EuZ
ZEITSCHRIFT FÜR EUROPARECHT

AUSGABE:
03 | 2024

LEITARTIKEL:

Chayanis Aueamnuay / Carmen Berjón / Stella Galehr / Luca Graf / Andreas Heinemann
Digital Regulation in the European Union

Digital Regulation in the European Union

Chayanis Aueamnuay/Carmen Berjón/Stella Galehr/Luca Graf/
Andreas Heinemann*

Content

* Chayanis Aueamnuay, MLaw, Carmen Berjón, MLaw, Stella Galehr, MLaw and LLM (UC Berkeley), and Luca Graf, MLaw and LLM (King's College London), are predoctoral assistants at the Chair of Commercial, Economic and European Law of Prof. Dr. Andreas Heinemann, University of Zurich, Faculty of Law.

A. Introduction

Walter Hallstein, the first president of the European Commission (serving from 1958 to 1967), called the Commission the "motor" of European integration. Ever since, the presidents of the European Commission have tried to react to the challenges of their time by adopting ambitious programs that were intended to solve the problems of the present and shape the future. One milestone was the Delors Commission's goal of achieving the single market by the end of 1992. In a similar vein, the Juncker Commission defined the goal of creating a "Digital Single Market" in 2015. This was based on the finding that very few consumers were shopping online in other Member States at the time, and that small and medium enterprises were not seizing the digital opportunities either. The regulatory hurdles were to be torn down by a series of measures, e.g. by the abolition of roaming charges ("roam like at home"), simple cross-border contract rules for consumers and businesses, easier cross-border parcel delivery, the prevention of unjustified geo-blocking

and the cross-border portability of online content services. Moreover, under the Juncker Commission, the General Data Protection Regulation (GDPR)[1] was passed.

The von der Leyen Commission (2019-2024) is building on the work of its predecessors. It has commemorated the 30th birthday of the single market in 2023 and has made further work on a digital single market one of its six priorities. So, alongside the "European Green Deal" for example, "A Europe fit for the Digital Age" has launched a "Digital Decade" that is supposed to implement concrete targets and objectives by 2030. Nothing less is intended than a digital transformation that will extend far beyond the economic sphere. The basic text is the "European Declaration on Digital Rights and Principles for the Digital Decade", a joint declaration by the European Parliament, the Council and the European Commission, that connects the digital transformation to the European Union (EU)'s core values such as human dignity, freedom, equality and solidarity (Recital 1 of the Preamble). The declaration is more symbolic than legal since it has a "declaratory nature" and therefore "does not affect the content of legal rules or their application" (Recital 10 of the Preamble).[2] However, the declaration clarifies the significance of the general legal provisions for digital environments and places them in a general context. For example, the text vividly articulates: "What is illegal offline, is illegal online" (Recital 3 of the Preamble). And as far as the foundations of the economic system and the Internet are concerned, the declaration states that "everyone should have the possibility to compete fairly and innovate in the digital environment" (no. 11) and advocates "a neutral and open Internet where content, services, and applications are not unjustifiably blocked or degraded" (no. 3 b of the Declaration).

The different European strategies in the field of the digital economy are not easy to disentangle. Many initiatives overlap since a new Commission regularly has the ambition to add a new layer without necessarily discontinuing older projects. Therefore, the Digital Agenda for Europe from 2010, the "Digital Single Market" strategy from 2015, the "second Digital Agenda for Europe" from 2020 composed of the strategic communications "Shaping Europe's Digital Future" and "Europe's Digital Decade" are the expression of an increas-

---

1 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 May 2016, 1–88.

2 Therefore, the European Declaration on Digital Rights has been published in the "C" series of the EU Official Journal, not in "L", see OJ 2023, 23 January 2023, C 23/1.

ingly pronounced digital strategy, which also has an international background. Digital Sovereignty shall be strengthened, and the EU wants to set its own standards, rather than following those of others.

The aim of this article is to provide an overview of the complex field of digital regulation in the EU by presenting the most important legislative texts. As dozens of measures are planned, a choice has to be made. In accordance with the European Commission's "clear focus on data, technology, and infrastructure"[3], the Digital Markets Act (DMA) is placed at the beginning since its rules for gatekeepers and core platform services are essential for the entire architecture of the Internet and fair and open markets. While only a small number of very large Internet platforms are subject to this regulation, the Digital Services Act (DSA) contains rules for all providers of intermediary, hosting or platform services, whether they are large or small, with the intensity of regulation depending on their size. The DSA aims to prevent illegal activities and disinformation online and to effectively protect fundamental rights. As data is key to the digital economy, the European Commission has adopted a European Data Strategy that extends the single market objective to data. Several legislative acts are part of this strategy, for example the Data Act (DA) that provides rules on data sharing with respect to product data and related service data, the Data Governance Act (DGA) that aims to make more data available by promoting the development of trustworthy data-sharing systems, and the European Health Data Space (EHDS), that creates the first common EU data space for a specific sector. Finally, with respect to technology, the Artificial Intelligence Act (AI Act) will be portrayed. The AI Act would be a world first and has the potential to set a global standard for a technology with disruptive potential.

B. Digital Markets Act (DMA)

I. Context

The digital revolution has considerably stimulated competition by facilitating market access, accelerating transactions, expanding markets geographically and increasing the pressure to innovate to new dimensions. On the other hand, important economies of scale and scope, the ability to intermediate between different user groups, strong network effects, vertical integration as well as the control of large amounts of data and of intellectual property rights

[3] <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en>.

have led to lock-in effects and to considerable economic power.[4] As this power has not always been used responsibly, competition authorities have come into play. In Europe, the Google cases should be mentioned, especially *Google Shopping*[5] and *Google Android*[6]. However, the application of competition law (in particular Art. 102 TFEU) to these cases is complicated: Relevant markets have to be defined, dominance has to be proven and abusive behaviour has to be shown. It is not helpful that recent case law has created ambiguities regarding the correct application of Art. 102 TFEU, in particular with respect to the necessity of an *as efficient competitor* test (AEC test).[7] Moreover, the duration of procedures in Art. 102 TFEU cases has become unacceptable and stands in contrast to the dynamics of the digital economy.[8]

Against this background, it is not surprising that the European Commission has chosen a different path to solve the competition problems posed by the large Internet platforms. The result is the Digital Markets Act (DMA) which

---

4 See the economic analysis of the platform economy in 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 (Digital Markets Act), OJ L 265, 12 October 2022, 1–66, Recital 2.

5 EC, Commission Decision of 27 June 2017, Case AT.39740 – Google Search (*Shopping*); largely confirmed by the General Court: GC, Judgement of the General Court of 10 November 2021, Case T-612/17, ECLI:EU:T:2021:763 – Google and Alphabet/Commission (*Google Shopping*); an appeal is pending before the European Court of Justice under case number C-48/22 P; see the opinion of Advocate General Kokott of 11 January 2024, Case C-48/22 P, ECLI:EU:C:2024:14.

6 EC, Commission Decision of 18 July 2018, Case AT.40099 – Google Android; largely confirmed by the General Court: GC, Judgement of the General Court of 14 September 2022, Case T-604/18, ECLI:EU:T:2022:541 – Google and Alphabet/Commission (*Google Android*); an appeal is pending before the European Court of Justice under case number C-738/22 P.

7 See for example Di Giovanni Bezzi Raffaele, Anticompetitive Effects and Allocation of the Burden of Proof in Article 102 Cases: Lessons from the Google Shopping Case, JECLAP 2022, 112-124, 112; Heinemann Andreas, Comment on European Court of Justice, Lietuvos geležinkeliai AB/European Commission, EuZW 2023, 285-292, 292; regarding the future of the AEC test in the Guidelines on exclusionary abuses announced by the European Commission see Neven Damien J, The As-Efficient Competitor Test and Principle. What Role in the Proposed Guidelines?, JECLAP 2023, 565-581, 565.

8 See for example the *Intel* case on the question of fidelity rebates that began with the complaint of the main competitor AMD in 2000 and is still not over, but pending a second time before the European Court of Justice (C-240/22 P); see the opinion of Advocate General Medina of 18 January 2024, Case C-240/22 P, ECLI:EU:C:2024:65. The procedure is further complicated by the fact that the Commission has since taken a new decision regarding the "naked restrictions" part of the case, which in turn has been challenged and is pending before the General Court (case T-1129/23).

was adopted in 2022 and became applicable on 2 May 2023.[9] The DMA is a new form of *ex ante* regulation for platform companies that control access to the Internet as gatekeepers. The new rules are not competition law in the proper sense, but are based on the internal market competence (Art. 114 TFEU). Contrary to traditional competition law, the DMA does not require an individual assessment of market positions or of the behaviour in question on a case by case basis and does not admit an efficiency defence or other objective justifications.[10] The hope is that this will speed up procedures considerably and maintain competition in the platform economy.

II. Content

On the one hand, the DMA defines the concept of "core platform services" and "gatekeepers", i.e. the conditions under which a firm falls within the scope of the DMA (1.). On the other hand, the rules are specified to which designated gatekeepers are subject (2.).

1. Core Platform Services and Gatekeepers

Only firms that run a "core platform service" are potential gatekeepers. Art. 2(2) DMA contains a list that exhaustively enumerates such core platform services, e.g. online intermediation services, online search engines, online social networking services, video-sharing platform services, operating systems and web browsers. According to Art. 3 DMA, however, a platform service provider in this sense can only be deemed a gatekeeper if it has a significant impact on the internal market (e.g. annual EU turnover ≥ EUR 7.5 billion Euro or market capitalization ≥ EUR 75 billion), if its core platform service is an important gateway for business users to reach end users (e.g. ≥ 45 million monthly active end users in the EU and ≥ 10 000 yearly active business users in the EU), and if it enjoys an entrenched and durable position (e.g. if the thresholds mentioned were met in each of the last three years). The presumptions triggered by the thresholds can be rebutted; on the other hand, one can also be declared a gatekeeper below the thresholds.

---

9 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 (Digital Markets Act), OJ L 265/1.

10 Cf. Recitals 5 and 10 Regulation (EU) 2022/1925.

The designation as gatekeeper is constitutive. In September 2023, the European Commission designated six gatekeepers with a total of 22 core platform services.[11] These are the five companies traditionally known as GAFAM plus the Chinese company ByteDance that runs the video hosting service TikTok. As two of the major technology companies have meanwhile changed their names, the new abbreviation MAMBAA is suggested here.[12]

2. Substantive Rules

Designated gatekeepers have to comply with the DMA obligations for each of the designated core platform services. The catalogues of dos and don'ts in articles 5 to 7 form the nucleus of the DMA. They have been inspired by competition law cases,[13] but through the transformation into platform law they have gained autonomy. For example, gatekeepers must not combine personal data from a core platform service with any other data from the gatekeeper or third parties ("data silos"), prevent consumers from accessing businesses outside the gatekeeper's platform or do "self-preferencing", i.e. rank more favourably its own services compared to products of a third-party. Moreover, gatekeepers are obliged to inform advertisers and publishers in a timely manner about the details and calculation of prices and fees, to enable end users to un-install any software applications on the operating system of the gatekeeper, to allow third parties to inter-operate with the gatekeeper's services as well as to provide business users access to the data they generate and to grant end users effective portability of data.

III. Assessment

The DMA constitutes an innovative approach to tackle the concentration of power in digital markets. While it is impossible to eliminate the strong economic forces of centralization such as economies of scale, network effects and control of big data, it is feasible to ensure that as much competition as possible is maintained in the markets neighbouring the gatekeepers' central platform services. The DMA is a response to shortcomings in the application

---

11 <https://digital-markets-act.ec.europa.eu/commission-designates-six-gatekeepers-under-digital-markets-act-2023-09-06_en>. Several appeals are pending before the General Court regarding the designation as gatekeeper or as a core platform service or the opening of a market investigation under the DMA, see pending cases T-1077/23, T-1078/23, T-1079/23, T-1080/23.

12 MAMBAA: Meta, Alphabet, Microsoft, ByteDance, Amazon and Apple.

13 See Caffarra Cristina/Scott Morton Fiona, The Digital Markets Act: A Translation, World Commerce Review, Spring 2021.

of traditional competition law. The procedures have become too slow, which is partly due to an incomplete economic approach that only takes into account the substantive law, but not the costs and duration of the procedure. The DMA takes an extreme swing in the opposite direction. Based on a "more legal approach", the terms of gatekeeper and core platform services are defined in a formal manner, with great weight being given to presumptions, and lists of specific obligations and prohibitions are established. Neither relevant markets are to be defined, nor is an efficiency justification permitted. This is intended to avoid the lengthy disputes of classical competition law.

The question can be asked if the DMA would have been necessary if traditional competition law had been applied more effectively in the past. But perhaps even then, given the strong concentration tendencies in the digital economy, it would have been necessary to install a special mechanism to protect competition. Against this backdrop, the regulatory innovation introduced by the DMA should be viewed positively.

IV. Outlook

As the official title of the DMA indicates, its goal is to keep the digital sector contestable and fair. As the DMA itself emphasises, this task is enormous since some of the high-tech companies "exercise control over whole platform ecosystems in the digital economy and are structurally extremely difficult to challenge or contest" (Recital 3 DMA). It remains to be seen if the DMA will be up to its ambitions. In any case, the first steps are encouraging: The European Commission has designated the first gatekeepers and core platform services. Much will now depend on whether the application of the new rules will be as effective as planned. Will the designated gatekeepers comply voluntarily, or will lengthy proceedings arise which is what the new type of ex ante regulation was supposed to avoid? As the DMA covers a wide range of business strategies, there will certainly be turbulent developments here.

C. Digital Services Act (DSA)

I. Context

A landmark new set of EU rules for a safer and more responsible online environment has been launched with the entry into force of the DSA[14], which came into full effect for all regulated entities on 17 February 2024.[15] The aim of the DSA is to improve the governance of digital services and markets in the EU by setting out harmonised rules for a safe, predictable and trusted online environment for consumers in the use of online platforms and digital services. These harmonised rules should create a level playing field for the digital economy in the EU, while facilitating innovation and competition in the internal market and effectively protecting fundamental rights.[16] Ultimately, this regulation is about responding to the need to regulate the digital space arising from digital transformation and the increased use of intermediary services.[17] It is for this reason that some have justifiably referred to the DSA as a *European constitution for the Internet*.[18] As a result, the EU, bestowed with the legislative function, is being described as *the Global Regulator of the Internet*.[19]

With the application of the DSA, a wide range of online intermediaries and platforms, including marketplaces, social networks, content sharing platforms, app stores and online travel and accommodation platforms that provide intermediary services, will be subject to due diligence obligations to combat illegal content, online disinformation or other societal risks.[20] The DSA creates comprehensive new obligations for digital services that connect consumers to goods, services or content, without being sector-specific. In other words, the DSA is a piece of regulation with a horizontal effect.[21]

---

14 Regulation (EU) 2022/2065 of The European Parliament and of The Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27 October 2022, 1–102.

15 Art. 93 para 2 Regulation (EU) 2022/2065.

16 Art. 1 para 1 Regulation (EU) 2022/2065.

17 Recital 1 Regulation (EU) 2022/2065.

18 See <https://europe-calling.de/en/europe-calling-dsa-deal/>.

19 See Tourkochoriti Ioanna, The Digital Services Act and the EU as the Global Regulator of the Internet, Chicago Journal of International Law, Vol. 24, No. 1, 2023, 129.

20 <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en>.

21 Steinrötter Björn, Digital Services Act, in: Steinrötter Björn (ed.), Europäische Plattformregulierung DSA | DMA | P2B-VO | DGA | DA | AI Act | DSM-RL: Rechtshandbuch, Baden-Baden 2023, 24.

II. Content

1. Subject matter and scope

To achieve its objectives of empowering and protecting users, preventing the dissemination of illegal content, and increasing transparency and accountability online, the DSA classifies online service providers into different categories. Each of these categories contains a set of specific obligations that online service providers must comply with. Given the nature of online services, which operate in a borderless world, the DSA applies the principle of substantial connection.[22] As a result, online service providers offering their services in the European Single Market are subject to the DSA, regardless of where they are established.[23]

2. Which providers of online services are covered?

The DSA categorises providers of intermediary services according to their role, size and the impact of their services in the online ecosystem. These categories include intermediary services, hosting services, online platforms and very large online platforms and very large online search engines (often referred to as "VLOPs and VLOSEs" for service providers reaching an average of 45 million or more online recipients in Europe[24] – equivalent to 10% of the EU population[25]). The European Commission has currently designated 20 VLOPs and 2 VLOSEs.[26] As the name suggests, service providers falling within the scope of VLOPs and VLOSEs must comply with additional rules because they are considered to pose a particular risk of spreading illegal content and causing social harm.[27]

---

22 Art. 3 point (e) Regulation (EU) 2022/2065.

23 Art. 2 para 1 in conjunction with the definition provided for in Art. 3 point (d) Regulation (EU) 2022/2065.

24 Art. 33 para 1 Regulation (EU) 2022/2065.

25 Recital 76 Regulation (EU) 2022/2065.

26 The list of designated VLOPs and VLSEs as of 1 March 2024 is available on <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>.

27 <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en>.

3. Obligations for providers of intermediary services

All providers of intermediary services falling within the scope of the DSA are required to comply with the general obligations laid down in Art. 4 to 15. While Art. 16 to 18 lay down further obligations for a broader category of providers of hosting services, Art. 19 to 32 lay down additional requirements for online platforms – classified as a subcategory of hosting services – such as social networks. The additional obligations relate to the fact that online platforms not only store users' information, but also make this information available to the public as a main feature of the services they offer.[28] Although providers of intermediary services do not have a general duty of monitoring or active investigation to identify the illegal content that they transmit or store,[29] they do have a general duty to remove or disable access to such content once they become aware of its illegality.

As regards VLOPs and VLOSEs, additional obligations beyond those set out in the aforementioned Articles are contained in Art. 33 to 48. These obligations, which focus on enhancing users' rights and protecting users engaged in online services, required VLOPs and VLOSEs, for example, to assess the impact and risks of their services on critical issues. These risks include, for example, negative impacts on electoral processes, public security, users' physical and mental well-being, and fundamental rights such as freedom of expression and non-discrimination.[30] To mitigate these risks, VLOPs and VLOSEs need to take appropriate measures, such as adapting their content moderation tools to address the identified risks, or incorporating age verification and parental control tools in their services to protect children's rights when the users concerned are minors.[31]

III. Assessment

As Margrethe Vestager – Executive Vice-President of the European Commission – emphasised in an interview when asked what consumer organizations and users of digital services wanted to see in this legislation – "what is illegal in the real world [will] also [be] seen and treated as illegal in our online world".[32] It seems fair to say that the DSA serves this purpose and improves the governance of digital services and online markets. Through the designation of

---

28 Recital 13 Regulation (EU) 2022/2065.

29 Art. 8 Regulation (EU) 2022/2065.

30 Art. 34 Regulation (EU) 2022/2065.

31 Art. 35 Regulation (EU) 2022/2065.

32 <https://audiovisual.ec.europa.eu/en/video/I-239322>.

national Digital Services Coordinators, Member States will now be equipped with a full range of powers to monitor illegal content and goods in the digital world on an ongoing basis and to enforce this Regulation.[33] For major players, designated as VLOPs and VLOSEs, the DSA grants the European Commission both supervisory and sanction powers.

Failure to comply with an obligation set out in the DSA could result in a fine of up to 6% of the annual global turnover of the provider of intermediary service concerned.[34] The possibility of being subject to this substantial financial penalty will undoubtedly put providers of intermediary services on notice that any company that fails to comply diligently with the obligations imposed by the DSA may now face greater legal and financial risks.

IV. Outlook

Following the establishment of the DSA framework, which harmonises the conditions for the provision of intermediary services within the EU, the next challenge will undoubtedly be the effectiveness of its application. The principle of substantial connection embedded in the DSA, which makes its rules applicable to digital service providers regardless of their place of establishment or location, implies that its effects will be felt beyond the territories of the EU Member States and will have a global impact. Such a phenomenon is characterised as the "Brussels Effect".[35]

In the context of the DSA, the Brussels effect has already raised some concerns in the United States, where many major players in digital services and online platforms are based. One of the concerns expressed is that the DSA's goal of combating illegal content or online disinformation may come at the expense of restricting freedom of expression due to the imperfection of the relevant detection technologies used to distinguish legal from illegal content.[36] There is also a possibility that the application of the rules under the DSA could lead to conflicts with American laws due to the diverging views of the two regimes on the regulation and protection of freedom of expression or speech.[37] In either case, content moderation will inevitably become a challenge for online platforms that have their place of operation or substantial connection in both the EU and the United States.

---

33 Art. 49 Regulation (EU) 2022/2065.

34 Art. 52 para 3 Regulation (EU) 2022/2065.

35 Bradford Anu, The Brussels Effect, Nw. U. L. Rev., Vol. 107(1) 2012, 19–22.

36 Tourkochoriti, 138-144.

37 See Nunziato Dawn Carla, The Digital Services Act and the Brussels Effect on Platform Content Moderation, Chicago Journal of International Law: Vol. 24: No. 1, Article 6, 115-128.

D. Data Act (DA)

I. Context

The DA focuses on a specific type of data: Data that is generated, collected or stored by companies through the use of products or services. While focused on a specific type of data, the act carries vast implications as its scope covers a large part of the data economy. Until the DA, manufacturing companies either exclusively held and developed this data, or it remained dormant, unused for innovation. The DA changes this landscape, allowing both companies and users to utilise user data. This shift has dual implications: Firstly, it breathes new life into existing data, fostering economic value through innovative uses. Secondly, it empowers users to understand the data they generate, enabling them to make informed decisions about its use.

The DA already entered into force on 11 January 2024 and will become applicable 20 months later, i.e. on 11 September 2025.

II. Content

The DA focuses on access to data throughout sectors and industries, and in particular on the relationship between different actors. The underlying premise is that the potential of data can only be fully harnessed if access to and the use of data, as well as the value derived from it, is fairly allocated and not restricted to a few companies.[38] In a nutshell: The DA stipulates what fair access to, and the use of product or device generated data should look like, by determining who may access, which data in the data economy and under what conditions.

1. Notions

The definition of 'data' is very broad and captures "any digital representation of acts, facts or information and any compilation" of the three concepts. A 'product' under the DA is any item with the ability to generate "data concerning its use or environment, and that is able to communicate [that] data", e.g., via an Internet connection or a nearby telephone networks. Broadly speaking, the DA therefore applies to Internet of Things (IoT) devices, such as fitness tracker

[38] Cf. Recital 2 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 December 2023.

devices, smart home technologies, such as fridges, to production machinery, car data, and so on. Importantly, the DA's scope excludes products whose primary function is data storage or processing, such as, Cloud services. The 'user' can be a natural or a legal person. Therefore, the DA applies to both, B2B and B2C relationships. The 'data holder' is the legal or natural person, who has the right, or in some cases the obligation, to make the data available to 'data recipients', legal or natural persons other than the users, for commercial purposes.[39]

2. Data access

The DA mandates manufacturers to provide users *by default* with direct access to data generated by their products. Additionally, users must be informed, upon contract conclusion, about the types of data likely to be generated, how to access them, and about any intentions to share data with third parties.[40] In cases where data are not directly accessible through the product, users should have the ability to request this data through a simple process. Manufacturers must provide the requested data without undue delay, without charge, and, where relevant, in real-time.[41] Users can also enable third parties to request data. Again, the request must be addressed without undue delay, free of charge to the user, in real-time, and the data must be of the same quality as is available to the data holder.[42] The third party may be a data intermediary (as provided for in the DGA) and in this capacity facilitate sharing.[43] However, where data holders make data available in a B2B relationship, the data holder may ask for reasonable compensation and must comply with FRAND (fair, reasonable, and non-discriminatory) terms.[44] In order to further prevent unfair contractual

---

39 Art. 2 paras 1, 2, 5, 6, 7 Regulation (EU) 2023/2854.

40 Art. 3 paras 1, 2 Regulation (EU) 2023/2854.

41 Art. 4 para 1 Regulation (EU) 2023/2854; on the possible configuration of "data accessibility by default", see Mendelsohn Juliane/Richter Philipp, § 20 Plattformspezifische Vorgaben des Data Acts, in: Steinrötter Björn, Europäische Plattformregulierung, Baden-Baden 2023, para 21.

42 Art. 5 para 1 Regulation (EU) 2023/2854.

43 See part E. Data Governance Act.

44 See Art. 8 para 1 Regulation (EU) 2023/2854; some perceive the high transaction costs that come with the need to negotiate a contract with FRAND conditions as an obstacle to fulfilling the DA's objectives, see Kerber Wolfgang, Governance of IoT Data: Why the EU Data Act Will not Fulfill its Objectives, GRUR International 2023, 123.

terms in data sharing agreements, the DA restricts the terms one party can unilaterally impose in an order to strengthen the weaker party's negotiating position.[45]

3. Important exemptions

Entities designated as gatekeepers under the DMA[46] are not an eligible third party to request data.[47] Considering the significant economic influence wielded by gatekeepers, it would be disproportionate in relation to the data holders to subject them to access obligations and have gatekeepers as its beneficiaries.[48] Further there exists an additional limitation, whereby a third party is prohibited from exploiting its rights under the DA to gain a competitive advantage in markets where the data holder and the third party may be competing directly.[49] The sharing obligations also do not apply to micro, small and medium-sized enterprises.[50]

4. Enforcement

The enforcement of the DA lies within competent authorities in the Member States.[51] If a natural or legal person finds that their rights have been violated, they may lodge a complaint with the competent authority. When it comes to enforcing the DA regarding personal data, the responsibility remains with the Data Protection Authorities.[52]

III. Assessment

The DA addresses a critical concern whereby manufacturers have historically maintained de facto exclusive control over generated data, depriving users and other stakeholders of potential benefits. This disparity is particularly pronounced considering existing interoperability provisions primarily focused

---

45 Recital 58 et seq., Art. 13 et seq. Regulation (EU) 2023/2854; discussed also in more detail by Graf von Westphalen Friedrich, Das Datengesetz und seine umfassende AGB-Kontrolle für KMUs, EuZW 2023, 1121 et seq.

46 See part. B Digital Markets Act.

47 Art. 5 para 2 Regulation (EU) 2023/2854.

48 Recital 40 Regulation (EU) 2023/2854; some fear that gatekeepers could nonetheless access IoT data streams through backdoors, see Kerber, 130.

49 Recital 32 Regulation (EU) 2023/2854.

50 Art. 7 Regulation (EU) 2023/2854.

51 Art. 31 para 1 Regulation (EU) 2023/2854.

52 Art. 3 para 2 point h in combination with Art. 31 para 3 point b Regulation (EU) 2023/2854.

on personal data, which are now extending to encompass broader data sets. The underlying rationale is to mitigate network effects and reintroduce competitive dynamics into digital markets.[53]

Additionally, the DA provides notable exemptions for micro, small, and medium-sized enterprises, as well as gatekeepers, to accommodate differences in size as well as protect trade secrets. However, a concern arises regarding the potential breadth of these exemptions, which could hinder the act's objectives. Specifically, there is uncertainty about how trade secrets are protected under these exemptions, potentially leading to the withholding of certain data. Determining ex-ante whether a claim of trade secret protection is legitimate or veiled protectionism poses a challenge.[54]

It is essential to recognise that the DA does not supersede the GDPR. In cases involving personal data, provisions of the GDPR apply and require a lawful basis for processing. The DA itself does not constitute a lawful basis in this context.

IV. Outlook

Given the scope of the DA across various sectors and stakeholder levels, significant impacts are anticipated for both users and companies. Users are likely to have heightened awareness regarding the types of data generated by their behaviours, potentially leading to more informed utilization of this information. For instance, users may leverage data insights to explore cheaper alternatives in product aftermarkets, such as seeking out repair services. The extent to which different market sectors capitalise on these opportunities remains to be observed. As mentioned above, the DA will become applicable on 11 September 2025. The timing of the DA's implementation also aligns with the growing number of Artificial Intelligence (AI) applications. With the concurrent enforcement of the AI Act, there is a clear imperative for the availability and quality of data to feed and steer AI applications.

---

53 Some criticise that the right to data portability under Art. 20 GDPR failed to achieve its goals and are skeptical as to why the mechanism of the Data Protection Act should work better, see Kerber 125 et seq.

54 See Kerber, 126.

E. Data Governance Act (DGA)

I. Context

The DGA, as the name suggests, establishes a governance framework for the handling and sharing of data. The DGA is thus closely linked to the DA, as it creates processes and structures for the sharing of data between companies, individuals, and the public sector. By fostering trust in data sharing and strengthening available mechanisms, the DGA aims to increase the availability of data. Increased availability and quality of data shall consequently lead to more innovation and overall improved data use. So, while the DA sets out if and what data must be made accessible, the DGA stipulates *how* data can be shared.[55] The DGA has entered into force on 23 June 2022 and became applicable from 24 September 2023.

II. Content

The DGA contains three key topics that will be further discussed: the reuse of certain categories of public sector data, data intermediation services, and so-called data altruism.

1. Data held by public sector bodies

The DGA encourages the reuse of data held by public bodies, which safeguard such data for reasons such as commercial or statistical confidentiality, protection of intellectual property rights, and data protection rights.[56] Public sector bodies include institutions such as public libraries, archives, museums, theatres and public broadcasting services.[57] Some data, such as data stored by public companies, as well as data stored for reasons of public security, defence or national security, do not fall within the scope of application.[58]

The DGA restricts exclusive use agreements to ensure that data is shared as freely as possible.[59] To increase transparency, public sector bodies must share the terms for reuse and those terms must be fair, transparent and

---

55 See Schreiber Kristina et al, Das neue Recht der Daten-Governance, Baden-Baden 2023, 40.

56 Art. 3 para 1 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), OJ L 152, 3 June 2022, 1–44.

57 See Specht-Riemenschneider, Artikel 2, in: Specht Louisa/Hennemann Moritz (eds), Handkommentar zum Data Governance Act, para 147.

58 Art. 2 para 2 Regulation (EU) 2018/1724.

59 Art. 4 Regulation (EU) 2018/1724.

proportionate. The information must be shared via a "single information point" set up in each Member State, where also the permission for reuse of the data may be requested.[60] Essentially, this is intended to streamline and simplify access to data held by public sector bodies. These organisations have the discretion to impose fees for permitting the reuse of data. However, to incentivise reuse for non-commercial purposes and reuse by SMEs and start-ups, public bodies may provide data to these companies at a reduced price or even free of charge.[61]

It is important to mention that the DGA does not create any obligation for public sector bodies to share data, it merely sets up and harmonises the conditions under which they can do so.[62] The Member States continue to decide which data should be made available, to what extent and for what purposes.

2. Data intermediaries

The DGA regulates data intermediation services and sets out the ground rules for their operation. Data intermediaries are services that aim to establish business relationships involving the sharing of data, between data subjects and data holders on the one hand, and data users on the other. The act includes services that enable data subjects to exercise their data protection rights.[63] In order to become a data intermediary, the entity must meet certain requirements and must be registered with the competent authorities.[64] Intermediaries must not use the data for purposes other than putting them at disposal for data users. They must further ensure that access to their service is fair, transparent, and non-discriminatory for data subjects, data holders, and data users.[65] Data intermediaries shall operate as reliable coordinators of data sharing within the EU, providing a level playing field for all parties involved.[66]

Each Member State designates a competent authority responsible for the supervision and monitoring of data intermediary services. If a competent authority confirms that an intermediary service meets the requirements, that

---

60 Art. 5 paras 1, 2 Regulation (EU) 2018/1724.

61 Art. 6 paras 1, 4 Regulation (EU) 2018/1724.

62 Art. 1 para 2 Regulation (EU) 2018/1724.

63 Art. 2 para 11 Regulation (EU) 2018/1724.

64 Art. 11 para 1 Regulation (EU) 2018/1724.

65 Art. 12 lit a, f Regulation (EU) 2018/1724.

66 For an overview of different types of data intermediaries, see Carovano Gabriele/Finck Michele, Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy, CLSR 2023, 4.

service may use the designation "data intermediation services provider recognized in the Union" and the corresponding logo. This ensures that intermediaries are easily recognizable throughout the EU and benefit from the trust that the strict regulation is intended to create.

3. Data altruism

The third concept introduced by the DGA is data altruism. As the name suggests, it aims to promote the use of data for altruistic purposes. Data altruism describes the voluntary sharing of non-personal data by a data subject on the basis of consent, making data available to further objectives of general interest, such as projects related to healthcare, combating climate change, or for scientific purposes.[67] In order for people to "donate" their data, a culture of trust must be created and it must be ensured that the data is used for the stated purposes.[68] For this reason, like data intermediation services, organizations that fulfill the requirements laid down under the DGA, can – voluntarily – register with the competent authorities and carry the label "EU recognized Data Altruism Organisation" together with the corresponding logo.

4. European Data Innovation Board (EDIB)

To effectively implement the DGA, a new export group is formed: the European Data Innovation Board. The board is composed of representatives from competent authorities, representatives of the European Data Protection Board, relevant EU agencies such as the EU Agency for Cybersecurity (ENISA), as well as other stakeholders, e.g., relevant industry representatives, academics and civil society.[69] The EDIB is tasked to coordinate national practices and strategies and provide support and advice to the Commission.

5. Restriction of international data transfers

The DGA establishes a regime for international transfers of non-personal data. The aim is to protect publicly held data that is being reused from foreign governmental access as well as to protect trade secrets and prevent infringements of intellectual property rights or industrial espionage.[70] Appropriate

---

67 Art. 2 para 16 Regulation (EU) 2018/1724.

68 It remains to be seen whether there is such an advantage or whether the bureaucratic effort is too great to obtain the certification, see also HK DGA-Specht-Riemenschneider, Artikel 11, para 18.

69 Art. 29 Regulation (EU) 2018/1724.

70 Recital 20 Regulation (EU) 2018/1724.

safeguards including technical, legal and organizational, must therefore be taken for transfers that could conflict with EU law or national law of a Member State.[71] In contrast to the known mechanism under the GDPR, not all transfers underlie this regime, but only those that create a potential conflict of law.[72] The Commission will provide for model standard contractual clauses or can adopt an adequacy decision if the level of protection is essentially equivalent to that of the EU. The need for implementing an adequacy decision will be identified by the introduced European Data Innovation Board.[73]

III. Assessment

One important aspect of the DGA is that it will lead to increased awareness regarding data value. This can empower individuals and also SMEs to take a more active role in the data economy, by sharing and accessing data. This helps leveraging the full potential of data that is currently unused. The DGA provides for strict regulation of data intermediaries, which is aimed at fostering trust in data sharing. However, some question whether the DGA thereby truly enables data sharing or restricts it even further by imposing too many rules,[74] and whether its means contradict with its ends.[75]

Additionally, as with the DA, the DGA is not creating a legal basis for the processing of personal data and explicitly states the parallel application of the GDPR.[76] On the one hand, this ensures that the protection of personal data of data subjects is not undermined. On the other hand, remaining data protection hurdles and a lack of legal certainty with regards to the GDPR application may hinder the full potential of data sharing.[77] Another critical aspect to consider is the system established for international transfers, which mirrors the structure of the GDPR. The implementation of the GDPR in this regard has brought about numerous challenges, particularly concerning data transfers to jurisdictions with disproportionate government access. Despite the abundance of paperwork, doubts persist whether the mechanism is suitable to safeguard data.

---

71 Art. 31 para 1 Regulation (EU) 2018/1724.

72 See HK DGA-Specht-Riemenschneider, Artikel 31, para 12.

73 Cf. Recital 21 Regulation (EU) 2018/1724.

74 See von Ditfurth Lukas/Lienemann Gregor, The Data Governance Act – Promoting or Restricting Data Intermediaries? CRNI 2022, 270-295.

75 See Carovano/Finck, 1.

76 Art. 1 para 3 Regulation (EU) 2018/1724.

77 See Savary Fiona, § 19 Plattformspezifische Vorgaben des Data Governance Acts, in: Steinrötter Björn, Europäische Plattformregulierung, Baden-Baden 2023, para 17; also von Ditfurth /Lienemann, 287.

The DGA also applies without prejudice to applicable competition law.[78] Therefore, while the DGA aims to foster collaboration around data use, it is crucial for entities to ensure that, while making use of new opportunities, they comply with competition law.[79]

IV. Outlook

As of the writing of this article, the DGA has only been applicable for a few months, and there has been limited observable impact. A single data intermediary is listed on the Commission's website,[80] and no altruistic organizations thus far.[81] However, it is important to recognise that realising the long-term benefits of the setup of the DGA may require time, particularly as it is closely intertwined with other upcoming EU texts, such as the DA.[82]

F. European Health Data Space (EHDS)

I. Context – The EHDS: Crafting a Path for Electronic Health Data

Everybody wants it – no one has it (yet). The access to a Europe-wide pool of electronic health data. While the ambitions in this area are high, given the enormous potential that lies in the use of health data, the current barriers are even higher. However, while Switzerland is entangled in endless discussions regarding the secondary use of data, the EU took some actual steps towards the creation of a European Health Data Space (EHDS).[83] In May 2022 the European Commission unveiled its proposal for a EHDS, marking the initial step in aligning with its proposed "EU data strategy".[84] The main objectives

78 Art. 1 para 4 Regulation (EU) 2018/1724.

79 Cooperation of data use still underlies competition law concerns, see Mendelsohn/Richter, para 11.

80 <https://digital-strategy.ec.europa.eu/en/policies/data-intermediary-services>.

81 <https://digital-strategy.ec.europa.eu/en/policies/data-altruism-organisations>.

82 See also Carovano/Finck, 14.

83 For the current situation in Switzerland, see: Sprecher Franziska, Digitalisierung im Gesundheitswesen – Zum Umgang mit Gesundheitsdaten und zur Schaffung von Gesundheitsdatenräumen, in: Epiney Astrid, Havalda Stefanie, Zlătescu Petru Emanuel (eds), Datenschutz und Gesundheitsschutz / Protection des données et protection de la santé, Zürich 2023, 29-44, 32.

84 Communication from the Commission on a European strategy for data, COM (2020) 66 final; Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM (2022) 197 final.

of the EHDS are to encourage greater sharing of health data for primary use and to improve access to health data for secondary purposes, therefore facilitating control of personal health data for individuals on the one hand, and promoting access to relevant electronic health data to researchers, innovators and policy-makers on the other hand.[85] In order to achieve these aspiring goals, the proposal foresees the establishment and implementation of common technical standards and infrastructure.[86]

II. Content – Background and General Provisions

The fact that the EHDS is the first of the data spaces to be created is not surprising, given the existing challenges in optimising efforts to improve the sharing of health data.[87] This is attributed to various legal and technical barriers, coupled with a general reluctance to share data.[88] In particular, the lack of uniform implementation and interpretation of the GDPR concerning health data has led to considerable legal uncertainty.[89] Additionally, the CBHC Directive[90], which partially deals with the cross-border sharing of health data in Europe, has demonstrated ineffectiveness due to the voluntary nature of the guidelines established within its framework.[91] The European Commission's draft regulation aims to address these shortcomings. In essence, the proposal strives to enhance the sharing of health data through two main approaches:

1. Primary use (Art. 3 seq. EHDS proposal)

Today, individuals face difficulties in accessing and controlling their personal electronic health data, both in their own country and at the EU level.[92] The EHDS proposal seeks to enhance individual control over health data in relation to primary use by introducing certain rights and mechanisms complementing GDPR subject rights.[93] In particular, the proposal provides for individuals to have free access to their personal electronic health data and for each individual to be able to add or amend certain information in their electronic

85 COM (2022) 197 final, 2.

86 Li Wenkai/Quinn Paul, The European Health Data Space: An expanded right to data portability?, Computer Law & Security Review 52 (2024), 1-13, 1.

87 Sprecher Franziska, Gesundheitsdatenraum Schweiz, LSR 2022, 131-133, 131.

88 Li/Quinn, 5.

89 COM (2022) 197 final, 1.

90 Directive (EU) 2011/24 of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross border healthcare, OJ L 88, 4 April 2011, 45–65.

91 See Art. 14 Directive (EU) 2011/24; COM (2022) 197 final, 3.

92 COM (2022) 197 final, 1.

93 Li/Quinn 5.

health record (EHR).[94] Furthermore, by including the establishment of common standards and technical specifications for electronic health records, the Commission aims at creating a pan-European infrastructure to facilitate the sharing of essential components of EHRs across Europe.[95]

2. Secondary use (Art. 33 seq. EHDS proposal)

Not only the individual, but also research and innovation should benefit from easier access to electronic health data. The so-called secondary use of health data refers to the processing of electronic health data for specific purposes defined in chapter IV of the proposal.[96] Accordingly, electronic health data can be processed for secondary use *i.a.* for scientific research, activities for reason of public interest, for education and teaching activities and for the development and innovation of medicinal products or services.[97] However, seeking access to and processing electronic health data to take decisions detrimental to an individual, to exclude an individual from the benefit of insurance contracts and for advertising or marketing purposes is prohibited.[98] In order to enable the availability of data for these purposes, the EHDS proposes the establishment of so-called *health data access bodies*, designated by the Member States.[99] Data users seeking access to specific datasets must fulfil certain access requirements and have an obligation to explain the intended use, the reasons and the purpose of the access.[100] If the authorisation is granted, the health data access body requests the health data from the data holder, who shall put it at the disposal of the former within two months from receiving the request.[101]

III. Assessment – Balancing Convenience with Data Security and Privacy

At first glance, the facilitated access to one's electronic health data may seem appealing, as certain processes, such as obtaining a medical prescription in another Member State, will be simplified. However, the risk of a data leak or of health data being used for purposes not foreseen in the EHDS could – if

94 Art. 3 para 2 and 6 COM (2022) 197 final.
95 Li/Quinn 5.
96 Art. 2 para 2 point e COM (2022) 197 final.
97 Art. 34 COM (2022) 197 final.
98 Art. 35 COM (2022) 197 final.
99 Art. 36 COM (2022) 197 final.
100 Art. 45 COM (2022) 197 final.
101 Art. 41 para 4 COM (2022) 197 final.

realised – undermine the credibility of the European institutions and citizens' trust in them. Acknowledging this risk, the Parliament's Committees on the Environment, Public Health and Food Safety (ENVI) and on Civil Liberties, Justice and Home Affairs (LIBE) foresee in their joint report the mandatory storage of personal electronic health data within the EU which shall mitigate the risk of a data leakage.[102] However, further critique extends beyond general security concerns regarding the EHDS' infrastructure, with specific apprehension surrounding data protection. An instance of this is the disapproval of the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) to include data generated by wellness applications in the secondary use of health data under chapter IV of the proposal.[103] According to the EDPB and the EDPS, wellness applications generate significant volumes of highly invasive data (e.g. via mobile devices or wearables such as smartwatches) that differ in characteristics and quality requirements from those generated by medical devices.[104] While it might be possible to separate health data from other data types, making inferences about habits, including food practices, remains possible, which could result in unveiling highly sensitive information, such as religious orientation.[105] Moreover, the use of wellness applications for secondary use also reflects an invitation for Big Tech to strengthen their position in the EHR market and puts important market considerations at risk.[106] While recognizing the importance of providing individuals with convenient access to their health records, an unquestioning promotion of interoperability, without considering market imbalances, increases the likelihood of intensifying the reliance of crucial public functions on Big Tech and their infrastructures.[107]

---

102 Report A9-0395/2023 on the proposal for a regulation of the European Parliament and of the Council on the European Health Data Space (COM(2022)0197 – C9-0167/2022 – 2022/0140(COD)), 291.

103 EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, 4.

104 Joint Opinion 03/2022, 4; Sprecher (2023), 29.

105 Joint Opinion 03/2022, 4.

106 See e.g. Amazon partnering with One Medical to create the Amazon Clinic, <https://www.forbes.com/sites/katiejennings/2023/11/08/amazon-primes-new-one-medical-discount-undercuts-amazon-clinic-prices/>; Terzis Petros/Santamaria Echeverria Enrique, Interoperability and governance in the European Health Data Space regulation, Medical Law International 2023, 1-9, 4.

107 Terzis/Santamaria Echeverria, 4.

IV. Outlook

At time of writing, Parliament's Committees ENVI and LIBE adopted their joint report. Worth mentioning is the creation of a partial or entire opt-out mechanism for natural persons regarding the secondary use of health data.[108] The rapporteurs stress that in order to ensure the right to object under Art. 21 para 6 GDPR, an opt-out mechanism with regards to the secondary use of health data should be provided.[109] Although the opt-out model does not go far enough for many data protectionists because it is difficult to reconcile with the principle of digital self-determination, this step significantly restricts the Commission's former plan to create a European Health Data *Paradise* for researchers, innovators and public authorities.[110]

G. Artificial Intelligence Act (AI Act)

I. Context

> *"We had one objective: to deliver a legislation that would ensure that the ecosystem of AI would develop with a human-centric approach, respecting fundamental rights and European values."*[111]
>
> – *Brando Benifei (co-rapporteur of the European Parliament on the AI Act trilogue).*

Although the looming shadow of a (supposedly overdue)[112] Skynet may not have been on the mind of the EU institutions during the negotiations of the AI Act, the words above nevertheless suggest that the so-called "alignment problem"[113] is not merely relegated to the realm of science fiction. The AI Act puts forward an answer to the problem: alignment with European values.

The definitive version of the text is not yet available, as the Member States still have to vote on its final iteration. Consequently, the purpose of this

---

108 Report A9-0395/2023, 290.

109 Report A9-0395/2023, 290.

110 Sprecher (2023), 43.

111 Benifei Brando, Press conference of 9 December 2023, available at <https://newsroom.consilium.europa.eu/events/20231206-artificial-intelligence-act-trilogue/142864-2-press-conference-part-2-20231209>.

112 According to the original terminator movie, the human resistance lead by John Connor is bound to destroy Skynet's defence system in 2029.

113 For a seminal discussion on the AI alignment problem see Bostrom Nick, Superintelligence: Paths, Dangers, Strategies, Oxford 2017.

contribution will be to give a general overview of the AI Act on the basis of its latest version.[114]

The AI Act sets up a legal framework with multiple, conflicting goals. It seeks to foster the development and use of AI in the internal market while also guaranteeing a high level of protection of European values such as health, safety, protection of fundamental rights, democracy, the rule of law, and environmental protection. According to the architects of the AI Act, these targets will be achieved through a combination of measures fostering innovation (with a particular focus on SMEs), and clear and robust rules which protect European values. The balance sought should enable the EU to remain a global leader in the development of secure, trustworthy, and ethical AI.[115]

The EU's chosen legislative instrument for AI regulation follows a proportional, risk-based approach. The AI Act consequently imposes its most stringent requirements only on those AI systems which present a high risk for such violations to occur and outright prohibits only certain AI applications which present unacceptable risks. The last residual category only deals with transparency obligations.[116] AI systems which do not fall under any of these risk categories are not subjected to any obligations under the AI Act. Yet, they remain subject to other EU laws like the General Product Safety Regulation when AI systems are integrated into other products[117] or the GDPR when AI systems process biometric personal data.[118]

The AI Act sets up a regulatory framework in which Member States and the EU (through the newly founded AI Office) collaborate in directing and overseeing private actors' own governance choices. The AI Office will be mainly responsible for the oversight of the most powerful General Purpose AI (GPAI) models

---

114 For the latest (leaked) version of the text of 21 January 2024 see <https://artificialintelligenceact.eu/wp-content/uploads/2024/01/AIA-Final-Draft-21-January-2024.pdf>; for the older, official text see Proposal for a Regulation of the European Parliament and the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM/2021/206 final.

115 Para 15 (Recital 5) AI Act.

116 Para 24 (Recital 14) AI Act.

117 See Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC, OJ L 135, 23 May 2023, 1–51.

118 See Regulation (EU) 2016/679, see in particular Art. 9 Regulation (EU) 2016/679.

(e.g. ChatGPT and Dall-E), while national authorities will play a more prominent role (mostly in terms of market surveillance) in enforcing the rest of the AI Act.[119]

As such, the AI Act should not be understood as a regulatory instrument for AI as a technology itself but rather only for certain applications of AI. In particular, it shows features characteristic of product safety/liability regulations.

II. Content

The AI Act differentiates between three risk levels: unacceptable risks, high risks, and low risks.[120] Additionally, GPAIs (although this last point is still the subject of contention) will be subjected to additional specific obligations, independently of whether the GPAI itself represents a high-risk application or whether it may be a component of another high-risk application.[121]

Art. 5 lists AI applications prohibited by the Act as they pose "unacceptable risks". There are four main categories, with the first three applying across the board (points a, b and c), and the last one only to law enforcement (point d).

Points a and b respectively prohibit AI applications which use subliminal (and other comparable intentional manipulation techniques), and those that exploit particular groups' vulnerabilities (stemming, for example, from disabilities, or specific social/economic circumstances).[122] Point c instead bans the use of AI for the evaluation of individuals (or groups) for social scoring based on social behaviour or personal characteristics.[123]

Point d is, at the moment, the most contentious of the "prohibited" practices, which finds itself in a debate between privacy and security.[124] It restricts the use of AI for real-time remote biometric identification in publicly accessible spaces. However, it also contains a list of exceptions. Examples are the search

---

119 See EC, Commission Decision of 24 January 2024 establishing the European Artificial Intelligence Office, OJ C, C/2024/1459, 14 February 2024; see in particular Art. 3 AI Act; see also para 90 (Recital 80) AI Act.

120 Para 24 (Recital 14) AI Act.

121 Para 67a (Recital 57a) AI Act.

122 Paras 181-182a (Art. 5(1) point a and b) AI Act.

123 Paras 183-186 (Art. 5(1) point c) AI Act.

124 <https://www.euronews.com/my-europe/2024/01/30/could-the-eus-artificial-intelligence-act-increase-mass-surveillance-systems>.

for victims of human trafficking, the prevention of terrorism but also broader categories such as the search for *suspects* of certain crimes,[125] for which Member States established a maximum prison sentence of at least four years.[126]

Title III covers AI Systems deemed "high risk" based on either Annex II or Annex III. Art. 6 (1) applies to AI systems which fall, either directly or through their integration as safety components of products, under certain EU harmonisation legislations. Examples range from toy safety regulation to civil aviation and machinery.[127] Art. 6 (2) instead is based on Annex III, which then classifies AI systems as high-risk directly through the Act itself. Examples are biometric identification systems, safety components of critical infrastructure, applications which impact education/vocational training, employment, and access to essential services.[128] It is also worth noting that, based on Art. 7, the Commission is empowered, under certain conditions, to update Annex III.

The last category of risks is focused on transparency. Art. 52 imposes transparency requirements on AI systems that, although not deemed high-risk, are going to interact with natural persons (this definition also includes all GPAIs). The purpose of this obligation is to enable individuals to be aware when they interact with an AI, give consent prior to their processing of biometric data, and be aware that the content they are exposed to has been altered (e.g. deepfakes).[129]

III. Assessment

The AI Act's chosen product liability approach shows several advantages. First, it pre-empts the fragmentation that would ensue from each Member State's adoption of their individual AI regulations. Second, the risk-based approach allows prioritisation of the most serious risks and allows SMEs to reduce compliance costs. At the same time, reliance on private actors' self-governance would reduce the public resources needed for monitoring compliance.[130] Third, the product safety regulation approach falls well within the area of competency and expertise of the EU as a mainly sectoral regulator, well poised to protect values like health and safety.

---

125 For the list see para 806a (Annex IIa) AI Act.

126 See para 189 (Art. 5(1) point d(iii)) AI Act.

127 Para 200 (Art.6(1)) and paras 785-806 (Annex II) AI Act.

128 See para 203 (Art.6(2)) and paras 807-837c (Annex III) AI Act.

129 Paras 513-516a (Art. 52) AI Act.

130 <https://www.euronews.com/next/2024/02/01/commissions-staffing-and-financing-of-ai-office-raises-eyebrows-in-capitals>.

However, this approach, biased towards the logic of market integration, is not without its shortcomings. At a conceptual level, the assessment of risks to fundamental rights does not follow the same logic of product safety, which is instead geared towards the protection of health/safety. To summarise a complex topic, the latter aims to establish technical parameters where it does not matter whether the system barely meets the minimum requirements or surpasses them with flying colours (i.e. a satisficing logic), whereas the former requires fundamental rights to be protected and promoted to the maximum extent, and only the least possible restrictions are accepted (best exemplified by the principle of proportionality's maximisation logic).[131] In this regard, the adoption of a separate type of assessment—which follows one of the two underlying logics, depending on whether the European value at stake is health/safety or the protection of a fundamental right—would have been a welcomed improvement. Such a change would also be realistic since the "high risk" classification based on either Annex II or Annex III mentioned above, already seems to reflect the health/safety and fundamental rights dichotomy to some degree.

The contrast between the two opposing logics can be observed in Art. 6 (2a) and (2b), which allows providers to exempt themselves from the substantive rules for high-risk systems if they deem that their AI System, despite falling under Annex III, nevertheless does not pose "significant risk of harm" to the values protected by the Act.[132] While this approach indeed reduces compliance and monitoring costs, it is perhaps underestimated how the person with the ability to decide what and why (i.e. on the basis of which logic) something poses "significant risks of harm" will radically change the impact of the Act.

From a completely opposite perspective, it has been questioned whether the AI Act is going to harm innovation. This sentiment has been most prominently echoed by Macron's words, "we will regulate things that we will no longer produce or invent".[133] This objection can be countered by the fact that, as history teaches us, innovation's impact is never inherently beneficial (or harmful) but rather the outcome of political decisions which we make as a

---

131 For a more in-depth discussion see Almada Marco/Petit Nicolas, The EU AI Act: A Medley of Product Safety and Fundamental Rights?, RSC Working Paper 2023/59, available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4617276>.

132 See paras 203b-203k (Art. 6 (a) and(b)) AI Act.

133 <https://www.ft.com/content/9339d104-7b0c-42b8-9316-72226dd4e4c0>.

society.[134] The AI Act is supposed to inject European values into the direction that innovation should take. Not every innovation should be sought, but only those that are compatible with fundamental rights and other basic values.

IV. Outlook

The AI Act's text was adopted by the European Parliament and Council in December 2023 after three days of "marathon talks". It is now the turn of the Member States, which will discuss the text during the coming months. In particular, at the time of writing, the bloc of France, Germany, and Italy seem to oppose the text. Should the Act nevertheless be approved by the Member States, it is not expected to enter into force before 2025.[135]

H. Perspectives

The overview of six key texts for the digital sphere illustrates the EU's great ambitions in the area of digital regulation. The DMA attempts to control bottleneck power, provides for a special mechanism against the tipping of markets and thus aims to counteract concentration trends with the overall objective to strengthen competition in markets that rely on the use of gatekeeper platforms. The DSA constitutes a European constitution for the Internet and contains rules with a horizontal effect that are intended to create a reliable online environment for consumers in the use of online platforms and digital services. While the DA provides for new rules on the access to data generated by IoT-Devices, the DGA establishes a general system of how data can be shared. Both regulations seek to improve the availability of data and thereby to increase its actual use. The EHDS project, on the other hand, would create the first common EU data space for a specific area, in which data sharing would be encouraged for primary use (individual use of health data) and secondary use (e.g. research and innovation). Finally, the AI Draft not only provides for transparency requirements and special product safety rules based on a risk-based approach but has the ambition to safeguard fundamental rights and values in the most disruptive area of the digital sphere.

All the texts presented here have one goal in common: to promote innovation in various ways. The fundamental question therefore is whether the European approach to regulation is suited to achieving this goal. On the one hand, it

---

134 See Acemoglu Daron/Johnson Simon, Power and Progress: Our Thousand-Year Struggle Over Technology and Prosperity, UK 2023.

135 <https://www.theverge.com/2023/12/14/24001919/eu-ai-act-foundation-models-regulation-data>.

is certainly conducive to innovation when data is made accessible that would otherwise have remained hidden and unused. Moreover, it seems obvious that the rules for the traditional economy should also apply in the digital world. On the other hand, the question may be raised as to whether further-reaching obligations, for example with respect to gatekeepers or AI, will impair the incentives for innovation. It cannot be overlooked that the accents are set differently here. With regard to interoperability, for example, the European and American approaches differ: while Europe traditionally points to the innovation-promoting effects of disclosure obligations, the USA rather tends to emphasise its innovation-dampening risks. On a more general level, with regard to the latest technologies, there is a risk that the EU will only be the world champion of AI regulation, while the US remains the world champion of AI.[136] Instead of relying on a "Brussels Effect", it would be desirable if similar regulatory requirements could be achieved at a worldwide level. The Executive Order on AI by the American President creates hope for convergence.[137] However, it is crucial to go one step further and take the necessary measures in the global forums such as the WTO, in other words to strengthen rules-based multilateralism again. Nothing has changed in the truism that global problems can only be solved globally. This statement is particularly true for the challenges of the digital world.

136 Heller Piotr, Weltmeister der Regulierung, Frankfurter Allgemeine Sonntagszeitung of 17 December 2023, 53.

137 President Joseph R. Biden, Executive Order 14110 of 30 October 2023 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence <www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence>.

EuZ
ZEITSCHRIFT FÜR EUROPARECHT

26. Jahrgang

Herausgeber

Europa Institut an der
Universität Zürich
Hirschengraben 56
8001 Zürich
Schweiz
eiz@eiz.uzh.ch

Institut für deutsches und
europäisches Gesellschafts-
und Wirtschaftsrecht der
Universität Heidelberg
Friedrich-Ebert-Platz 2
69117 Heidelberg
Deutschland

LL.M. Internationales
Wirtschaftsrecht
Universität Zürich
Hirschengraben 56
8001 Zürich

Redaktion
Dr. Tobias Baumgartner, LL.M., Rechtsanwalt (Leitung)
MLaw Sophie Tschalèr
Dr. Wesselina Uebe, Rechtsanwältin

Cover-Foto: svstudioart, Freepik

Erscheinungsweise
EuZ – Zeitschrift für Europarecht erscheint zehnmal jährlich online. Die Leitartikel werden zu Beginn des Folgejahres zusätzlich in Form eines Jahrbuchs als eBook sowie im Wege des print on demand veröffentlicht.

Zitierweise
EuZ, Ausgabe 3/2024, C 13.

ISSN
1423-6931 (Print)
2813-7833 (Online)

Kontakt
EIZ Publishing c/o Europa Institut an der Universität Zürich
Dr. Tobias Baumgartner, LL.M., Rechtsanwalt
Hirschengraben 56
8001 Zürich
Schweiz
eiz@eiz.uzh.ch

Version 1.00-20240314

DOI
Chayanis Aueamnuay, Carmen Berjón, Stella Galehr, Luca Graf, Andreas Heinemann, Digital Regulation in the European Union, https://doi.org/10.36862/eiz-euz2024-03