EDPS

**EUROPEAN DATA PROTECTION SUPERVISOR**

The EU's independent data protection authority

15 January 2025

# Towards a Digital Clearinghouse 2.0

## Concept Note

edps.europa.eu

**Executive Summary**

Since 2014, the EDPS has been working on the interplay and synergies between EU rules on data protection, consumer protection and competition law including the establishment a Digital Clearinghouse ('DCH') of authorities competent to enforce them to promote coherent enforcement of EU legislation applicable to the EU digital sector. As a result of the meetings of the DCH between 2017 and 2021, participating authorities developed personal connections, attained a better understanding of each other's areas of competence and expertise, and gained insights from each other's enforcement experiences.

Since then, several examples of multilateral cooperation initiatives between regulators from different legal fields have emerged at national level (e.g., in France, Germany, and the Netherlands). While they are not necessarily formalized in their legal systems, some of these initiatives involve multiple authorities that are competent to supervise the same or similar data-related practices under different legal frameworks. However, a forum where authorities competent to enforce the different parts of the EU Digital Rulebook and other laws applicable in the Digital Single Market can come together to discuss matters of coherent application (including to exchange enforcement-related information when possible) does not yet exist at EU level.

In parallel, the number of cases in which different authorities cooperate to exchange information and expertise is increasing. The need for both dimensions of cooperation, including in the context of enforcement, has recently become more prominent. The reason for this increased prominence is due, in no small part, to the recent proliferation of regulatory requirements stemming from the EU's new 'Digital Rulebook'. EU data protection law is often referred to as the 'cornerstone' upon which the EU Digital Rulebook is built, as is underscored by the reliance on GDPR definitions and obligations in various legislative acts which compose the EU Digital Rulebook.

Parallel investigations by various authorities into the same practices of the same entities reveal the complexities inherent in applying different rules — such as data protection, consumer rights, and new laws such as the Digital Markets Act and the Digital Services Act — but also the importance of achieving a coherent regulatory approach. Besides, case law has clarified that where two EU legal acts of the same hierarchical value do not establish priority of one over the other, they should be applied in a compatible manner, which enables a coherent application of them. Simultaneous actions by various regulators highlight the potential for conflicts and inconsistencies when data-related practices are scrutinized from different legal perspectives, and emphasize the critical need for enhanced dialogue, cooperation, and coordination among regulatory bodies to ensure a predictable and effective legal environment that places fundamental rights at the core. This need has also been recognized by the Council of the EU in May 2024 when it outlined its priorities for the 2024-2029 legislative mandate concerning digital policy, and by the European Commission in its June 2024 second report on the application of the GDPR.

The EDPS therefore proposes the establishment of a Digital Clearinghouse "2.0" that would provide authorities and bodies with a forum to exchange and coordinate on issues of common interest. This forum should facilitate proactive, collaborative efforts among participating authorities to address potential issues before they become practical problems, ensuring that different authorities are aligned on goals, methods, and responsibilities from the outset to attain tangible outcomes. Participants of this forum should include existing structures for cross-regulatory cooperation at EU Member State level, as well as EU-level structures such as the European Data Innovation Board and the High Level Group of the Digital Markets Act.

A Digital Clearinghouse 2.0 should promote cooperation in 'variable geometry', providing relevant authorities, bodies and networks the flexibility to join only discussions and working groups on issues that are important for them and where they have or need relevant expertise. The Digital Clearinghouse 2.0 should also be a forum where participating authorities share information - to the extent such sharing is legally allowed - about ongoing enforcement actions so as to facilitate further (bilateral or multilateral) engagement with other authorities on those concrete cases where relevant. Recent national experiences of fostering cross-regulatory dialogue indicate that there is added value in having a well-resourced central body providing a secretariat for the Digital Clearinghouse 2.0, in particular to ensure the timely delivery by participating authorities of concrete outcomes promoting cross-regulatory coherence.

While much progress could continue to be made in the absence of legislative intervention, both bilaterally between regulators and multilaterally in the context of the Digital Clearinghouse 2.0, the EDPS considers that legislative intervention is necessary to address the challenges ahead. Different policy options are available in this regard, which could range from minimal intervention to facilitate coordination and cooperation to legislative changes that systematically address potential issues of inconsistency across different regulations.

The EDPS considers it essential to remove recurring obstacles 'on-the-ground' to cooperation between competent authorities from different legal fields, in particular in what concerns exchanges of information and evidence during investigations. Therefore, against the background of the principles of sincere cooperation and *ne bis in idem*, the EDPS encourages the European Commission to consider introducing a legislative proposal during the new mandate that would allow competent supervisory authorities under the various parts of the EU Digital Rulebook to cooperate effectively, both with each other and with other relevant authorities competent to supervise sectoral or horizontal EU laws (such as data protection, competition and consumer protection law) that apply to the digital economy.

In the longer term, the EDPS considers that further legislative interventions may be needed to more systematically address potential issues of inconsistency and tensions arising from the application of different parts of the EU Digital Rulebook. Such a revision could notably seek to clarify the relationship between several obligations enshrined in different EU acts, streamline the number of regulators in charge of overseeing closely-related frameworks and formally create an independent central body to promote consistency and coherence in their practical application.

# Contents

# 1. Origins of the Digital Clearinghouse

1. In 2014, the EDPS issued a *Preliminary Opinion on Privacy and Competitiveness in the Age of Big Data*[1]. In that Opinion, the EDPS observed a tendency, despite obvious synergies like transparency, accountability, choice and general welfare, for EU rules on data protection, consumer protection and antitrust enforcement and merger control to be applied in silos. The EDPS launched a debate on how the EU's objectives might be applied more holistically, and how its rules might be applied in a more coherent manner in the digital economy. In particular, the EDPS stated that "*EU principles and rules on data protection, competition and consumer protection have been designed to promote a thriving internal market and to protect the individual. Greater convergence in the application of these policies could help meet the challenges posed by the big data economy. However, to date, policies have tended to develop in parallel with little interaction on subjects of common concern*"[2].

2. In 2016, the EDPS recommended the establishment of a Digital Clearinghouse ('DCH') to promote coherent enforcement of EU legislation applicable to the EU digital sector[3]. The DCH was conceived as a voluntary network of regulatory bodies to share information, voluntarily and within the bounds of their respective competences, about possible breaches of the laws applicable in the digital ecosystem and to align on the most effective ways of tackling them. Among other tasks, the EDPS proposed that the DCH should "*discuss the most appropriate legal regime for pursuing specific cases or complaints related to services online, especially for cross-border cases where there is a possible violation of more than one legal framework*", as well as "*identifying potential coordinated actions or awareness initiatives at European level which could stop or deter harmful practices*" [4].

3. At the time, growing concentration in digital markets further underlined the need for a mechanism for coherent enforcement across the different fields of EU law of obligations relating to the rights and interests of individuals and the impact on fundamental rights. Such concentration could harm the interests of individuals not only as consumers, but also as data subjects, adversely impacting their fundamental rights to privacy and to the protection of personal data, enshrined, respectively, in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

4. The growing concentration in digital markets has made the convergence and overlap between consumer protection, competition and data protection law increasingly evident. The rights and interests at stake in the digital economy further extend to other fundamental rights, such the right to non-discrimination (Article 21 of the Charter) and to economic aspects of daily life, for instance price-discrimination[5]. The concentration in digital markets also raises significant concerns having regard to freedom of information and consumer manipulation[6].

---

[1] EDPS Preliminary Opinion on "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy", issued on 26 March 2014.
[2] Idem, paragraph 2.
[3] EDPS Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data, issued on 23 September 2016.
[4] Idem, page 15.
[5] EDPS Opinion 8/2016, p. 6: "*Meanwhile unfair price discrimination - by exploiting differences in consumers' identifiable sensitiveness to price - could lead to extraction of consumer surplus and increase in profits. Recent studies have pointed to the potential in the future of machine-learning algorithms to achieve perfect first degree price discrimination, with firms segmenting the market into each individual consumer and charging him according to his willingness to pay.*"
[6] EDPS Opinion 8/2016, p. 8: "*A majority of people now access news on social media, and web-based service algorithms determine the content to be served to individual users according to their profile, with growing concerns that the online experience could be filtered and become a series of echo chambers.*"

5. The DCH leveraged excellent work by and cooperation with academia[7]. It was a journey into the interfaces between data protection, consumer and competition law, which started before the new digital 'Acts' were even proposed. The DCH acted as a voluntary network of regulators and academic experts willing to share information and ideas on how to ensure synergies and coherence in the application of the different areas of law relating to the digital economy, with a special focus on online platforms.

6. The DCH met for the first time in 2017[8]. In several meetings organised first by the EDPS, then by academia, competent authorities for consumer protection, competition, electoral oversight, and data protection discussed common issues, such as data portability and sharing, fake news, voter manipulation, regulation of zero-price services, the emergence of 'attention markets', the opacity of algorithms, integrating privacy into merger assessments and cross-regulatory cooperation. By virtue of these meetings, participating authorities developed personal connections, attained a better understanding of each other's areas of competence and expertise, and gained insights from each other's enforcement experiences.

7. Current trends in the digital economy and recent legislative developments show that the DCH - and more broadly establishing a dialogue between privacy and data protection regulators and their counterparts in others fields of law - was and remains a much needed strategic action. The need for increased dialogue has been made even more evident with the adoption of the EU 'Digital Rulebook', which has further increased the number of authorities with a mandate to scrutinise the data-related practices of companies active in digital markets[9].

## 2. Experiences at national level

8. There are multiple examples of cooperation initiatives surfacing at national level to foster cooperation among administrative authorities that supervise different aspects of the digital economy[10]. Some of them concern bilateral arrangements between authorities in a single jurisdiction competent to enforce two or more different fields of law. An example is the recent joint declaration of the French authorities responsible for the oversight of competition and data protection rules, which refers to the provisions under national law that allow them to consult each other in the context of investigations and commits both parties to continue to seek the expertise of the other authority when appropriate[11]. In the past, both regulators have sought each other's opinion concerning the application of their respective fields of law to

---

[7] The origins, the concept and the work done in the context of the Digital Clearinghouse '1.0' are described by Christian D'Cunha and Anna Colaps in '*A clear imbalance between the data subject and the controller': data protection and competition law*' (Chapter 15) in the EDPS 20th Anniversary book *Two decades of personal data protection. What's next?*, p. 191-205.

[8] The DCH met for the first time in Brussels on 29 May 2017 (statement available here). The second meeting of the DCH on 27 November 2017 focused on the four areas of common concern identified in the first meeting, namely fake news and voter manipulation, the emergence of attention markets and opacity of algorithms which determine how personal data are collected and used (statement available here).The third meeting of the Digital Clearinghouse took place on 21 June 2018 (statement available here) and the fourth meeting of the Digital Clearinghouse took place on 10 December 2018 (statement available here). From 2019, the DCH was jointly hosted by the Research Centre in Information, Law and Society (CRIDS) at the University of Namur, the Tilburg Institute for Law, Technology, and Society (TILT) at Tilburg University, and the European Policy Centre (EPC) in Brussels. Regulators met for the fifth meeting on 5 June 2019 (statement available here). The sixth meeting of the network took place on 19 November 2019 (statement available here).The seventh meeting of the network took place on 10 June 2020 (statement available here).

[9] See also G. Zanfir-Fortuna, '*Follow the (personal) data: positioning data protection law as the cornerstone of EU 'Fit for the Digital Age' legislative package*' (Chapter 16) and N. Smuha '*The paramountcy of data protection law in the age of AI (Acts)*' (Chapter 17), EDPS, *Two decades of personal data protection. What's next?*, EDPS 20th Anniversary. pp. 206-223 and 225-239.

[10] OECD Directorate for Financial and Enterprise Affairs Competition Committee, '*The intersection between competition and data privacy – Background Note*', DAF/COMP(2024)4, 13 June 2024, paragraph 7.

[11] Commission Nationale Informatique & Libertés (CNIL) and Autorité de la concurrence, *Concurrence et données personnelles : une ambition commune*, 12 December 2023, p. 12.

conduct that was under investigation by the requesting authority[12]. Consultations of this nature are important to ensure that, where laws protecting different legal interests may be enforced by different authorities against the same behavior, enforcement actions do not lead to inconsistent outcomes[13].

9. Another notable instance of bilateral cooperation between a national competition authority and a data protection authority was the action of the German competition authority (*Bundeskartellamt*) against Facebook (now Meta Platforms). In this case, the *Bundeskartellamt* established that Facebook was abusing its dominant position on the market for online social networks by making the use of its Facebook service conditional upon users' acceptance of terms of service that "allowed" Facebook to combine personal data obtained via its Facebook service with personal data obtained from other services owned by Facebook (e.g., Instagram and Whatsapp) and third-party services (via tools such as social plug-ins). After contacting the Hamburg Data Protection Commissioner (HmbBfDI), the Federal Commissioner for Data Protection and Freedom of Information (BfDI) and Facebook's lead data protection supervisory authority in Ireland (the Data Protection Commissioner), the *Bundeskartellamt* concluded that Facebook's conduct breached the GDPR[14] for a lack of valid consent for combining personal data in the manner described, and hence abused its dominant position on the market for online social networks[15]. While Facebook judicially contested the *Bundeskartellamt*'s ability to establish infringements of the GDPR in the exercise of its competences under German competition law, the Court of Justice of the European Union ('CJEU') confirmed that ability for competition authorities provided that they consult the competent data protection supervisory authority in the process[16]. The case was closed in October 2024 by the *Bundeskartellamt*, after Meta took measures to comply with the regulator's February 2019 decision and withdrew its appeal in the proceedings before the Düsseldorf Higher Regional Court[17].

10. While they are not necessarily formalized in their legal systems, some initiatives to facilitate cross-regulatory cooperation in EU Member States involve multiple authorities that are competent to supervise the same or similar data-related practices under different legal frameworks. In the Netherlands, the Digital Regulation Cooperation Forum ('SDT') includes the Dutch competition and consumer protection authority ('ACM'), the financial regulator ('AFM'), the data protection authority ('AP'), and the media regulator ('CvdM'). The SDT was created in 2021 as a voluntary network of competent authorities to "*work together in the oversight of digital services*", such as artificial intelligence, data processing, online design, personalization, manipulation, and deception[18]. Participating authorities wish to "*ensure*

---

[12] See the French competition authority's request for an opinion of the French data protection authority pertaining to the application of privacy and personal data protection legislation in case 'GDF Suez': Decision 14-MC-02 of 9 September 2014 regarding a request for interim measures submitted by Direct Energie in the gas and electricity sectors. See also the more recent decision of the French competition authority in the investigation of Apple's iOS operating system, which was also informed by an opinion of the French data protection authority, from 17 March 2021.

[13] OECD Directorate for Financial and Enterprise Affairs Competition Committee, '*The intersection between competition and data privacy – Background Note*', DAF/COMP(2024)4, 13 June 2024, paragraphs 100-103.

[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.

[15] Bundeskartellamt (6th Division), Decision in Case B6-22/16, from 6 February 2019.

[16] 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 52-57 and 62.

[17] Bundeskartellamt, Case summary '*Facebook; Implementation of the Bundeskartellamt's decision of 6 February 2019 (Abusive business terms due to inappropriate data processing)*', 10 October 2024.

[18] Authority for Consumers & Markets, *The Digital Regulation Cooperation Platform (SDT)*.

*efficient and effective enforcement of compliance with rules and regulations (Dutch and European)*"[19].

11. Similar initiatives to the SDT have already been established in Ireland, Germany, and France:

    a. The Irish Digital Regulators Group (DRG) includes the Commission for Communications Regulation (ComReg), the Data Protection Commission (DPC), the Competition and Consumer Protection Commission (CCPC), and the Broadcasting Authority of Ireland (BAI). Its primary purpose is to develop strong cross-functioning communications between participating authorities whose work has direct ramifications for Ireland's digital economy, so that current and future digital legislation is applied in a consistent and cohesive manner"[20]. The DRG regularly also regularly meets with the government (a senior officials group chaired by the Irish Prime Minister's office) to inform government decisions about resource allocation to competent authorities and even legislative changes that might be necessary.

    b. The Digital Cluster Bonn from Germany is composed of the Federal Financial Supervisory Authority (BaFin), the Federal Office of Justice (BfJ), the Federal Office for Information Security (BSI), the Federal Commissioner for Data Protection and Freedom of Information (BfDI), the Federal Cartel Office (FCO) and the Federal Network Agency (BNetzA). It aims to foster knowledge-sharing among such competent authorities to develop common positions and to apply the laws that regulate the digital economy consistently and coherently[21].

    c. In May 2024, the French legislator set up the national network for coordination of the regulation of digital services, which is composed of Authority for Audiovisual and Digital Communication (ARCOM), the Authority for Telecommunications, Postal Services and Print Media (ARCEP), the Competition Authority (AdC), the Cybersecurity Agency (ANSSI), the Authority for Labour Relations in Platforms (ARPE), the Data Protection Authority (CNIL), and the competent State services, and is coordinated by ARCOM. It is chaired by the Ministers for digital and culture, and the secretariat is provided by the Minister for digital. The network aims to ensure the exchange of information and encourage coordination between its members, as well as synergies in their work in the regulation of information society services, while respecting their respective responsibilities and, where applicable, their independence[22]. The network is organized in two distinct, but interdependent levels: the Network for Digital Regulators (political level) and the Taskforce on Digital Regulation (technical level).

12. Beyond the borders of the EU, the Digital Regulation Cooperation Forum (DRCF) was set up in 2020 in the United Kingdom by four local regulators with responsibilities for digital regulation, notably the Competition and Markets Authority (CMA), the Financial Conduct Authority (FCA), the Information Commissioner's Office (ICO) and the Office of

---

[19] Authority for Consumers & Markets, *SDT members to expand their collaboration regarding digital regulation*, 24 March 2023.: "*In addition to the Chamber for general discussions between the four SDT members, two more Offices will be created: a Chamber regarding the enforcement of the DSA (which will look at digital services, such as digital platforms) and a Chamber regarding oversight over algorithms & AI, which will also involve other regulators. The individual regulators will conduct oversight over parts of these regulations, each within their own area of expertise. In addition, the SDT members will discuss any areas of overlap, and where regulatory problems may occur.*"

[20] Competition and Consumer Protection Commission, *2022 Annual Report*, p. 36.

[21] See Digital Cluster Bonn, *Digital Cluster Bonn: Sechs Bundesbehörden arbeiten bei der Digitalisierung enger zusammen*, 15 January 2024. The six participating authorities have also signed a Memorandum of Understanding in January 2024.

[22] On 21 May 2024, Article 51 of *Loi n°2024-449* added Article 7-4 to *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, which provides for the creation of such network.

Communications (Ofcom). One of the goals of the DRCF is precisely to foster coherence of participants' supervisory activities where their respective regimes intersect. The DRCF provides indications of good practices that initiatives aiming to foster multilateral cross-regulatory cooperation might consider. For instance, the DRCF has an AI and Digital Hub that advises innovators on cross-regulatory queries from all participating authorities. Even if the DRCF does not have legal personality, the four member authorities commit resources and funding to the DRCF, including to support a DRCF CEO and core team which are dedicated to the pursuit of the DRCF's goals full time. The CEO and core team develop and oversee the delivery of the DRCF's annual work plan, which is defined by participating regulators and delivered by project teams which include members of those regulators[23]. This model of cooperation has allowed participating authorities to maintain open channels of communication and produce deliverables in the form of joint statements, blogs and articles, papers, and annual reports.

13. Such frameworks for multilateral cross-regulatory cooperation have a strong potential for mutually enhancing and ensuring consistency of participants authorities' respective enforcement activities, and for delivering the best outcome for individuals' rights and welfare. However, this will only be achieved if participating authorities are able to collaborate effectively with their counterparts and share relevant information where appropriate. Therefore, it is important to be aware of existing obstacles to making cross-regulatory cooperation a reality, which may include:

    - a lack of resources of competent authorities;

    - a lack of awareness/expertise in other legal fields or lack of knowledge about other enforcement activities to detect potential regulatory overlaps and tensions;

    - lack of willingness to engage beyond one's own regulatory remit, due to a tendency to protect one's own competence ('regulatory tribalism'); and

    - lack of ability to lawfully share information and evidence concerning pending investigations which are typically subject to confidentiality requirements and may even be subject to criminal penalties[24].

    Moreover, some competent authorities may not enjoy a level of independence that would allow them to swiftly enter into and execute cooperation with authorities from other legal fields[25].

14. Despite the various initiatives at national level, a forum where authorities competent to enforce the different parts of the EU Digital Rulebook and other laws applicable in the Digital Single Market can come together to discuss matters of coherent application of these laws (including to exchange enforcement-related information when possible) does not yet exist at EU level.

---

[23] Digital Regulation Cooperation Forum, DRCF Terms of Reference (ToR).

[24] See also Global Privacy Assembly, *An Enforcement Cooperation Handbook*, Last Updated and Presented at the 43rd Global Privacy Assembly, Mexico City, October 18 – 21, 2021, p. 13: "*Sharing confidential information and/or personal data is often crucial to enforcement cooperation (even if only for authorities to share that they are in fact, or are considering, investigating a matter). In many cases, parties will be able to share such information, in compliance with their respective legal limitations, pursuant to a non-binding memorandum of understanding (MOU) or an arrangement. Such a document will detail each party's expectations regarding the circumstances under which they may share information. It is important to note, however, that some authorities will not be able, either practically or legally, to share information pursuant to a non-binding arrangement, while others may not be in a position to sign binding agreements.*"

[25] See also BEUC, *Need for independent national market surveillance authorities under the AI Act - Commission*, 25 June 2024. BEUC's letter to the European Commission notes that "*some of the first market surveillance authorities to be appointed would fail to meet the independence and impartiality requirements of the AI Act, as they are politically governed or government dependent*". By contrast, data protection supervisory authorities must be independent, as a requirement of primary and secondary EU law (Article 8(3) Charter and Article 52 GDPR), meaning that they shall remain free from external influence and instructions, and not engage in any incompatible occupation.

# 3. An enhanced digital rulebook

15. The regulatory and technological landscape has evolved significantly since the EDPS issued his *Preliminary Opinion on Privacy and Competitiveness in the Age of Big Data*. The need to protect fundamental rights is much higher now with the advent of artificial intelligence ('AI') and the continuous reliance on personal data processing in today's economy. There is a clear need to keep the application and enforcement of data protection a 'cornerstone' of this increasingly complex regulatory setting, in line with the EU commitment to upholding EU values in its digital strategy[26].

16. To help ensure that Europe is 'fit for the digital age', the European Union has recently adopted several important pieces of legislation that aim to regulate digital markets, services and technologies, including the Digital Governance Act ('DGA')[27]; the Digital Markets Act ('DMA')[28]; the Digital Services Act ('DSA')[29]; the Data Act ('DA')[30]; and the Artificial Intelligence Act ('AI Act')[31]. This short list does not include all EU legislative initiatives in the digital domain but focuses on those which directly and explicitly aim to regulate data processing practices of economic operators already falling within the scope of the GDPR[32]. This concept note refers to these legislative acts as "EU Digital Rulebook".

17. Regulatory consistency and cooperation are paramount in ensuring the coherent application of EU law regulating the digital economy, as well as legal certainty. Furthermore, through collaboration between regulators from different fields, individual regulatory goals may be achieved more effectively, as regulators can benefit from each other's knowledge and experience. The focus of cooperation should not be on expanding the missions of individual authorities, but rather on enabling them to accomplish their assigned mandates more effectively. Strong cooperation mechanisms can also help reduce administrative burden and potential redundancies in enforcement actions that tackle the same or similar practices (by preventing the duplication of efforts).

18. The importance of regulatory consistency and cooperation was underlined by several EDPS Opinions and EDPB-EDPS Joint Opinions, which highlighted the critical interplay between the different parts of the EU Digital Rulebook and EU data protection law, both the perspective of the requirements they sought to impose on covered entities, and of the diverging governance and enforcement structures they envisaged. In particular, these opinions advised to co-legislator to:

---

[26] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Shaping Europe's Digital Future, COM(2020) 67 final, 19 February 2020.
[27] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance), OJ L 152, 3.6.2022, p. 1-44.
[28] 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) (Text with EEA relevance), OJ L 265, 12.10.2022, p. 1–66.
[29] 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) (Text with EEA relevance), OJ L 277, 27.10.2022, p. 1–102.
[30] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L, 2023/2854, 22.12.2023.
[31] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024.
[32] While they are not analysed in this concept note, other recently adopted or proposed legislative initiatives worth recalling include the Regulation establishing the European Digital Identity Framework, the (proposal for a) Regulation on a framework for Financial Data Access, the (proposal for a) Regulation on the establishment of the digital euro, the (proposal for a) regulation on the European Health Data Space, the Directive on improving working conditions in platform work, the Regulation on the transparency and targeting of political advertising, among others.

- ensure that the new digital acts complement and align with existing rules and do not adversely affect the level of protection for individuals regarding the processing of personal data under Union and national law[33];
- promote consistency in terminology and definitions where relevant[34];
- provide for a clear articulation of individual rights, safeguards and remedies across the different pieces of legislation[35].

19. In terms of governance and enforcement, the EDPS, as well as the EDPB, have emphasized the need for robust supervision and clear roles for oversight authorities under the legislative Proposals composing the EU Digital Rulebook[36]. The EDPS has consistently recommended the establishment of institutionalized and structured cooperation among relevant competent authorities in his Opinions, including with a view to ensure information exchange and fulfillment of complementary roles[37]. Such calls were echoed in the EDPB *Statement on the Digital Services Package and Data Strategy*, which recommended legally enabling the competent supervisory authorities under the different parts of the EU Digital Rulebook to share information obtained in the context of any audits and investigations that relate to the processing of personal data with the competent data protection authorities, either upon request or on their own initiative[38].

## 3.1. Different purposes, objectives and scope

20. As previously highlighted by the EDPS, competition, consumer protection, and data protection law have different, but often complementary, objectives[39]. The same observation applies to the more recent pieces of the EU Digital Rulebook when compared with each other and those three fields of law. For instance, greater contestability of digital markets (which is an objective of the DMA) can lead to more choice for individuals, which in turn may increase incentives for companies to develop and implement data protection and privacy features, in line with data protection by design and by default[40]. But while the objectives of the different legal instruments are often complementary, they can also diverge. Having a clear overview of these objectives is therefore helpful to understand how the different policy areas articulate with each other and how this interplay can lead to a better enforcement of EU law in the digital economy.

---

[33] See EDPS Opinion 1/2021 on the Proposal for a Digital Services Act, adopted on 10 February 2021, paragraph 13; EDPS Opinion 2/2021 on the Proposal for a Digital Markets Act, adopted on 10 February 2021, paragraph 16. See also EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), version 1.1, adopted on 9 June 2021, paragraph 27.

[34] EDPS Opinion 2/2021 on the Proposal for a Digital Markets Act, adopted on 10 February 2021, paragraph 19. See also EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), version 1.1, adopted on 9 June 2021, paragraphs 29-46.

[35] See e.g. EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), adopted on 18 June 2021, paragraphs 18, 73.

[36] EDPS Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative developments, adopted on 23 October 2023, paragraph 79(12) and 79(10). See also EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), version 1.1, adopted on 9 June 2021, paragraph 218.

[37] EDPS Opinion 2/2021 on the Proposal for a Digital Markets Act, adopted on 10 February 2021, paragraph 40. See also EDPS Opinion 1/2021 on the Proposal for a Digital Services Act, adopted on 10 February 2021, paragraph 87.

[38] EDPB Statement on the Digital Services Package and Data Strategy, adopted on 18 November 2021, p. 4.

[39] EDPS Preliminary Opinion on "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy", issued on 26 March 2014, p. 11: "*Separate rules on data protection, competition and consumer protection all converge around a two-fold purpose – the protection and promotion of the welfare of the individual and the facilitation of the creation of a single European market.*"

[40] Article 25 GDPR.

21. Another example of complementarity is how the GDPR is intended to protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data[41], but on the other hand, it also promotes the free movement of personal data within the European Union[42]. The AI Act also pursues several objectives, notably: the improvement of the functioning of the internal market; the promotion of and the uptake of human centric and trustworthy AI while ensuring a high level of protection of health, safety, fundamental rights; and supporting innovation[43].

## 3.2. EU data protection law as a 'cornerstone'

22. EU data protection law - and, in particular, the GDPR - is often referred to as the 'cornerstone' upon which the EU Digital Rulebook is built. According to the European Commission, the different pieces of the Digital Rulebook complement the GDPR or specify how it should be applied in specific areas, to pursue particular objectives[44]. At the same time, it is possible to find multiple references to GDPR definitions and obligations across the various regulations which make out the EU Digital Rulebook[45].

23. Already in 2017, the EDPS expressed concerns related to the adoption of laws applying to the digital sector that could overlap with the GDPR. Back then, the EDPS warned that '*[t]he EU should … avoid any new proposals that upset the careful balance negotiated by the EU legislator on data protection rules. Overlapping initiatives could inadvertently put at risk the coherence of the Digital Single Market, resulting in regulatory fragmentation and legal uncertainty. The EDPS recommends that the EU apply the GDPR as the means for regulating use of personal data in the digital economy*'.[46] In the same vein, the EDPB stressed in its 2021 Statement on the Digital Package and Data Strategy that "*processing of personal data already is or will be a core activity of the entities, business models and technologies regulated by these proposals*". The EDPB added that, "*the combined effect of the adoption and implementation of the proposals will therefore significantly impact the protection of the fundamental rights to privacy and to the protection of personal data, enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union and in Article 16 of the Treaty on the Functioning of the European Union*"[47].

24. Each of the legal acts that have come to make up the EU Digital Rulebook include a specific wording addressing their articulation with the GDPR (and other data protection principles). While the DGA and the DA explicitly state that, in case of conflict, the rules of the GDPR and ePrivacy shall prevail[48], the DSA and the DMA establish that they are without prejudice to the rules laid down by Union law on the protection of personal data[49]. Even if the articulation of

---

[41] Article 1(2) GDPR.
[42] Article 1(3) GDPR. In this context, it should be recalled that the primary legal basis for Directive 95/46/EC was Article 100a TEC (now Article 114 TFEU) which grants the EU the power to adopt measures for the approximation of laws, regulations, and administrative provisions of the Member States that have as their object the establishment and functioning of the internal market.
[43] Recital 1 and Article 1, AI Act.
[44] Communication from the Commission to the European Parliament and the Council, Second Report on the application of the General Data Protection Regulation, COM(2024) 357 final, 25 July 2024, p. 16.
[45] For example, Article 26(3) of the DSA prohibits the presentation of online advertising by online platforms "*based on profiling using special categories of data*" as per Articles 4(4) and 9(1) GDPR. Article 38 then requires providers of very large online platforms ('VLOPs') and of very large online search engines ('VLOSEs') that use recommender systems to provide at least one option for each of their recommender systems which is not based on "profiling" within the meaning of the GDPR. Articles 6(9) and (10) DMA include rights for users of gatekeepers' core platform services designated by the European Commission (and third parties those users authorise) to obtain portability and access to the data (including personal data) they or their own customers (in case they are business users) generate when they use the core platform service, upon end users' consent.
[46] EDPS Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, issued on 14 March 2017, p. 3.
[47] EDPB Statement on the Digital Services Package and Data Strategy, adopted on 18 November 2021, p. 1.
[48] Article 1(3) DGA and 1(5) DA.
[49] Article 2(4)(g) and Recitals 10 and 68 DSA; Article 8(1) and Recital 57 DMA.

the relationship of each act to EU data protection law is not identical across the different regulations, it is clear that the existing protections under EU data protection law continue to remain fully applicable.

### 3.3. Need for coherent application

25. The CJEU has clarified that, where two EU legal acts of the same hierarchical value (e.g., two regulations, such as the DMA and the GDPR) do not establish priority of one over the other, they should be applied in a compatible manner, which enables a coherent application of them[50]. To contribute to consistent and coherent interpretation and application of EU law[51], the EDPB has recently committed to provide guidance on the interplay between the application of the GDPR and other EU legal acts, particularly the AI Act and those derived from the EU Data Strategy and the Digital Services Package[52]. In that context, it is important to recall, among other factors, that:

    a. The right of natural persons to the protection of personal data has a singular importance when compared with the other fundamental rights included in the Charter, as has been underlined by Advocate General Szpunar. This Opinion underlines the 'very broad definition of the material scope of the GDPR', which reflects the 'cross-cutting' nature of issues relating to personal data and the intention of EU Member States to strengthen its protection[53]; and that

    b. Personal data is often combined or inextricably mixed with non-personal data. As noted by the Commission, "*[m]ixed datasets represent the majority of datasets used in the data economy and are common because of technological developments such as the Internet of Things (i.e., digitally connecting objects), artificial intelligence and technologies enabling big data analytics*"[54]. The EDPB and the EDPS already recalled that as per the Regulation on the free flow of non-personal data[55], a mixed dataset is subject to all the obligations of the GDPR[56]. Consequently, a mixed dataset will as a rule be subject to the obligations of data controllers and processors and the data subject's rights established by the GDPR.

---

[50] Judgment of the General Court of 3 May 2018 in Case T-653/16, Malta v Commission, 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.*"

[51] As regards the relationship between consistency and coherence, see Majcher K., 'Coherence between Data Protection and Competition in Digital Markets', Oxford University Press, 2023, p. 154-155, arguing that striving for consistency means striving for the elimination of conflicts between different fields of law, whereas coherence means establishing a higher degree of their convergence and positive connections through common principles and values.

[52] EDPB Strategy 2024-2027, April 2024, pillar 3, key action 1. See also EDPB Statement 6/2024 on the Second Report on the Application of the General Data Protection Regulation - Fostering Cross-Regulatory Consistency and Cooperation, Adopted on 3 December 2024.

[53] Opinion of Advocate General Szpunar in Case C-33/22 Österreichische Datenschutzbehörde, delivered on 11 May 2023, ECLI:EU:C:2023:397, paragraphs 33, 64 and 77,

[54] Communication from the Commission to the European Parliament and the Council, Guidance on the Regulation on an Framework for the Free Flow of Non-personal Data in the European Union, COM(2019) 250 final, 29 May 2019, pages 8- 10.

[55] Comments of the EDPS on a Proposal for a Regulation of the European Parliament and of the Council on a framework for the free-flow of non-personal data in the European Union, 8 June 2018.

[56] EDPB-EDPS Joint Opinion 02/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), adopted on 4 May 2022, paragraphs 70-71; EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), adopted on 10 March 2021, paragraph 61; EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, adopted on 12 July 2022, paragraph 41.

26. At the same time, there is a need to avoid instances of 'strategic over-compliance' with EU data protection law, where entities that fall under new EU laws from the EU Digital Rulebook justify their non-compliance with those EU laws with the need to preserve or deploy data protection safeguards that are not necessary to comply with the requirements of the GDPR[57]. It is important to recall that "*the right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.*"[58]

## 3.4. Need for cross-regulatory cooperation

27. The need for cross-regulatory cooperation in the application of different EU laws in the digital economy becomes particularly evident when authorities from different legal fields initiate investigations under their own regimes concerning the same practices of the same entities[59]. Some of these authorities are even called upon to apply rules and concepts stemming from fields of law that are under different authorities' supervision. A prime example is Article 5(2) DMA, whose supervision will require the Commission to apply the requirements of consent under Articles 4(11) and 7 GDPR, including by checking whether consent obtained by gatekeepers is 'specific' (i.e., sufficiently granular) and 'free'.

28. The examples of regulatory actions highlighted in this section mainly serve as illustrations that the potential benefit and/or need for cross-regulatory cooperation are not merely theoretical, but are apparent having regard to recent supervisory actions by different regulators.

29. One recent example concerns the supervisory actions against the targeted advertising practices of social networking service provider LinkedIn. In 2018, the Irish data protection authority initiated an inquiry based on a complaint from La Quadrature du Net, a French digital advocacy organization representing 8450 users of the service in this case[60]. The complaint concerned the lawfulness of LinkedIn's processing of users' personal data for targeted advertising. The complainants claimed that LinkedIn's processing lacked valid user consent, as the consent obtained was not freely given nor unambiguous. Additionally, the complaint argued that LinkedIn could not base its processing on legitimate interests or the performance of a contract under Article 6(1)(f) and (b) GDPR, rendering the processing unlawful under Article 6 GDPR. In October 2024, the DPC announced its final decision in the matter, which included a fine of 310 million Euros against LinkedIn for the platform's use of personal data in violation of the GDPR[61]. In a separate instance, in March 2024, the European Commission launched an inquiry against LinkedIn under the DSA following a complaint submitted by civil society organisations[62]. The Commission requested information concerning the company's compliance with the prohibition of presenting advertisements based on profiling using special categories of personal data which stems from Article 26(1) DSA. Subsequently, LinkedIn announced that it had disabled the functionality that allowed

[57] Majcher K., 'Coherence between Data Protection and Competition in Digital Markets', Oxford University Press, 2023, p. 197-201.
[58] Recital 4 GDPR.
[59] See a similar concern expressed by the European Commission concerning the parallel application of EU consumer law with other areas of EU law, in Commission Staff Working Document - Fitness Check of EU consumer law on digital fairness, SWD(2024) 230 final, Section 4.1.2.2.
[60] La Quadrature du Net, *Réclamation contre LinkedIn*, 28 May 2018.
[61] Data Protection Commission, *Irish Data Protection Commission fines LinkedIn Ireland €310 million*, 24 October 2024.
[62] European Commission, *Commission sends request for information to LinkedIn on potentially targeted advertising based on sensitive data under Digital Services Act*, 14 March 2024.

advertisers to target users based on their membership in LinkedIn Groups within the EU Single Market[63].

30. Another example of related inquiries by a data protection authority under the GDPR, on the one hand, and the European Commission under the DSA, on the other hand, concerns default privacy settings for minors and age verification practices of TikTok. In September 2023, the Irish DPA concluded an investigation into TikTok and issued its final decision[64]. The inquiry focused on TikTok's compliance with GDPR obligations regarding the processing of personal data of child users. It found that TikTok had set profile settings for child accounts to public by default, thus infringing Articles 25(1), 25(2), 5(1)(c) and 24(1) GDPR. Additionally, after an objection raised by the Italian DPA and following the EBPB's binding decision[65], the Irish DPA determined that there was insufficient information to confirm TikTok's compliance with Article 25(1) GDPR in relation to the age verification measures it had implemented. After the adoption of the Irish DPA's decision, the European Commission has initiated formal proceedings to investigate potential breaches of the DSA by TikTok[66]. This investigation covers several areas including the protection of minors and managing risks associated with addictive design and harmful content. Specifically, the inquiry will scrutinize, among others, TikTok's compliance with DSA obligations related to age verification tools aimed at preventing minors from accessing inappropriate content. It will also assess whether TikTok has implemented appropriate and proportionate measures to ensure a high level of privacy, safety and security for minors with regard to default privacy settings.

31. The recent action by the *Bundeskartellamt* against Alphabet Inc., (parent company of Google), in the context of which the competition regulator closely cooperated with the European Commission (as the enforcer of the DMA), also highlights the need for a consistent application of laws to data-related practices, even beyond the remit of the GDPR. Leveraging the new Section 19a of the German Competition Act, the Bundeskartellamt initiated proceedings that led Google to commit to providing users with clear choices regarding the cross-use and combination of their data across different services[67]. Although such obligations are already mandated by Article 5(2) DMA for core services designated by the European Commission, the Bundeskartellamt's decision ensures the same restrictions apply to Google's additional services, ensuring that Google needs to obtain consent from its users before processing their personal data across services[68]. In the same vein, the Italian competition authority ('AGCM') has opened investigation proceedings against Alphabet and Google with regard to Google's consent practices, scrutinizing whether Google's requests for consent to the linking of services offered, provide clear and adequate information in a manner that complies with consumer protection requirements. The AGCM is concerned that Google's mechanisms could manipulate users into consenting to data cross-use and combination more broadly than intended[69].

32. The 'pay or consent' model recently rolled out by Meta, where users are required to either pay for using the online platform or consent to having their personal data processed for online

---

[63] European Commission, *Statement by Commissioner Breton on steps announced by LinkedIn to comply with DSA provisions on targeted advertisement*, 7 June 2024.
[64] Data Protection Commission, Decision in the matter of TikTok Technology Limited made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation, adopted on 1 September 2023.
[65] EDPB Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR), adopted on 2 August 2023.
[66] European Commission, *Commission opens formal proceedings against TikTok under the Digital Services Act*, 19 February 2024.
[67] Bundeskartellamt, *Bundeskartellamt gives users of Google services better control over their data*, 5 October 2023.
[68] Bundeskartellamt, Decision pursuant to Section 19a(2) sentence 4 in conjunction with Section 32b(1) GWB-Public version.
[69] AGCM, *PS12714 - Italian Competition Authority: investigation launched against Google for unfair commercial practices*, 18 July 2024.

behavioural advertising has triggered scrutiny from the perspective of data protection, consumer protection and competition law:

a. **From the perspective of EU data protection law**: On 31 December 2022, the Irish supervisory authority ('DPC') issued two final decisions concerning Instagram and Facebook services in which it found that Meta Platforms Ireland Ltd (Meta IE) did not have a valid legal basis for processing personal data for behavioural advertising purposes by relying on 'contractual necessity' under Article 6(1)(b) GDPR[70]. These decisions followed a binding decision of the EDPB under the consistency mechanism provided under Article 65 GDPR[71]. In October 2023, at the request of the Norwegian SA, the EDPB adopted an urgent binding decision instructing the Irish Data Protection Commissioner to impose a ban on Meta's processing of personal data for behavioral advertising based on the legitimate interest legal basis under Article 6(1)(f) GDPR[72]. Following this urgent binding decision of the EDPB, the DPC issued an enforcement notice against Meta, ordering it to comply with the EDPB urgent binding decision[73]. Shortly before said notice (in October 2023), Meta had announced the roll-out of its new 'pay or consent' subscription model for its Facebook and Instagram services. In April 2024, the EDPB issued an Opinion under Article 64(2) GDPR on this type of models, which found that "[i]*n most cases, it will not be possible for large online platforms to comply with the requirements for valid consent if they confront users only with a binary choice between consenting to processing of personal data for behavioural advertising purposes and paying a fee*"[74]. The Irish DPA is currently assessing Meta's 'pay or consent' business offers to evaluate their compliance with the GDPR[75].

b. **From the perspective of EU consumer protection law**: In February 2024, the European Consumer Organisation (BEUC) filed a complaint against Meta with the Consumer Protection Cooperation Network (CPC)[76]. The complaint accused Meta of engaging in unfair commercial practices and breaching EU consumer protection laws by coercing users into a choice between paying for the service or consenting to targeted ads. In July 2024, the CPC issued a warning to Meta, expressing concerns that the 'pay-or-consent' model might violate EU consumer protection laws by potentially misleading or unduly pressuring users into making a rapid decision and required Meta to respond by September 1, 2024, to address these concerns[77].

c. **From the perspective of the DMA**: concurrently, in March 2024, the European Commission opened an investigation into Meta under the DMA for potential non-

---

[70] Data Protection Commission, Decision of the Irish Data Protection Commission of 31 December 2022, DPC Inquiry Reference: IN-18-5-5, concerning a complaint directed against Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) in respect of the Facebook Service; Decision of the Irish Data Protection Commission of 31 December 2022, DPC Inquiry Reference: IN-18-5-7, concerning a complaint directed against Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) in respect of the Instagram Service.

[71] EDPB Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR), adopted on 5 December 2022; EDPB Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), adopted on 5 December 2022.

[72] EDPB Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR), adopted on 27 October 2023.

[73] Data Protection Commission, Enforcement notice in the matter of Meta Platforms Ireland Limited made pursuant to Sections 133(9) and 133(10) of the Data Protection Act, 2018 and Articles 60 and 66 of the General Data Protection Regulation, 10 November 2023.

[74] EDPS Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, Adopted on 17 April 2024.

[75] Politico, *An exit interview with Europe's most powerful privacy regulator*, 18 January 2024.

[76] BEUC, *Consumer groups file complaint against Meta's unfair pay-or-consent model*, 30 November 2023.

[77] European Commission, *Commission coordinates action by national consumer protection authorities against Meta on 'pay or consent' model*, 22 July 2024, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3862.

compliance with Article 5(2) DMA[78]. The Commission considers that the 'pay or consent' model may not provide an effective less personalised equivalent alternative in case users do not consent, as required under Article 5(2) and Recitals 36 and 37 DMA.

d. **From the perspective of the DSA:** in March 2024, the Commission has formally sent Meta a request for information under the DSA in relation to the Subscription for no Ads options for both Facebook and Instagram. In particular, Meta is requested to provide additional information on the measures it has taken to comply with its obligations concerning Facebook and Instagram's advertising practices, recommender systems and risk assessments related to the introduction of that subscription option[79].

33. The parallel investigations by various authorities into the practices of a number of covered entities underscore the multifaceted nature of regulatory oversight in the digital age. These overlapping inquiries reveal not only the complexities inherent in applying different legal frameworks — such as data protection, consumer rights, and the new rules enacted by the EU during its last parliamentary mandate — but also the challenges in achieving a coherent regulatory approach. Simultaneous actions by various regulators concerning the same practices highlight the potential for conflicts and inconsistencies when such practices are scrutinized from different legal perspectives.

34. Furthermore, these parallel investigations emphasize the critical need for enhanced dialogue, cooperation, and coordination among regulatory bodies to ensure a predictable and effective legal environment that places fundamental rights at the core. Such a need has been increasingly acknowledged by key stakeholders in recent months, including the European Commission. In its July 2024 report on the application of the GDPR, the Commission notes that "[t]*he development of digital regulations raises the need for close cooperation across regulatory fields. Such cooperation is all the more necessary since data protection issues increasingly intersect with questions of, for example, competition law, consumer law, digital markets rules, electronic communications regulation and cybersecurity.*" And although the Commission acknowledges that certain positive developments on cross-regulatory cooperation at EU and national level, it now stresses the "*need for more structured and efficient means of cooperation, in particular to address situations that affect a large number of individuals in the EU and involve several regulators*"[80].

## 3.5. A heterogeneous landscape for cross-regulatory cooperation

35. Under the different parts of the EU Digital Rulebook, supervision is assigned to different regulators. For example, the supervision of gatekeepers under the DMA is entrusted to the European Commission, who will also supervise compliance of VLOPs and VLOSEs under the DSA. In relation to intermediary service providers other than VLOPs and VLOSEs under the DSA, and in the context of other acts of the Digital Rulebook, Member States must designate

[78] European Commission, *Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act*, 25 March 2024, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689.
[79] European Commission, *Commission sends request for information to Meta under the Digital Services Act*, 1 March 2024.
[80] Communication from the Commission to the European Parliament and the Council, Second Report on the application of the General Data Protection Regulation, COM(2024) 357 final, 25 July 2024, p. 18.

competent supervisory authorities[81]. Member States may also decide to designate multiple competent authorities to monitor compliance with different provisions of the same act[82].

36. In some cases, acts of the EU Digital Rulebook foresee bilateral cooperation between authorities competent to supervise them and other authorities, including data protection supervisory authorities. For instance, Member States may facilitate coordination between market surveillance authorities and other relevant national authorities or bodies which supervise the application of Union law that might be relevant for the high-risk AI systems referred to in Annex III of the AI Act[83]. The latter may include data protection supervisory authorities, but also regulators competent to supervise requirements in the areas of employment, finance, education, healthcare, and others. The Dutch data protection authority and the Dutch authority for digital infrastructure (in consultation with twenty other Dutch supervisory authorities that may play a role in AI supervision) have recently made suggestions to the government about the distribution of competences and cross-regulatory cooperation among regulators with regard to AI systems under the scope of the AI Act[84].

37. A distinctive element of various regulations in the EU Digital Rulebook is the creation of fora to promote multilateral cooperation between authorities competent to supervise each of those regulations. Interestingly, several regulations also allude - to significantly varying degrees - to the possibility to cooperate with authorities competent to supervise other EU laws. For example:

    a. Article 29 of the DGA establishes a European Data Innovation Board ('EDIB') in the form of an expert group chaired by the Commission, consisting of representatives of the competent authorities for data intermediation services and the competent authorities for the registration of data altruism organisations of all Member States, the EDPB, the EDPS, the European Union Agency for Cybersecurity ('ENISA'), the Commission, the EU SME Envoy or a representative appointed by the network of SME envoys, and other representatives of relevant bodies in specific sectors;

    b. Article 40 of the DMA mandates the establishment by the European Commission of a high-level group of representatives of European bodies and networks (including the EDPB and the EDPS, the Body of the European Regulators for Electronic Communications, the European Competition Network, the Consumer Protection Cooperation Network, and the European Regulatory Group of Audiovisual Media Regulators) to provide the Commission with advice and expertise in the areas falling within the competences of its members, including for promoting a consistent regulatory approach across different regulatory instruments. The HLG may identify,

---

[81] E.g., in France, ARCOM, the DGCCRF, and the CNIL have been designated as competent authorities in accordance Article 49 of the DSA. See Article 51 of *Loi n°2024-449*, which amended Article 7 of *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*.

[82] For example, in Ireland, nine authorities will be responsible for protecting fundamental rights under the AI Act: the An Coimisiún Toghcháin, Coimisiún na Meán, Data Protection Commission, Environmental Protection Agency, Financial Services & Pensions Ombudsman, Irish Human Rights & Equality Commission, Ombudsman, Ombudsman for Children, and the Ombudsman for the Defence Forces. See Department of Enterprise, Trade and Employment, *Minister Calleary announces key milestone in the implementation of the EU regulation on AI*, 31 October 2024.

[83] Article 74(10) AI Act.

[84] Autoriteit Persoonsgegevens, *AP and RDI: Supervision of AI systems requires cooperation and must be arranged quickly*, 11 June 2024. In their detailed advice of 16 May 2024, the authorities propose that the supervision of high-risk AI applications for which no CE marking is currently required should largely lie with the data protection supervisory authority, which should cooperate with sectoral or domain-specific supervisory authorities to ensure complementary and mutually reinforcing supervision. In particular, "*The starting point is that market surveillance of the AI Act should support and strengthen existing supervision and not frustrate it. Sector and domain-specific supervisors involved will need to exchange and coordinate extensively and frequently with market surveillance authorities. This requires a multilateral coordination and consultation structure that requires capacity and for which resources must also be made available.*"

assess and make recommendations to ensure regulatory consistency concerning the current and potential interactions between the DMA and the sector-specific rules applied by national authorities (including data protection supervisory authorities)[85].

c. National competent authorities under the AI Act will be supported by the European AI Office ('AI Office') and the European Artificial Intelligence Board ('AI Board'). Among other tasks, the AI Office will help the Member States cooperate on enforcement, including on joint investigations[86], and act as the Secretariat of the AI Board. Importantly, the AI Office shall ensure that supervision and enforcement of EU legislation which the Commission is competent to oversee (such as the DMA and the DSA) is fully coordinated with the supervision and enforcement of the AI Act[87]. In turn, the AI Board is the intergovernmental forum for coordination between national competent authorities under the AI Act.

38. Despite these examples that show a degree of awareness of the need to promote cross-regulatory cooperation and consistency at the time of the adoption of the different pieces of the EU Digital Rulebook, several limitations to structured and institutionalised cross-regulatory cooperation can be identified:

- Some of the new regulations explicitly provide for consultation or cooperation between the competent supervisory authority and other authorities[88], while others do not;
- Very limited attention is given to the possibility to exchange information and how it relates to confidentiality obligations[89];
- Most exchanges between competent authorities are foreseen to take place on a 'per-act' basis, without a central coordination mechanism that would bridge the different acts (either at national or EU levels);
- While some of the new regulations foresee the possibility of inviting authorities other than competent authorities to 'board' meetings[90], only the DMA envisages exchanges between multiple authorities on a structural level (via the HLG).

39. Regardless of the introduction of bilateral and multilateral cooperation initiatives at practical and policy levels as outlined above, competent authorities across the EU would still be lacking a dedicated forum where they can iron out potential issues of consistency or promote coherence in the application of EU law in the digital space. As the EDPS's experience with the Digital Clearinghouse showed, it is possible to foster a cross-regulatory dialogue that

---

[85] Article 40(6) DMA.
[86] Article 74(11) AI Act.
[87] Article 3 of the Commission Decision of 24 January 2024 establishing the European Artificial Intelligence Office C/2024/390 OJ C, C/2024/1459, 14.2.2024.
[88] See e.g., Articles 37 and 38 DMA, Article 37(5)(g) DA, and Article 13(3) DGA.
[89] Among the notable exceptions, see Article 74(2) AI Act. See also Articles 15(1) and 36(3) DMA and Recital (72) DMA, which establish that the Commission shall transmit to the EDPB the audited description of profiling techniques submitted to it by gatekeepers *"to inform the enforcement of Union data protection rules*". In addition, see Article 24(2) of the Directive on improving working conditions in platform work, which states that data protection supervisory authorities "*and other national competent authorities shall, where relevant, cooperate in the enforcement of this Directive within the remit of their respective competences, in particular where questions on the impact of automated monitoring systems or automated decision-making systems on persons performing platform work arise. For that purpose, those authorities shall exchange relevant information with each other, including information obtained in the context of inspections or investigations, either upon request or at their own initiative*".
[90] See e.g., Recital (143) DSA: "*In view of possible cross-cutting elements that may be of relevance for other regulatory frameworks at Union level, the Board should be allowed to cooperate with other Union bodies, offices, agencies and advisory groups with responsibilities in fields such as equality, including gender equality, and non-discrimination, data protection, electronic communications, audiovisual services, detection and investigation of frauds against the Union budget as regards custom duties, consumer protection, or competition law, as necessary for the performance of its tasks.*"

surpasses the 'borders' enacted in the various pieces of legislation that apply in the digital economy.

# 4. The way forward: towards a Digital Clearinghouse 2.0

40. The ever-extending web of regulatory requirements applicable to the digital economy in the EU creates further need and impetus for cross-regulatory dialogue and cooperation, to support exploring linked concepts and synergies between different regulations. The need for cross-regulatory cooperation is also highlighted in the recent calls by the Council of the EU[91] and the European Commission[92] to support the dialogue between national and EU regulators competent to oversee rules applicable in the digital economy, in particular those established under the new digital legislation.

41. A particular challenge lies in addressing practical questions of consistent and coherent application and enforcement stemming from both new asymmetrical and existing horizontal regulations, with supervision responsibilities and legal frameworks for cooperation that vary across national borders. Addressing this challenge is also made urgent by the entrenchment of certain players in digital markets. The EDPS proposes paving the way to a Digital Clearinghouse 2.0 to enable effective cross-regulatory cooperation that is fit for the digital age.

## 4.1. Objectives and format

42. As with the first Digital Clearinghouse, its successor should in first instance provide a forum for regulators to identify emerging areas and practices of cross-regulatory concern, facilitate coordination and exchange knowledge, experiences and resources. It should facilitate proactive, collaborative efforts among participating authorities to address potential issues before they become practical problems, ensuring that different authorities are aligned on goals, methods, and responsibilities from the outset.

43. Given the increase in both the number and diversity of relevant authorities, bodies and networks, a Digital Clearinghouse 2.0 would require a slightly different format. While it would be very important to secure the participation of representatives of each body or network that gathers national competent authorities in specific fields at the European level (e.g., the EDPB, ECN, ERGA and others), it needs to be acknowledged that not every issue or topic may be of equal importance to all participants.

44. Therefore, an important feature of this new format would be the facilitation of cooperation in 'variable geometry', providing relevant authorities, bodies and networks the flexibility to join only discussions and working groups on issues that are important for them and where they have or need relevant expertise. Despite acknowledging that participation in this forum would require the investment of time and resources, such 'variable geometry' could be more attractive for authorities, bodies and networks in view of their limited resources and still

---

[91] In May 2024, the Council of the EU outlined its priorities for the 2024-2029 legislative mandate concerning digital policy, with a focus on ensuring an effective, coherent, and efficient implementation of recently adopted laws. See p. 6 of the Council Conclusions: *"UNDERSCORES the need for the Commission and the Member States to foster synergies, avoid duplication and adopt a coordinated approach to the existing governance structures, taking into account the division of competences at EU and national level, in order to avoid the fragmentation of the EU's Digital Single Market as well as to ensure legal certainty. (...) CALLS UPON the Commission, in collaboration with the Member States, to reflect on tools and solutions to build synergies and ensure consistency in the application of existing legislative acts and to explore ways to reduce administrative burden for public and private actors, (...) as well as local authorities."*

[92] Communication from the Commission to the European Parliament and the Council, Second Report on the application of the General Data Protection Regulation, COM(2024) 357 final, 25 July 2024, p. 28.

providing foreseeability in terms of the "when and how" of cooperation. The work programme of the Digital Clearinghouse 2.0 may include a variety of projects or dedicated working groups where regulators plan to work bilaterally or multilaterally, depending on the interests manifested by each participating authority, body or network in a given subject-matter[93].

45. To ensure proximity to the operational work of participants, the activities of the Digital Clearinghouse 2.0 should not focus on abstract themes, but rather on specific goals that would facilitate tangible outcomes (e.g., streamlining cooperation between specific authorities in enforcement scenarios where there is a clear intersection of competencies, focused on the complexities arising in practice from the different touchpoints under various regulations). The Digital Clearinghouse 2.0 should also be a forum where participating authorities share information - to the extent such sharing is legally allowed - about ongoing enforcement actions so as to facilitate further (bilateral or multilateral) engagement with other authorities on those concrete cases where relevant[94]. Several layers of cooperation could thus be envisaged, some focusing on cooperation and coordination at policy level and others focusing on cooperation and coordination at operational level.

46. Specific objectives of the Digital Clearinghouse 2.0 could include:

    a. identifying needs for common guidance[95] as well as identifying enforcement actions requiring further cooperation or coordination, notably where there is an overlap of competences and/or possibilities for synergies;

    b. exchanging knowledge, experiences and resources (e.g., mapping industry trends and practices to provide foresight on emerging technologies and business practices, as well as to identify common enforcement priorities);

    c. exchanging information and promoting best practices as regards cross-regulatory governance and cooperation, including by proposing resources and tools to facilitate cooperation between specific authorities (e.g., a model cooperation protocol or MoU and templates for joint information requests);

    d. preparing recommendations to the EU legislator on how to create necessary (legal) enablers for effective cross-regulatory cooperation among competent authorities.

47. There should be no shortage of substantive issues for a Digital Clearinghouse 2.0 to tackle. From the use of algorithms by large online platforms to deliver advertisements to users based on their inferred attributes, to the exercise of data portability rights across GDPR, DMA and DA, to the collection of personal data from third party sources to develop high-risk AI systems, to the use of deceptive design patterns to subvert users' autonomy, many are the topics in which individuals, covered entities and competent authorities themselves would benefit from further clarity and cross-regulatory alignment, including when it comes to enforcement.

---

[93] See, for example, DRCF, *Workplan 2024/25*, April 2024, available at https://www.drcf.org.uk/__data/assets/pdf_file/0030/283188/DRCF-Workplan-202425.pdf, or the model put forward by Article 7-4 of *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, which created the French national network for coordination of the regulation of digital services. The provision establishes that the network can set up working groups bringing together, on a voluntary basis, representatives of its members with a view to sharing thoughts on particular themes. The Dutch SDT also has a dedicated 'specialized' chamber to discuss the enforcement of the DSA, and another one focused on oversight over algorithms and AI.

[94] To be clear, the Digital Clearinghouse 2.0 would not directly intervene or provide advice on ongoing enforcement activities carried out by competent authorities, but would rather serve as a forum for participating authorities to identify instances where further cooperation may be necessary or beneficial.

[95] A recent example is the ongoing developments of joint guidance on the interplay between the DMA and the GDPR, which the European Commission and the EDPB have announced in September 2024.

48. In terms of coordination, recent national experiences of fostering cross-regulatory dialogue seem to indicate the added value of having a central body providing a secretariat for the Digital Clearinghouse 2.0. In particular, the example of the UK DRCF shows that the presence of a CEO and core team which are dedicated to the pursuit of the DRCF's goals full time - funded by participating regulators - significantly helps the timely delivery of concrete outcomes promoting cross-regulatory coherence, including joint statements, blogs, articles, and papers that garner each participants' expertise. At the same time, it is important to ensure that all concerned regulators are effectively able to contribute on an equal footing and that no single entity unilaterally imposes the agenda for cross-regulatory dialogue and cooperation. For example, all concerned regulators should be able to actively contribute to the development of agendas and work programmes, submit discussion points for meetings of the group, and join (and lead) the work on projects of common interest for participating authorities[96].

49. In order to keep learning from experiences at national, EU and international level it would be important for the existing structures for cross-regulatory cooperation across the EU (such as the Dutch SDT or the Irish DRG), as well as EU-level structures such as the EDIB and the DMA HLG, to participate and share relevant experiences and results. This way, the Digital Clearinghouse 2.0 could also serve as a sort of forum of fora, in many respects the EU equivalent to the International Network for Digital Regulation Cooperation[97] as a European platform for promoting best practices and discussions on digital regulatory cooperation and promoting a coherent approach in that regard across the EU.

50. Although participation in the meetings and activities of the Digital Clearinghouse 2.0 would, in principle, be limited to relevant competent authorities, bodies and networks, the activities of the Digital Clearinghouse 2.0 should also remain sufficiently transparent and open. This could be achieved in several ways, such as publishing activity reports. The secretariat could also organise public consultations and invite relevant stakeholders (like trade associations, civil society organisations, and academics) to gather inputs for matters that are under discussion.

## 4.2. Removing obstacles to 'on-the-ground' cooperation

51. There are important practical challenges that need to be carefully considered in order to facilitate effective cross-regulatory cooperation. As outlined at the end of Chapter 2 of this Concept Note, such challenges may arise from a lack of authorities' own resources to make cross-regulatory cooperation a reality, a lack of internal willingness or willingness from their counterparts to cooperate, as well as insufficient legal or administrative frameworks under EU or national law providing for cooperation mechanisms.

52. Concerning resources to create and maintain cross-regulatory cooperation, the example of the DRCF in the UK illustrates the importance of having dedicated teams within competent authorities focused on establishing permanent contacts with authorities from other legal fields. At a minimum, authorities should consider appointing dedicated contact points and share information on a regular basis. It is equally important, however, to discuss and align on

[96] See, as an example, Article 7-4 of *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, which states that the secretariat of the French national network for coordination of the regulation of digital services (the Ministry for digital) proposes the agenda of the meetings of the network, which can be supplemented by its members.

[97] The INDRC counts on the digital regulation coordination bodies from Australia, Canada, Ireland, the Netherlands and the United Kingdom, and aims to foster discussion between regulators on coherence across digital regimes, and to gather insights into how jurisdictions are approaching domestic regulatory coherence. See the DRCF's latest Statement on the workshop it organized with the OECD on this topic, 8 November 2024.

enforcement priorities to allow the efficient use of each authority's enforcement powers and resources.

53. In cases where risks are lower, it may not make sense to have two authorities investigating the same company for the same conduct under their respective frameworks. In other cases where there are higher stakes, parallel or even joint investigations may be appropriate. Coordination of enforcement activities together may equally help avoid situations of under-enforcement, where competent authorities assume that an authority from a different field is investigating the conduct of a specific company where it is in fact not. Increased cooperation and coordination may also help mitigate the risks of "divide and conquer" strategies that might otherwise be deployed by parties under investigation.

54. To tackle the lack of willingness issue, it is important that authorities motivated to work on the intersection between their and overlapping frameworks come forward and propose to their counterparts from other legal fields to initiate and commit to cooperation initiatives. This sort of proactive attitude towards cooperation may put out fears from other authorities that their competences will be taken over by counterparts from other fields, and contribute to prevent (rather than merely react to) overlaps/conflicts in regulatory actions. In addition to a multilateral MoU that authorities that eventually participate in the Digital Clearinghouse 2.0 may enter into, it might be logical to also enter into more detailed bilateral agreements with authorities from other legal fields (within or beyond their jurisdiction) to stimulate and make binding (on a best-efforts basis) cooperation between them[98]. Such agreements may contain elements that could be impractical to include in a multilateral agreement, such as specifying the frequency of mutual consultations, information obligations, coordination in cases with overlapping competences, joint investigations, and even consequences for non-compliance with its provisions.

55. When it comes to legal bases for cross-regulatory cooperation, existing confidentiality and professional secrecy requirements applicable to the information (including personal data) and evidence collected during investigations are often invoked by competent authorities that hesitate to join efforts with authorities competent to supervise other fields of law[99]. These laws can establish explicit exceptions to such requirements[100]. Ideally, competent authorities should be able in principle to rely on a clear legal basis in national or EU law that allows relevant information, including personal data and trade secrets, to be shared with other competent authorities to the extent necessary for the performance of the respective tasks of the bodies involved. This is without prejudice to the possibility of competent authorities to share or seek information from their counterparts in a manner that would not infringe existing confidentiality and data protection rules (e.g., asking questions about the legality of a certain practice from the perspective of another legal framework in general terms, without disclosing case-specific information that relates to the entity under investigation). If there are difficulties in establishing a functioning cooperation at the level of investigations, authorities should in any case monitor enforcement activities, guidelines, market analysis and other activities undertaken by authorities responsible for the oversight of frameworks that overlap with their own. If important issues are identified, it is advisable to contact the competent authority and offer to exchange information or cooperate on the subject-matter[101].

---

[98] See, for example, the existing coordination protocol that exists between the Dutch consumer protection and competition authority and the local data protection supervisory authority, from 3 November 2016. See also the administrative arrangement between the European Commission and Ofcom to support the enforcement of the DSA and the UK's Online Safety Act, announced on 16 May 2024.
[99] See, for example, Article 54(2) GDPR, Article 84 DSA, Article 36(4) DMA, Article 37(16) DA, Article 26(6) DGA, and Article 70 AI Act.
[100] See, for example, Article 36(3) DMA, which together with Recital 72 DMA, provides that information collected pursuant to Article 15 DMA shall also be transferred to the EDPB to inform the enforcement of the GDPR.
[101] Global Privacy Assembly, *An Enforcement Cooperation Handbook*, Last Updated and Presented at the 43rd Global Privacy Assembly, Mexico City, October 18 – 21, 2021, p. 23: "*it is important to recognize that enforcement cooperation can be as simple and informal as*

56. Even in the absence of clear exceptions to confidentiality and professional secrecy requirements, primary EU law already provides authorities competent to supervise different fields of EU law with reason to share at least certain information with each other.

    a. First, the principle of sincere cooperation under Article 4(3) of the Treaty on European Union - which binds the Member States, including their administrative authorities - obliges those authorities to assist each other in carrying out tasks which flow from the Treaties. This assistance may include, as a minimum, exchanging all strictly necessary information to request clarifications from other authorities and to dispel the requesting authority's doubts regarding the scope of the assessment carried out by the consulted authority[102]. The principle of sincere cooperation is also a general principle of EU administrative law[103] that has a close connection with the principle of administrative cooperation enshrined in Article 197 TFEU[104].

    b. Second, the CJEU has recently set conditions for a duplication of proceedings and penalties to respect the essence of the *ne bis in idem* principle laid down in Article 50 of the Charter, which prohibits double jeopardy[105]. In particular, there should be "*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*"[106]. Otherwise, even where the proceedings initiated by two different authorities pursue complementary aims relating to different aspects of the same unlawful conduct, the sanction resulting from the proceeding initiated second in time may be deemed invalid.

57. Still, these principles, in the absence of specific provisions of EU or EU Member State law providing for more structural cooperation between competent authorities in different fields of EU law, can hardly be said to provide blanket exceptions to confidentiality and professional secrecy obligations that bind said competent authorities. They should, however, provide strong incentives for competent authorities to cooperate with authorities from other fields of EU law to the greatest legally-permitted extent, including by entering into formal and informal cooperation agreements where useful[107]. These agreements could specify when the authorities

---

*sharing best practices, innovative enforcement strategies or other non-confidential information*". See also OECD Directorate for Financial and Enterprise Affairs Competition Committee, *The intersection between competition and data privacy – Background Note*, DAF/COMP(2024)4, 13 June 2024, paragraph 111: "*Informal co-operation may often take place without legislative reforms or a formal legal basis. For more advanced co-operation, a relevant legal basis would be needed for information sharing between authorities and possibly for other kinds of co-ordinated action*".

[102] 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 57 and 58.

[103] European Parliament Policy Department C: Citizens' Rights and Constitutional Affairs, *The General Principles of EU Administrative Procedural Law*, 2015, p. 8.

[104] Lottini, Micaela, '*From 'Administrative Cooperation in the Application of European Union Law to 'Administrative Cooperation in the Protection of European Rights and Liberties'*', European Public Law 19, no. 1 (2012) 127-147, p. 131.

[105] The *ne bis in idem* principle prohibits a duplication both of proceedings and of penalties of a criminal nature for the same acts and against the same person. See Judgement of the Court of Justice of 20 March 2018 Menci, C-524/15, ECLI:EU:C:2018:197, paragraph 25 and the case-law cited.

[106] 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.

[107] The EDPB has defined as one of its main priorities for the next three years the cooperation with other authorities "*on matters with an impact on data protection, in particular with consumer protection authorities, competition authorities, and authorities competent under other legal acts, including the EU Artificial Intelligence Act or those adopted under the European Data Strategy and the Digital Services Package*". See EDPB Strategy 2024-2027, adopted on 18 April 2024, p. 4. In its recent Report on the review of the functioning of the GDPR, the Commission invites the EDPB and national data protection authorities to "*establish regular cooperation with other sectoral*

should consult each other and what information they should exchange, including in the context of their supervisory proceedings.

58. The EDPS is of the opinion that certain cross-regulatory cooperation initiatives can be implemented within the currently applicable legal framework. However, the principles of sincere cooperation and *ne bis in idem* should motivate the EU and Member States' legislators to introduce legal requirements providing for structured and institutionalised cooperation between the various authorities competent to supervise the EU Digital Rulebook[108]. Legislative intervention could provide legal certainty about the specific elements of information that competent authorities are required or allowed to share with each other in relation to investigations, since existing CJEU case law is not very specific in this regard. Such uncertainties are not only likely to stifle effective cross-regulatory cooperation, there is also a real risk of divergent approaches to this issue across different regulatory domains. There is therefore still a compelling argument to be made for legislative intervention, including at EU level, either via 'first-level' legislation or via implementing the existing basic acts, to lay down arrangements for cooperation and coordination between the various competent authorities.

## 4.3. Raising cross-regulatory cooperation to another level: the need for legislative intervention

59. Beyond general information exchange and policy and priorities alignment, in an increasingly complex regulatory architecture, authorities competent to oversee compliance with EU laws that apply in the digital economy are often missing a clear, explicit, and sufficiently detailed legal basis allowing them to exchange information that might be relevant for enforcement in their respective areas of competence[109]. If it were to be introduced, such a legal basis should explicitly refer to the competent authorities involved in the cooperation (e.g., by referring to the specific EU legislative acts whose supervision would be fostered via the legally-mandated cooperation)[110], and identify at a high level the circumstances in which cooperation should take place among them, including the general purpose of such exchanges and the moments when they may take place. Authorities obtaining data via such exchanges would need to be

*regulators on issues with an impact on data protection, in particular those established under new EU digital legislation, and actively participate in EU-level structures designed to facilitate cross-regulatory cooperation*". See Communication from the Commission to the European Parliament and the Council, Second Report on the application of the General Data Protection Regulation, COM(2024) 357 final, 25 July 2024, p. 28.

[108] See again 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, paragraph 55: "*(...) the existence of a provision of national law providing, as does Article 14 of the loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges (Law of 17 January 2003 on the statute of the regulator of the Belgian postal and telecommunications sectors) (Moniteur belge, 24 January 2003, p. 2591), which it is for the referring court to verify, for cooperation and the exchange of information between the authorities concerned, would constitute an appropriate framework for ensuring the coordination to which reference is made in paragraph 51 of the present judgment*".

[109] Even where there are robust legal bases - such as under Section 50f of the German Competition Act -, exchanges of information are often limited to authorities within the Member State that approved the legislative measure, whereas there is often a need to share information with and obtain information from authorities from different fields that are established in a different Member State.

[110] A similar approach was followed by the EU legislator in Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC OJ L 409, 4.12.2020, p. 1–27, when defining the scope of the right to bring representative actions for infringements of EU law under Article 2(1) of the Directive: "*This Directive applies to representative actions brought against infringements by traders of the provisions of Union law referred to in Annex I, including such provisions as transposed into national law, that harm or may harm the collective interests of consumers*". Annex I then lists the (currently 66) EU legal acts whose infringements may be invoked under the Directive, including Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, the Unfair Commercial Practices Directive, the ePrivacy Directive, the GDPR, the Audiovisual Media Services Directive, Directive (EU) 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, the DSA, the DMA, the Data Act, and the AI Act.

subject to obligations of professional secrecy and confidentiality[111] and would be subject to EU data protection law insofar as personal data is shared.

60. The EDPS invites the European Commission to consider presenting a legislative proposal to enable effective cross-regulatory cooperation among the different regulators supervising the rules that apply in the digital economy, including information sharing in specific cases and joint enforcement actions. Such an initiative - which would not necessarily entail 'reopening' the texts of the different parts of the EU Digital Rulebook - would be well-aligned with the Commission's intention to "*reflect on how to better address the need for structured and efficient cross-regulatory cooperation to guarantee the effective, consistent and coherent application of EU digital rules, while respecting the competence of data protection authorities for all questions concerning the processing of personal data*"[112].

61. Besides the previously mentioned elements, such a legislative proposal should allow competent authorities to use information obtained from other authorities to exercise their respective tasks and duties where they deem such information to be relevant in those contexts[113]. At the same time, this legislative measure would need to include procedural safeguards to have due regard to the fundamental rights to good administration and effective judicial protection of investigated persons[114], including the right to be heard access to the file and compliance with the *ne bis in idem* principle.

62. In the long term, beyond making it possible for competent regulators from different legal fields to cooperate and share information with each other, there may be a need to address more systematically potential issues of inconsistency and tensions arising from the application of different parts of the EU Digital Rulebook to the same conduct. Therefore, the EDPS urges the Commission to carefully monitor the implementation of the EU Digital Rulebook, including from a cross-regulatory perspective. On the basis of such analysis, it may be appropriate to consider a revision of some parts of the EU Digital Rulebook in order to clarify the relationship between several of its substantive rules, streamline the number of regulators in charge of overseeing closely-related EU legal acts and formally create an independent central body to promote consistency and coherence in their practical application.

# 5. Conclusion

A. As this Concept Note has shown, the proliferation of (often overlapping) legal requirements applicable to market players in the digital economy at the EU level has placed such players, as well as the authorities competent to supervise them, in a difficult position. They are compelled to implement and apply rules that cover the same or similar conduct - although to pursue different policy objectives - , but that may produce inconsistencies that are not easily solved by isolated interpretative efforts. While some of the norms contained in the EU Digital

[111] Judgment of the General Court of 8 July 2008 Yves Franchet and Daniel Byk v European Commission, T-48/05, ECLI:EU:T:2008:257, paragraphs 217 and 218.
[112] See Communication from the Commission to the European Parliament and the Council, Second Report on the application of the General Data Protection Regulation, COM(2024) 357 final, 25 July 2024, p. 29.
[113] The rule under CJEU case law is that evidence and documents collected during an investigation should not be repurposed for another investigation without authorisation from the investigated party, in case of which new copies of the documents must be requested based on the newly authorised or legitimate procedure. See Judgment of the Court of Justice of 15 October 2002 Limburgse Vinyl Maatschappij and Others v Commission in Joined Cases C-238/99 P, C-244/99 P, C-245/99 P, C-247/99 P, C-250/99 P to C-252/99 P and C-254/99 P, ECLI:EU:C:2002:582, paragraphs 298 to 304. Authorities are more flexible when it comes to opening investigations on the basis of indicative information collected during an earlier separate investigation, as long as they do not use that indicative information as evidence in the second proceedings. See Judgment of the Court of Justice of 17 October 1989 Dow Benelux NV v Commission of the European Communities, Case 85/87, ECLI:EU:C:1989:379, paragraph 19.
[114] Articles 41, 47, and 50 Charter.

Rulebook refer to each other (e.g., the DMA and the DSA often referring to the GDPR concepts and obligations), and some establish precedence between them (e.g., EU data protection law prevailing over the DA), this is not always the case.

B. The initiation or conclusion of parallel legal proceedings by competent authorities against a few well-known companies under different EU frameworks (with Meta's "pay or consent" model being a prime example) demonstrates that cooperation among such authorities is no longer merely desirable, but a necessity. Recent judgments of the CJEU focused on the principle of sincere cooperation and the *ne bis in idem* principle underscore that alignment between regulators is mandatory as a matter of primary EU law, and authorities in many EU Member States have started to take note.

C. While bilateral and multilateral instances of dialogue - sometimes supported by semi-formalised structures - have appeared and are starting to effectively promote cross-regulatory coherence, many such initiatives face a number of important obstacles. Such obstacles may stem from a lack of resources of competent authorities, to a lack of expertise in other legal fields to detect potential regulatory overlaps and tensions, of willingness and the ability to lawfully share information and evidence concerning pending investigations. Moreover, many of the rules that competent authorities in EU Member States apply in the digital economy are EU law, which should be interpreted and applied consistently. Some acts of the EU Digital Rulebook foresee bilateral cooperation between authorities competent to supervise them and other authorities, as well as means designed to promote multilateral cooperation, albeit always in relation to a specific legal act. An EU-level forum where authorities competent to enforce the different parts of the EU Digital Rulebook can come together to discuss matters of coherent application of these laws more generally is yet to be established.

D. Against this background, and encouraged by recent calls by the Council of the EU and the Commission to address issues related to potential cross-regulatory inconsistencies, the EDPS proposes a number of possible actions that may be taken in the near future by relevant stakeholders. These actions may be taken simultaneously or progressively, given that they involve different degrees of effort, investment and impact.

    a. First, the EDPS proposes **paving the way to a Digital Clearinghouse 2.0** as a forum for interested regulators to identify emerging areas of cross-regulatory concern, facilitate coordination and to exchange knowledge, experiences and resources. The Digital Clearinghouse 2.0 would preferably have a secretariat and dedicated resources within it and each participating regulator to prepare concrete outputs of the cross-regulatory dialogue it would promote. Meetings and working groups could function in a 'variable geometry', providing relevant authorities and bodies the flexibility to join only work on issues that are important for them and where they have or need relevant expertise.

    b. Second, the EDPS notes that competent authorities are often missing a clear, explicit, and sufficiently detailed legal basis allowing them to exchange information that might be relevant for enforcement in their respective areas of competence. Therefore, it invites the European Commission to consider putting forward a new legislative proposal needed to enable effective cross-regulatory cooperation among the different regulators supervising the rules that apply in the digital economy. Such a legislative proposal should in particular allow competent authorities to use information obtained from other authorities to exercise their respective tasks and duties, while having due regard to the fundamental rights to good administration and effective judicial protection of investigated persons.

    c. Third, the EDPS urges the Commission to closely monitor the application of EU law in the digital economy during its next mandate to assess whether it may be appropriate to revisit some parts of the EU Digital Rulebook. Future regulatory interventions could

for instance clarify the relationship between the substantive rules of various EU acts, streamline the number of regulators in charge of supervising them, and formally create an independent and dedicated central body to promote coherence in their practical application.