Follow the (personal) data: Positioning data protection law as the cornerstone of EU’s ‘Fit for the Digital Age’ legislative package

Dr. Gabriela Zanfir-Fortuna*

Working Paper – Forthcoming in EDPS At 20 Anniversary Volume, June 2024

Abstract

This contribution explores the relationship between existing EU data protection law, in particular Article 8 of the EU Charter of Fundamental Rights (the right to the protection of personal data) and the General Data Protection Regulation¹, with the EU’s new digital rulebook, as announced in 2020 by the European Commission’s ‘Europe Fit for the Digital Age’ plan. With most of those legislative initiatives now adopted and in force, this analysis advances the idea that EU data protection law is inevitably the cornerstone of all legal frameworks that purport regulating conduct in the digital economy and the digital space involving personal data. It relies on Opinions and Statements published primarily by the European Data Protection Supervisor, sometimes in conjunction with the European Data Protection Board, as well as on case law of the Court of Justice of the EU applying Article 8 Charter. This chapter shows that regardless of the number, complexity and depth of various legal acts focusing on conduct and relationships in the digital space, ultimately data protection law and the supervisory authorities entrusted with its enforcement remain at the core of protecting the fundamental rights of individuals and society from risks and systemic risks resulting from the use of any technology relying on processing of personal data, as well as from personal data sharing among businesses and public authorities.


* Vice President for Global Privacy, Future of Privacy Forum, and former legal officer at the European Data Protection Supervisor. The opinions expressed are those of the author alone. The author can be contacted at gabrielazf@pm.me.

Electronic copy available at: https://ssrn.com/abstract=4794182
1. Tilting a carefully negotiated balance

The new digital rulebook of the European Union is taking up much of the public attention since 2020, when the European Commission presented its ‘Europe Fit for the Digital Age’ initiatives in a series of White Papers and Communications. The Commission did so only two years after the General Data Protection Regulation (‘GDPR’) became applicable and without waiting to see whether its strengths would change business models and data practices, or how it would strengthen people’s awareness of how their personal data is used, strengthening control over their digital traces and digital self.

The legislative package announced four years ago soon became reality. The Digital Services Act (‘DSA’), the Digital Markets Act (‘DMA’), the Data Act, the Data Governance Act (‘DGA’) are now adopted and most of them will become fully applicable in 2024. The EU’s AI Act (‘AIA’) is close to adoption, while other closely-linked initiatives, such as the Platform Workers Directive and the European Health Data Space are being advanced in their legislative journey. In an uphill battle during their legislative process, the European Data Protection Supervisor (‘EDPS’), sometimes with the support of the European Data Protection Board (‘EDPB’), pushed for cohesion of this regulatory juggernaut with the already established EU data protection law and its governance structure, flagging early on the risk of confusion, legal uncertainty, and ineffective enforcement.

---

11 See for example the EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), adopted on 4 May 2023, p. 2, stating ‘with this joint Opinion, the EDPB and the EDPS aim to draw attention to a number of overarching concerns on the Proposal on Data Act and urge the co-legislature to take decisive action’; or the EDPS Opinion 2/2021 on the Proposal for a Digital Markets Act, issued on 10 February 2021, p. 3, where the EDPS welcomed the legislative proposal, ‘as
It was as early as 2017 when the EDPS expressed concerns related to the adoption of laws in the digital realm that overlap with the (then) recently adopted GDPR. ‘Fundamental rights such as the right to the protection of personal data cannot be reduced to simple consumer interests, and personal data cannot be considered as a mere commodity’\(^\text{12}\), the EDPS wrote in its Opinion on the Proposal for a Directive on contracts for the supply of digital content. The same Opinion also clearly stated 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’\(^\text{13}\).

The European Commission did not take this advice to heart. In subsequent Opinions related to the avalanche of new legislation proposed following the ‘Europe fit for the digital age’ communications, the EDPS, sometimes in conjunction with the EDPB\(^\text{14}\), highlighted concerns related to the legal uncertainty created by the overlap of the scope of application and rules of the GDPR with the proposed legislation and systematically called for rules that are aligned to the comprehensive legal framework already in place and applicable to all processing of personal data, across industries, public services and regardless of the size of the entities processing it.

Starting with the Opinion on the EU Strategy for Data in 2020, before the Commission published any of the legislative proposals that were to come, the EDPS recalled that ‘the GDPR provides for a solid basis, also by virtue of its technologically neutral approach, for the development and implementation of the Strategy’\(^\text{15}\) and, optimistically, supported the ‘Commission’s commitment to develop the Strategy in full compliance with the GDPR’\(^\text{16}\).

Furthermore, in its Opinion on the White Paper on AI, the EDPS responded to the claims therein that transparency, traceability and human oversight of AI systems are not specifically covered under current legislation: the EDPS ‘is of the view that the GDPR fully reflects the mentioned key requirements and it applies to both private and public sectors processing personal data’\(^\text{17}\). The


\(^{13}\) 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.

\(^{14}\) In addition to the EDPB-EDPS Joint Opinions, see also the EDPB Statement on the Digital Services Package and Data Strategy, adopted on 18 November 2021.


EDPS specifically mentioned in this regard Article 5(1)(a) – the principle of lawfulness, fairness and transparency, Articles 12 to 14 – transparency requirements, including regarding the logic involved in automated decision-making, and more broadly Article 5(2) – accountability. ‘Therefore, this does not seem an issue for the EU’s data protection legislation’\textsuperscript{18}, the EDPS added.

As the legislative proposals for the DSA, DMA, DGA and AIA had been published by the end of 2021, and the proposed text of the Data Act was about to be published, the EDPB issued a sobering statement, saying that ‘\textit{without further amendments, the proposals will negatively impact the fundamental rights and freedoms of individuals and lead to significant legal uncertainty that would undermine both the existing and future legal framework. As such, the proposals may fail to create the conditions for innovation and economic growth envisaged by the proposals themselves}’\textsuperscript{19}.

Why are the EDPS and EDPB so concerned with overlapping laws in the digital realm and the legal uncertainty this may create? And where does the adoption of this full suite of new laws leave the GDPR, data protection law and the role of Data Protection Authorities (‘DPAs’)? This contribution will provide some answers to these questions. The following section will look into the scope of application of the DMA, DSA, DGA, Data Act and AIA and will show how they all ultimately regulate processing of personal data and the entities engaging in it, overlapping thus with the GDPR and triggering its application in several, if not most, scenarios regulated by the new laws (Section 2). Next, it will be argued that due to this fact Article 8 Charter will likely also be triggered in the application of the new laws, foreseeing possible future challenges at the CJEU (Section 3). The fourth section will show how the new laws establish precedence of the GDPR in sometimes clear and sometimes less clear terms, positioning thus the GDPR as the cross-functional backbone of the Data Strategy laws (Section 4). Before drawing conclusions (Section 6), the enforcement framework proposed by the new laws will be briefly analysed, showing that the supervisory authorities entrusted with the application of data protection law do not have a clear role in the new EU digital rulebook, despite the significant role that processing of personal data has in defining its scope (Section 5).

2. The EU’s New Digital Rulebook also regulates processing of personal data and the entities engaging in it

The GDPR applies to the ‘processing’ of ‘personal data’ wholly or partly by automated means (Article 2(1) GDPR) and to some non-automated processing, regardless of industries, business models, public services provided, contexts, nature or size of the entities processing the data. Both concepts of ‘processing’ and ‘personal data’ are broadly defined in Article 4 of the Regulation and


\textsuperscript{19} EDPB Statement on the Digital Services Package and Data Strategy, adopted on 18 November 2021, p. 2.
have also been interpreted broadly by supervisory authorities, national courts and the CJEU\(^\text{20}\). Both concepts refer to ‘any information’ that is related to an ‘identified or identifiable natural person’, and to ‘any operation or set of operations’ performed on such information.

Showing just how far-reaching the rules of the GDPR are, a case-law report on its Article 22 (the right not to be subject to automated decision-making), included cases involving the use of social media platforms, the use of facial recognition systems in schools and supermarkets, automated grading of students, automated assessing for distribution of social benefits by public authorities, management of gig workers through gig platforms, among many other scenarios\(^\text{21}\). The entities bearing legal obligations under the GDPR are ‘controllers’ and ‘processors’. Both of them can be any natural or legal person, as long as they establish the purposes and means of processing (controllers) or process personal data on behalf of an entity that does so (processors).

The DSA applies to intermediary services, including online platforms, offered to recipients of the service\(^\text{22}\) and sets out a complex set of rules, from takedown of illegal content online, to forbidding profiling of minors for ad targeting, forbidding profiling based on sensitive data for ad targeting, to offering researchers access to data held by Very Large Online Platforms and Search Engines (‘VLOPs’/‘VLOSEs’). As explained by the European Commission, the covered intermediary services may include online marketplaces, social networks, content-sharing platforms, app stores and online travel and accommodation platforms\(^\text{23}\). For instance, the same entities (‘providers of online platforms’) that under the DSA have a prohibition to present ads to users stemming from ‘profiling’ them based on sensitive personal data\(^\text{24}\) are also controllers under the GDPR whenever they engage in any type of profiling on their platforms.

The DMA applies to core platform services provided or offered by ‘gatekeepers’ to business users and end users\(^\text{25}\). Its defined purpose is ‘to contribute to the proper functioning of the internal market by laying down harmonized rules ensuring for all businesses, contestable and fair markets in the digital sector’\(^\text{26}\). The Commission explains that ‘gatekeepers’ are “digital platforms with a systemic role in the internal market that function as bottlenecks between businesses and consumers for important digital services’\(^\text{27}\). The rules of the DMA include obligations that specifically refer to processing personal data, such as a prohibition for gatekeepers to ‘combine personal data from

\(^\text{20}\) See, for instance, CJEU Research and Documentation Directorate, Fact Sheet on Protection of Personal Data, November 2021, p. 12-19.


\(^\text{22}\) Article 2(1) DSA.


\(^\text{24}\) Article 26(3) and Recital 68 of the DSA.

\(^\text{25}\) Article 1(2) DMA.

\(^\text{26}\) Article 1(1) DMA.

the relevant core platform service with personal data from any other services provided by the gatekeeper or with personal data from third-party services”\(^\text{28}\).

The Data Act lays down harmonised rules for a series of ‘data operations’, which often involve sharing or other types of processing of personal data, such as making available product data and related service data to the user of a connected product or a related service, or a vaguely worded ‘making available of data by data holders to data recipients’ and ‘to public sector bodies’\(^\text{29}\). In Article 1(2), which defines its scope of application, the Data Act confirms that it ‘covers personal and non-personal data’.

The DGA lays down, among other things, conditions for the re-use of certain categories of data held by public sector bodies, rules for the provision of data intermediation services and a framework for voluntary registration of entities processing data ‘made available for altruistic purposes’\(^\text{30}\). The DGA mentions both ‘personal data’ and ‘non-personal data’ in its provisions, usually involving ‘sharing’ or ‘making available’ such data as operations.

Finally, the AI Act lays down harmonised rules for the placing on the market, the putting into service and the use of AI systems and General Purpose AI models, as well as prohibitions of certain AI practices, specific requirements for high-risk AI systems and their operators, and transparency rules related to AI systems, among other issues\(^\text{31}\). Certain type of scoring based on personal data, including inferred personal data, as well as real time facial recognition systems are among the prohibited AI practices\(^\text{32}\). At the same time, providers of high-risk AI systems are under an obligation to process special categories of personal data as defined in Article 9 GDPR, ‘to the extent they are strictly necessary for the purposes of ensuring bias detection and correction’\(^\text{33}\).

Even briefly looking at the subject matter and scope of application of these legal acts, it is no surprise that the EDPB pointed out 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’\(^\text{34}\). The EDPB was thus worried 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’\(^\text{35}\).

---

\(^{28}\) Article 5(2)(b) DMA.
\(^{29}\) Article 1(1)(a), (b) and (c) Data Act.
\(^{30}\) Article 1(1) DGA.
\(^{31}\) Article 1(1) AI Act, as adopted by COREPER.
\(^{32}\) Article 5 AI Act, as adopted by COREPER.
\(^{33}\) Article 10(5) AIA, as adopted by COREPER.
The amendments to these proposals that followed in the legislative process did not alleviate the concerns of legal uncertainty due to the significant potential overlap of their scope of application with that of existing data protection law. Wojciech Wiewiórowski, the European Data Protection Supervisor, highlighted in public remarks at the end of 2023, that ‘even though each Act pursues its own objectives, several provisions explicitly regulate processing of personal data, sometimes even explicitly referring to GDPR definitions, concepts and obligations’\textsuperscript{36}.

As shown in the following section, this fact is particularly relevant in the light of case-law of the Court of Justice of the EU (‘CJEU’) on the effective application of Article 8 of the EU Charter of Fundamental Rights on the right to the protection of personal data.

3. The EU’s New Digital Rulebook includes interference with the fundamental right to the protection of personal data

In the seminal judgment of Digital Rights Ireland, which saw the 2006 Data Retention Directive\textsuperscript{37} annulled in its entirety eight years after it was adopted, the CJEU established unequivocally that the whole Directive at issue ‘constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data’\textsuperscript{38} (emphasis added). After finding, among other things, that the Directive ‘does not lay down any objective criterion by which the number of persons authorized to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued’\textsuperscript{39}, and that it ‘does not contain any substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use’,\textsuperscript{40} the Court established that the Directive ‘does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter’\textsuperscript{41}, and it annulled the entire legal act\textsuperscript{42}.

The finding that a legal act merely providing for the processing of personal data constitutes an interference with Article 8 of the Charter was confirmed in subsequent case-law of the CJEU. In Ligue des droits humains, the CJEU restated that ‘processing of PNR data as that covered by the PNR Directive also falls within the scope of Article 8 of the Charter because it constitutes

\textsuperscript{36} Wiewiórowski, W., Brussels Privacy Symposium on the EU Data Strategy, Opening Remarks, 14 November 2023.
\textsuperscript{38} Judgement of the Court of Justice of 8 April 2014, Digital Rights Ireland and Seitlinger and others, C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 36.
\textsuperscript{39} Digital Rights Ireland and Seitlinger and others, paragraph 62.
\textsuperscript{40} Digital Rights Ireland and Seitlinger and others, paragraph 61.
\textsuperscript{41} Digital Rights Ireland and Seitlinger and others, paragraph 65.
\textsuperscript{42} See also further the contribution by Kranenborg, H., ‘The EDPS and the never-ending story of data retention’, Chapter …. 

Electronic copy available at: https://ssrn.com/abstract=4794182
processing personal data within the meaning of that article, and, accordingly, must necessarily satisfy the data protection requirements laid down in that article.\footnote{Judgment of the Court of Justice of 21 June 2022, Ligue des droits humains, in C-817/19, ECLI:EU:C:2022:491, paragraph 95.} Additionally, the Court confirmed that ‘it is settled case-law that the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to those data with a view to their use by public authorities. In this connection, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference.\footnote{Ligue des droits humains, paragraph 96.}’ Assessing the safeguards put in place, ultimately the Court ruled that the PNR Directive is consistent with the provisions of the Charter, including Article 8.\footnote{Ligue des droits humains, paragraph 2 of the Executive part of the judgment.}

All legal acts from the European Commission’s ‘EU fit for the digital age’ package analysed in this chapter include at least some instances of clear obligations to process personal data for the actors covered, or lay down conditions for such processing, notwithstanding the overall potential overlap in scope of application with the GDPR and other EU data protection law. Understanding that the ‘data’ subject to the application of these laws include ‘personal data’ pursuant to their ‘Definitions’ clauses, there are obvious examples of such obligations:

- Article 40 of the DSA and its obligation for VLOPs/VLOSEs to provide access to the data necessary (i.e. ‘making [personal] data available’) to monitor their compliance with the regulation to competent authorities and vetted researchers;
- Article 6(9) of the DMA and its obligation for gatekeepers to ‘provide end users and third parties authorized by an end user, at their request and free of charge, with effective portability of data provided by the end user or generated through the activity of the end user … including by the provision of continuous and real-time access to such data’;
- Article 4 of the Data Act, including obligations to make product data and related service data accessible to the user and Article 14 of the Data Act including an obligation to make data available to public sector bodies;
- Article 10(5) AIA, including an obligation for providers of high-risk AI systems process special categories of personal data as defined in Article 9 GDPR ‘to the extent they are strictly necessary for the purposes of ensuring bias detection and correction’.\footnote{Article 10(5) AIA, as adopted by COREPER, see Council Doc. 8115/21, 26 January 2024.}

These are all provisions which constitute interference with the right to protection of personal data as provided by Article 8 Charter, to the extent that the data at issue includes personal data (which is more likely than not, given the nature of the regulated entities). Even though there is not an obvious instance where such interference is created directly by the DGA, that Regulation details...
conditions for re-use of data, including personal data, held by public sector bodies, as well as a framework for lawfully ‘donating’ personal data (making that data available to specific entities such data on the basis of consent), as well as a framework for recognising data intermediaries, explicitly dealing with requests from individuals that seek to make their personal data available and to exercise their rights under the GDPR. Regulating frameworks and procedures for sharing data including personal data, and for the exercise of the data subject rights under the GDPR is relevant for respecting the conditions of Article 8 Charter, especially taking into account its second paragraph which specifically refers to conditions of lawfulness for processing and to access and correction as data subject rights.

Assessing whether the interference with Article 8 of the Charter, stemming from the provisions summarised above is justified, as well as potentially other provisions of the ‘EU fit for the digital age’ legislative package, requires a detailed analysis of the law. The CJEU explained that law including interference with fundamental rights ‘must itself define the scope of limitation on the exercise of the right concerned’47, even if flexible for different contexts and changing circumstances, and that, with regard specifically to interference with the right to the protection of personal data, the law ‘in order to satisfy the proportionality requirement, ... must lay down clear and precise rules governing the scope and application of the measures provided for and imposing minimum safeguards, so that the persons whose data have been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse’48. As the effects of this legislative package and its various provisions stimulating processing of personal data at varying scale will unfold, it should not be surprising if challenges of the validity of these provisions will be brought to the CJEU in the light of Article 8 EU Charter in the following years.

Notwithstanding the potential interference with the right to the protection of personal data created directly by some of these provisions, another fact should be taken into account: the material and personal scope of application defined by the laws analysed in this chapter (see in particular Section 2) will inevitably overlap with ‘controllers’ and ‘processors’ ‘processing personal data’ under the GDPR or other relevant EU data protection secondary law. The next section will briefly discuss how this conflict of law is being solved and point to some additional areas of uncertainty.

4. The EU’s New Digital Rulebook applies without prejudice to the GDPR

Section 2 demonstrated that the legal acts of the Data Strategy package are also regulating the processing of personal data and the entities engaging in it. As a result, two questions arise: first, are the new laws consistent with the rules of the GDPR and other secondary data protection law, and second, if there are instances where they are not consistent, which of the two laws apply?

47 Ligue des droits humains, paragraph 114.
48 Ligue des droits humains, paragraph 117.
A survey of the EDPS and the EDPB-EDPS Joint Opinions on the legislative proposals of the new legislative acts shows that these questions are acute. Take, for instance, the Joint Opinion on the DGA, in which the EDPB and the EDPS considered that the Proposal raises significant inconsistencies with the GDPR, as well as with other Union law and laid out five aspects where this happens, from broad issues like the ‘subject matter and scope of the Proposal’, to specific issues like ‘legal basis for the processing of personal data’. Similarly, in their Joint Opinion on the Data Act, they considered that ‘additional safeguards are necessary to avoid lowering the protection of the fundamental rights to the privacy and the protection of personal data in practice’ and urged the co-legislature to take ‘decisive action’. Concrete examples of such inconsistencies included the obligation to make data available to public sector bodies, including Union bodies, in case of exceptional need, and the extension of a right to access data to entities other than the data subject, including businesses. They encouraged the Commission ‘to ensure that data protection rules and principle shall prevail whenever personal data are being processed’.

The EDPB-EDPS Joint Opinion on the EU AI Act proposal stressed that ‘the Proposal has prominently important data protection implications’ and specifically mentions that the GDPR, the EUDPR and the LED have to be ‘considered as a prerequisite on which further legislative proposals may build upon without affecting or interfering with the existing provisions, including when it comes to the competence of supervisory authorities and governance’. They also highlighted that the plea to ensure consistency with the data protection acquis ‘is not only for the sake of legal certainty’, but ‘also to avoid that the Proposal has the effect of directly or indirectly jeopardizing the fundamental right to the protection of personal data, as established under Article 16 of the TFEU and Article 8 of the Charter’.

All these concerns were raised during the legislative process. They focused both on ensuring the precedence of the GDPR (and other data protection law acquis where needed) in the final text of the law, and on aligning the provisions on substance in instances where future conflict of laws

---

seemed obvious or where there was a risk of non-compliance with the fundamental right to the protection of personal data.

Each of the five legal acts establish, without exception, the precedence of the GDPR (and other data protection acquis where necessary), some in clearer terms than others:

- The DSA, the DGA, and the Data Act include articles\(^{56}\) establishing that they are ‘without prejudice’ to EU law on the protection of personal data, all quoting the GDPR, and some also additional data protection legislative acts.

- The DMA includes similar wording establishing the precedence of the GDPR, but only in a recital\(^{57}\). It omits to include this language in the main text of the law, in Article 1 defining its scope which includes references to other law taking precedence over the DMA. However, the provision of the DMA establishing accountability of gatekeepers to ensure and demonstrate compliance with their main obligations in the Act (Article 8(1) DMA) also adds that the way in which gatekeepers implement those obligations must comply with all other applicable law, “in particular” the GDPR, the ePrivacy Directive and a suite of additional laws, from consumer protection to product safety.

- The AI Act also defines the relationship between itself and EU data protection secondary law in an article, but uses more evasive language, saying that the Act ‘shall not affect’ the GDPR, the EUDPR, the ePrivacy Directive and the LED. The first part of the provision also states that EU data protection and privacy law ‘applies to personal data processed in connection with the rights and obligations laid down in this Regulation’, which is a vague formulation since it does not seem to immediately include processing of personal data in relation to AI systems covered by the Act. A helpful recital further clarifies that the Act ‘does not affect the obligations of providers and deployers of AI systems in their role as data controllers or processors stemming from national or Union law on the protection of personal data in so far as the design, the development or the use of AI systems involves the processing of personal data’\(^{58}\).

Therefore, all these new legislative acts of the ‘EU fit for the digital age’ strategy acknowledge the potential of overlap between them and the GDPR (as well as other relevant data protection laws), by establishing rules for potential conflict of laws applying to the same material and personal scope delineated by (likely) processing of personal data as part of the conduit they regulate.

Despite establishing such precedence rules, avoiding divergence in interpreting and applying these new acts in conjunction with the GDPR and other data protection law will not be an easy task. Enforcement of the new rules is entrusted to a potentially very diverse set of new and old national

\(^{56}\) Article 2(4)(g) DSA, Article 1(3) DGA, and Article 1(5) Data Act.

\(^{57}\) Recital 12 DMA.

\(^{58}\) The Recital is provisionally numbered 5aa in the text adopted by COREPER, see Council Doc. 8115/21, 26 January 2024. See also further the contribution by Smuha, N., ‘The paramountcy of data protection law in the age of AI (Acts)’, Chapter …..
regulators to be appointed by Member States, in addition to some core enforcement functions that the European Commission has.

5. **The EU’s New Digital Rulebook does not have a clear role for DPAs in its enforcement structure**

The EDPS identified as significant the issue of enforcement of the new digital laws announced in the ambitious plans of the European Commission, starting with the Opinion on the Strategy itself, even before the texts of the proposals were published. ‘The EDPS underlines that in the context of future governance mechanisms the competences of the independent supervisory authorities for data protection must be properly respected. (...) Cooperation and joint investigations between all relevant public oversight bodies, including data protection supervisory authorities, should be encouraged’.59

Despite this advice, the EU legislator opted to create a new web of digital enforcers and regulators, leaving it to the Member States to choose one or more enforcers for the new Acts, with the exception of the centralized enforcement powers given to the European Commission in the DMA, the DSA for VLOPs/VLOSEs, and the AI Act for General Purpose AI models. The AI Act also has a role for the EDPS as enforcer, in relation to EU agencies and bodies acting as AI operators. Little attention was paid in the legislative acts themselves to enforcement cooperation and the key role Data Protection Authorities (‘DPAs’) have whenever natural or legal persons - be them gatekeepers, providers of AI systems, online marketplaces, or public authorities, process personal data covered by EU data protection law.

The EDPB succinctly described the problem in its 2021 Statement on the Data Strategy package:

> ‘While the processing of personal data is central to the activities regulated by the proposals, data protection supervisory authorities are not designated as the main competent authorities. The EDPB recalls that, as far as the protection and free flow of personal data is concerned, Article 16(2) TFEU and Article 8(3) of the EU Charter require that the supervision of the processing of personal data be entrusted to independent data protection authorities’.60

Indeed, both Article 16(2) TFEU and Article 8(3) Charter provide that compliance with the rules related to the fundamental right to the protection of personal data ‘shall be subject to the control of independent authorities’. The two provisions do not specify exactly what authorities, but they are clear that the supervisory authorities enforcing rules related to processing of personal data in the application of this right must be independent. In fact, the independent supervision of the

60 EDPB Statement on the Digital Services Package and Data Strategy, adopted on 18 November 2021, p. 3.
provisions related to processing of personal data is recognized as one of the key elements of the fundamental right to the protection of personal data. Notably, the main EU secondary legislation transposing Article 8 Charter, the GDPR, specifically recognizes DPAs as supervisory authorities for the enforcement of data protection law.

The EDPB also requested in the same 2021 Statement that ‘each of the proposals clearly mentions data protection supervisory authorities among the relevant competent authorities with whom cooperation shall take place’. This message was re-emphasized with some variations in all of the EDPS and EDPB-EDPS Joint Opinions on each of the legislative proposals.

The final version of the legal texts analysed recognises some role for DPAs, with notable variations. For instance, after the Data Act grants each Member State the power to designate one or more competent authorities to be responsible for its application and enforcement, it specifies in Article 37(3) that DPAs ‘shall be responsible for monitoring the application of this Regulation insofar as the protection of personal data is concerned’.

In turn, the DSA does not refer to DPAs in its chapter dedicated to enforcement, despite some of its key provisions relying on concepts defined in the GDPR, such as ‘profiling’, or involving obligations to process personal data, such as making personal data processed by platforms available to researchers. The DSA provides that Member States should designate one or more competent authorities, among which they should appoint a Digital Services Coordinator (‘DSC’). Recital 44, in its last sentence, mentions that ‘for any question requiring an assessment of compliance with [the GDPR], the competent authority for data intermediation services should seek, where relevant, an opinion or decision of the competent supervisory authority established pursuant to [the GDPR]’.

The DSA empowers the European Commission to enforce its rules targeting VLOPs/VLOSEs. A question arises regarding independence of the DSA enforcers. The DSCs ‘must perform their tasks ... in an impartial, transparent and timely manner’. The Act adds that ‘when carrying out their tasks and exercising their powers in accordance with this Regulation, the [DSCs] shall act with complete independence’. This may mean that the authority itself does not have to be an independent authority, but only that it must act with independence when carrying out its tasks under the DSA. This ‘qualified’ independence for national DSCs may be explained by the fact that the European Commission, the executive arm of the EU, is one of the enforcers of the DSA, and thus requiring independence similar to that of DPAs would be asymmetrical. However, creating

---

61 Gonzalez Fuster, G., Study on the essence of the fundamental rights to privacy and to the protection of personal data (EDPS 2021/0932), 2022, p. 33 and 34.
63 Article 49 DSA.
64 Article 50(1) DSA.
65 Article 50(2) DSA.
more confusion, recital 112 provides context on the independence requirement generally for the
competent authorities designated at national level – they should act in complete independence
‘from private and public bodies, without the possibility to seek or receive instructions, including
from the government, and without prejudice to the specific duties to cooperate with other
competent authorities’. Considering the significant role DSA enforcers have in enforcing how
personal data is being processed by online platforms, should they be required to meet the
independence criteria that DPAs have to meet? Or should this conundrum be solved by involving
DPAs formally in DSA’s enforcement process?

The European Commission is also the enforcer of the DMA, one of the laws of the new legislative
package that enshrines legal provisions related to the processing of personal data, including
obligations for gatekeepers to process personal data in specific ways and relying on legally defined
terms in the GDPR, such as ‘consent’. The DMA vaguely refers in a recital to the fact that it is
without prejudice to the GDPR, ‘including its enforcement network, which remains fully applicable
with respect to any claims by data subjects relating to an infringement to their rights under that
Regulation’\(^66\). This wording suggests that DPAs would not have competence over claims made by
data subjects relating to an infringement of the DMA, even where they act as ‘data subjects’, so
therefore in relation to rights concerning processing of their personal data which would be
governed by the GDPR.

Such a solution would be curious, especially following the recent Judgment of the CJEU in the
Bundeskartellamt case. The CJEU was explicit when stating in that case that ‘the examination by
a competition authority of an undertaking’s conduct in the light of the provisions of the GDPR may
entail the risk of divergences between that authority and the supervisory authorities in the
interpretation of that regulation’\(^68\).

The Court established two rules: First, competition authorities that must look into GDPR
compliance in the exercise of their powers ‘are required to consult and cooperate sincerely with
the national supervisory authorities concerned or with the lead supervisory authority, all of which
are then bound, in that context, to observe their respective powers and competences, in such a way
as to ensure that the obligations arising from the GDPR and the objectives of that regulation are
complied with while their effectiveness is safeguarded’\(^69\). Second, competition authorities must
ascertain whether the conduct they are investigating has already been the subject of a decision by

---


\(^{67}\) Recital 37 DMA.

\(^{68}\) Judgement of the Court of Justice of 4 July 2023, Meta Platforms and others (Conditions générales d’utilisation d’un réseau social), C-252/21, ECLI:EU:C:2023:537, paragraph 55.

\(^{69}\) Meta Platforms and others (Conditions générales d’utilisation d’un réseau social), paragraph 54.
a competent DPA or the Court, and if that is the case, it ‘cannot depart from it, although it remains free to draw its own conclusions from the point of view of the application of competition law’\textsuperscript{70}.

Finally, the AI Act does not have a clear role for DPAs either, other than a couple of narrowly defined interventions. For instance, in the case of specific high-risk AI systems used for law enforcement purposes and other three specifically defined types of high-risk systems, Member States must designate as market surveillance authorities DPAs as established by the GDPR or the LED. The EDPS is designated to act as market surveillance authority where Union institutions, agencies and bodies fall within the scope of the AIA\textsuperscript{71}. Additionally, DPAs should be notified of each use of a real-time biometric identification system, together with the relevant market surveillance authority (Article 5 AIA).

Given how the EU legislator ended up building the enforcement edifice\textsuperscript{72} of the new Data Strategy laws, the EDPS had a poignant message at the end of 2023, when the final text of most of the laws analysed here was already settled: ‘one of the biggest challenges ahead for the EU's digital rulebook, in my view, is going to be its enforcement’, and, specifically, ‘ensuring regulatory consistency’\textsuperscript{73}.

This analysis, even if brief, showed that there is a considerable disconnect between the ‘personal data processing’-heavy scope of application of the EU’s new Digital Rulebook, the mission of the DPAs as independent supervisory authorities entrusted with making sure that the fundamental right to the protection of personal data is respected in the EU, and the fairly marginal role DPAs have been specifically granted in the governance and enforcement of these new laws.

6. Conclusion

This chapter showed that data protection law, whose application is triggered whenever ‘personal data’ is ‘processed’, remains the cornerstone of EU’s Digital Rulebook, regardless of whether it is explicitly recognized as such in these new positive laws or not.

First, it briefly looked into the scope of application of the DMA, DSA, DGA, Data Act and AIA and identified clear instances where processing of personal data and the entities engaging in it are being regulated by these new laws, while at the same time triggering the application of the GDPR (Section 2).

\textsuperscript{70} Meta Platforms and others (Conditions générales d’utilisation d’un réseau social), paragraph 56.
\textsuperscript{71} Article 63 AIA – market surveillance and control of AI systems in the Union market, as provisionally numbered in the text adopted by COREPER, see Council Doc. 8115/21, 26 January 2024.
\textsuperscript{72} Or ‘labyrinth’ as it was coined by Hajduk, P., ‘A Walk in the Labyrinth. Evolving EU Regulatory Framework for Secondary Use of Electronic Personal Health Data for Scientific Research’, 18\textsuperscript{th} IFIP Privacy and Identity Management 2023, Sharing (in) a Digital World, Springer, forthcoming 2024.
\textsuperscript{73} Wiewiórowski, W., Brussels Privacy Symposium on the EU Data Strategy, Opening Remarks, 14 November 2023.
The following section (3) showed how several provisions of the Digital Rulebook are capable of directly engaging Article 8 EU Charter, in the light of established CJEU case-law that a legal measure which provides for processing of personal data amounts to an interference with Article 8. There was no assessment made regarding the lawfulness of any of the interference identified, as it sufficed to show for the purposes of this analysis that the right to the protection of personal data is at play in the Data Strategy legal framework.

Section 4 mapped provisions in each of the five laws analysed which established precedence of the GDPR (and sometimes other EU secondary data protection and privacy law), positioning it as the one common denominator cutting through the Digital Rulebook and engaging all of the new legal frameworks in various ways.

Finally, the last section (5) briefly discussed the enforcement architecture built by the EU legislator, observing that despite the significant role that processing of personal data has in the substance and material scope of the new digital rulebook, and despite the clear engagement with Article 8 Charter discussed earlier, DPAs do not have a well established role in the enforcement or governance of the EU’s Digital Rulebook.

The journey through these arguments and analysis was accompanied by Opinions and Statements published in the past four years by the EDPS, sometimes jointly with the EDPB, analysing these legislative proposals and clearly showing areas of tension with existing legal frameworks and their enforcement.

These areas of tension indicate challenges ahead in the implementation of EU’s new Digital Rulebook. Such challenges can be overcome by coherent policymaking and governance, which could start by recognizing the central role data protection law has in the digital regulatory space, especially through the lens of Article 8 EU Charter. This would be translated into consistent involvement of DPAs and the existing data protection ‘infrastructure’ permeating all public sector and all industries after the adoption of the GDPR, the LED and the EUDPR, such as Data Protection Officers, in the coherent interpretation and application of the new rules. The opportunities brought by the new legislative package could thus be easier to grasp.