's objectives (…). (…) in the light of this principle, when national competition authorities are called upon, in the exercise of their powers, to examine whether an undertaking's conduct is consistent with the provisions of the GDPR, they are required to consult and cooperate sincerely with the national supervisory authorities concerned or with the lead supervisory authority, all of which are then bound, in that context, to observe their respective powers and competences, in such a way as to ensure that the obligations arising from the GDPR and the objectives of that regulation are complied with while their effectiveness is safeguarded"*.

[170] See Article 37 DMA.

[171] Recital 90 DMA also states that "*The Commission and national authorities should cooperate and coordinate their actions necessary for the enforcement of the available legal instruments applied to gatekeepers within the meaning of this Regulation and respect the principle of sincere cooperation laid down in Article 4 of the Treaty on European Union (TEU)*".

DRAFT

216. Cooperation and coordination between the Commission and national data protection supervisory authorities may also be necessary to avoid double jeopardy (*ne bis in idem*[172]) where gatekeepers/controllers are subjected to proceedings or sanctions by the Commission and by a data protection supervisory authority in relation to the same conduct.[173]

217. In order to ensure a coherent, effective and complementary enforcement of the DMA and the GDPR, consultation is necessary in several cases[174]. Consultation will be required, in particular, where the Commission is called upon, in the exercise of its powers, to examine whether a gatekeeper's conduct is compliant with the DMA, when such examination also entails examining whether the gatekeeper's conduct is consistent with the provisions of the GDPR.[175] Conversely, should a national data protection authority be called upon, in the exercise of its powers, to examine whether a controller's or processor's conduct is compliant with the GDPR, when such examination also entails examining whether the controller's or processor's conduct is consistent with the provisions of the DMA, it is required to consult the Commission.

218. In cases where a gatekeeper has within its corporate structure a "main establishment" within the meaning of Article 4(16) GDPR, the interlocutor of the Commission should in principle be the relevant lead supervisory authority.[176] The lead supervisory authority should, in turn, make use of the appropriate mechanisms provided by the GDPR to cooperate with concerned supervisory authorities and inform the Commission accordingly.[177]

219. Any request for information or cooperation should be responded to within a reasonable period of time, taking into utmost account the investigatory needs and obligations that apply in a given case. The consulting authority may continue its investigation if it does not receive a reply within a reasonable time from the consulted authority, or where the

---

[172] The *ne bis in idem* principle is enshrined in Article 50 of the Union Charter of Fundamental Rights. Article 50 of the Charter provides that 'no *one shall be liable to be tried or punished again in criminal proceedings for an offence for which he or she has already been finally acquitted or convicted within the Union in accordance with the law'*. Therefore, the non bis in idem principle prohibits a duplication of proceedings and penalties of a criminal nature for the purposes of that article for the same acts and against the same person. See Judgment of the Court of Justice of 20 March 2018, *Luca Menci*, C-524/15, ECLI:EU:C:2018:197, paragraph 25 and the case-law cited. The principle is also mentioned in recital 86 DMA, reminding both the Commission and national authorities (including data protection supervisory authorities) that they are required to coordinate their enforcement efforts to avoid instances of double jeopardy: "*In particular, the Commission should take into account any fines and penalties imposed on the same legal person for the same facts through a final decision in proceedings relating to an infringement of other Union or national rules, so as to ensure that the overall fines and penalties imposed correspond to the seriousness of the infringements committed*."

[173] See Judgment of the Court of Justice of 22 March 2022, *bpost SA v Autorité belge de la concurrence*, C-117/20 ECLI:EU:C:2022:202, paragraphs 43 to 58. In analysing whether a duplication of proceedings and penalties respects the essence of the *ne bis in idem* principle laid down in Article 50 of the Charter, it should be determined "*whether there are clear and precise rules making it possible to predict which acts or omissions are liable to be subject to a duplication of proceedings and penalties, and also to predict that there will be coordination between the different authorities, whether the two sets of proceedings have been conducted in a manner that is sufficiently coordinated and within a proximate timeframe*".

[174] See also Article 37(1) and (2) DMA. The reference to "Member States" in Article 37(1) DMA encompasses, in line with Article 4(3) TEU and relevant case law, all public authorities of the Member States, both in the horizontal and the vertical structure of the State including data protection supervisory authorities.

[175] See by analogy the judgment of the Court of Justice of 4 July 2023, *Meta Platforms and others (Conditions générales d'utilisation d'un réseau social)*, C-252/21, ECLI:EU:C:2023:537, paragraphs 54, 56 and 57.

[176] Idem. See Article 56(1) GDPR.

[177] Judgment of the Court of Justice of 4 July 2023, *Meta Platforms and others (Conditions générales d'utilisation d'un réseau social)*, C-252/21, ECLI:EU:C:2023:537, paragraph 58. See Article 60 et seq. of the GDPR.

DRAFT

latter does not object to such an investigation being continued without having to wait for a decision on their part.[178]

220. In order to ensure coherence and effective complementarity in the implementation of the DMA and of other sectoral regulations applicable to gatekeepers, Article 40 DMA establishes a High-Level Group ('HLG') for the DMA, composed of various European bodies and networks – including the EDPB and the European Data Protection Supervisor ('EDPS').[179] In accordance with the Commission Decision setting up the HLG, the HLG cannot be involved in, or otherwise provide advice on, ongoing proceedings or investigations conducted by the Commission under the DMA.[180] The role of the HLG is instead to provide the Commission with advice and expertise in the areas falling within the competences of its members. Discussions within the HLG may concern any general matter of implementation or enforcement of the DMA, as well as the promotion of a consistent regulatory approach across different regulatory instruments, including the GDPR.[181]

221. Finally, it should be recalled that according to Article 15 DMA, gatekeepers have to submit to the Commission, within 6 months after their designation, the independently audited descriptions of any techniques for profiling of consumers that they apply to or across their CPS. The Commission then has to transmit those audited descriptions to the EDPB, pursuant to Article 15(1) DMA. In accordance with Article 36(3) DMA, the information collected pursuant to Article 15 also has to be used by the EDPB and national data protection supervisory authorities for the purposes of the GDPR. In particular, national data protection supervisory authorities may use it to inform the enforcement of the GDPR.[182]

DRAFT

[178] Judgment of the Court of Justice of 4 July 2023, *Meta Platforms and others (Conditions générales d'utilisation d'un réseau social)*, C-252/21, ECLI:EU:C:2023:537, paragraph 59.
[179] Article 40(5) DMA.
[180] Article 2(2) of Commission Decision of 23.3.2023 on setting up the High-Level Group for the Digital Markets Act, C(2023) 1833 final.
[181] Article 40(5) DMA. The Commission Decision setting up the HLG establishes that the HLG "*shall not be involved in, or otherwise provide advice on, ongoing proceedings or investigations conducted by the Commission*" under the DMA (Article 2(2) of Commission Decision of 23 March 2023 on setting up the High-Level Group for the Digital Markets Act, C(2023) 1833 final). This is without prejudice to the European Commission's obligation, under the duty of sincere cooperation under Article 4(3) TEU, to consult data protection supervisory authorities in concrete cases where issues related to the interpretation and application of EU data protection law arise.
[182] See also recital 72 DMA.