Norbert Bernsdorff*

E-Commerce and Data Protection - The Digital Services Act and its National Implementation

As part of a "European data strategy", the European Commission has long been endeavouring to create a uniform European internal data market and to establish new regulations for the use of artificial intelligence. In the area of conflict between the requirements of Article 8 of the Charter of Fundamental Rights of the European Union on data protection on the one hand and the need to facilitate the handling of personal data - which is important for the digital economy - on the other, several laws proposed by the European Commission (Data Governance Act, Data Act, Digital Services Act and Digital Markets Act) have created the necessary framework conditions. The Digital Services Act in particular regulates the new obligations for providers of digital services.

Keywords: *Data protection on the internet, Digital Services Act, internal data market, E-Commerce, digital services, transmission-, caching- and hosting-services, online platforms, imprint obligation, General Data Protection Regulation.*

1. Introduction

Digital services influence and facilitate our lives in many different ways. They are used, for example, to communicate with each other, shop online, find information on the internet or for digital entertainment such as gaming, music or films. There are therefore many categories of online services, from simple websites to app-stores and online platforms.

* Doctor of Law, Professor at the Philipps University of Marburg; Retired judge at the Federal Social Court of Germany. Member of the Editorial Board of the Journal of Personal Data Protection Law.

Anyone who handles personal data outside of the personal and family sphere must comply with the General Data Protection Regulation (GDPR)[1]. Providing information on a hotline to the wrong person can be a data protection offence, as can storing customer data for too long or providing information about data that a company stores about a person too late. These processes are regulated by the GDPR, as they involve the processing of personal data that is collected and stored in analogue or digital form from individuals. However, not all data is collected from individuals. Data processing also takes place when companies collect data on computers, mobile phones, etc. via software, operating systems or browsers. Without such access by the provider of a website or app to the device from which the page is accessed, the devices cannot communicate with the provider's servers.

However, they must do so in order for data transmission to take place, which results in content being transferred from the provider's server to the end device as images, text or sound. In the European Union (EU), this type of data processing is not regulated by the GDPR, but more recently by the new Digital Services Act (DSA).[2]

2. The Aim of the Digital Services Act

In future, the DSA will regulate the activities of digital service providers within the EU. This creates one of the most important sets of digital policy regulations in Europe. Together with the Digital Markets Act (DMA)[3] , the sibling of the DSA, the new regulations are intended to become a kind of basic law for the internet. The main aim is to restrict previously uncontrolled data processing in the area of E-Commerce.

The DSA has been officially in force in the EU since 16 November 2022. In an initial phase, the DSA was only mandatory for very large online platforms and very large online search engines. The regulations have been fully applicable since 17 February 2024. It aims to protect European consumers and their fundamental rights in the digital space and ensure a level playing field for companies. Together with the DMA, the DSA is intended to form an overarching guideline for the internet. In the coming months and years, digital

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data and Repealing Directive 95/46/EC, OJ 2016 L 119, 1.

[2] 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, OJ 2022 L 277, 1.

[3] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828, OJ 2022 L 265, 1.

providers will therefore be faced with substantial changes. The *European Council*, together with the *European Parliament*, has adopted the DSA to strengthen the digital single market.

The DSA strengthens consumer protection in the digital space through clear rules and transparency obligations. This includes imposing clear obligations on online platforms and social media. In particular, the DSA regulates the handling of illegal content and products that are brought into circulation in violation of data protection regulations. The DSA also promotes the creation of a secure and transparent digital environment. The provisions also include measures to protect freedom of expression by setting clear guidelines for the moderation of content. Providers of so-called intermediary services - for example hosting services, online marketplaces, social networks, etc. - are required by the DSA to ensure transparency. They are obliged by the DSA to be completely transparent and responsible. This will create a standardised legal framework for digital services in the EU.

3. Not a European Directive, but a European Regulation

The DSA has been directly applicable in all EU Member States since 17 February 2024, without the need for further national implementation by them. In legal terms, it is a European regulation and not just a directive.

European directives are limited to prescribing a certain result for EU Member States. However, they leave the achievement of this result to the Member States themselves; they must implement directives within certain deadlines through their own national legislation. In contrast, EU regulations are directly and immediately binding for all EU Member States and not, like a directive, only with regard to the result to be achieved.

What prompted the EU to adopt the DSA as a regulation?

With the previous data protection law, all EU Member States had the same legal basis. However, they were able to determine the implementation of data protection themselves. As a result, there was a considerable imbalance in the level of data protection in the individual EU Member States. The introduction of the DSA, which is directly and immediately binding for all Member States, was intended to eliminate this imbalance.

4. The Regulations of the DSA in Detail

The following pages present the main regulatory content of the DSA:

4.1. Material Scope of Application: "Digital Services"

The range of services covered by the DSA is immense, from online marketplaces to social networks and search engines.

The provisions of the DSA apply in principle to all "digital services". "Digital services" are generally information society services, i.e. all services that are generally provided electronically for a fee at a distance and at the individual request of recipients.[4] The DSA emphasises "intermediary services" under Article 2 (1) and includes the following services:

- "hosting" - service consisting of storing information provided by a user on their behalf[5]
- "caching" - service that consists of transmitting information provided by a user in a communication network, whereby this information is automatically cached for a limited period of time[6].
- pure "transmission" - service consisting of transferring information provided by a user to a communications network or providing access to a communications network.[7]

The specifics of the individual services are to be taken into account through a tiered regulatory system depending on their role, size and impact in the online environment: At the lowest level, there are regulations for all providers of intermediary services.[8] At the further levels, additional regulations apply cumulatively to "hosting" service providers[9] , "online platforms"[10] and "very large online platforms"[11] The former are exempted from all platform-specific obligations, meaning that they only have to comply with the

[4] See Art. 1 (1) of the Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a Procedure for the Provision of Information in the Field of Technical Regulations and of the Rules of Information Society Services, OJ 2015 L 241, 1.
[5] Art. 6 of the "DSA".
[6] Art. 5 of the "DSA".
[7] Art. 4 of the "DSA".
[8] See Art. 11 et seq. of the "DSA".
[9] Art. 16 et seq. of the "DSA".
[10] See Art. 19 et seq. of the "DSA".
[11] Art. 33 et seq. of the "DSA".

obligations that are usual for all providers. However, these obligations already include some that are specifically tailored to artificial intelligence.[12]

Comprehensive obligations also apply to „very large online platforms", a term that Article 33 (1) of the DSA defines as 45 million users in the EU, whereby the *European Commission* is to be able to adjust this figure to population trends by means of a delegated act in accordance with Article 33 (2) of the DSA so that it covers around 10 percent of the EU population. The "very large online platforms" must carry out annual risk analyses[13], undergo independent audits[14] and appoint a compliance officer.[15]

The DSA replaces parts of the European E-Commerce Directive from 2000[16], but goes beyond this in regulating online platforms and imposes a degree of "social responsibility" for their business model on them.[17]

4.2. Which Providers of Digital Intermediary Services are in Focus?

The DSA applies in principle to all providers of digital services. The size is generally irrelevant, as both small and large companies are affected. However, the scope of the regulations and due diligence obligations to be followed differs in relation to the type and size of the service. This applies regardless of whether they are based in the EU or outside the EU. However, the intermediary services concerned must have a "substantial connection" to the EU. This may be the case, for example, if the service provider is established in the EU. In principle, the addressees of the DSA include cloud services, internet providers, "hosting"- service providers, online marketplaces, web shops, messenger services and social networks. To date, 19 large online services are covered by the DSA. According to the *European Commission*, the "very large online platforms" include in particular:

- Alibaba Aliexpress
- Amazon Store
- Apple AppStore

[12] For more information see *von Lewinski K., Rüpke G., Eckhardt J. (eds.)*, Datenschutzrecht - Grundlagen und europarechtliche Umgestaltung, 2022, 256.
[13] Art. 34 et seq. of the "DSA".
[14] See Art. 37 of the "DSA".
[15] Art. 41 of the "DSA".
[16] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, OJ 2000 L 178, 1.
[17] On this see *Beck W.*, Der Entwurf des Digital Services Act - Hintergrund, Ziele und Grundsätze künftiger Regulierung des virtuellen Raums in der EU, Deutsches Verwaltungsblatt (DVBl) 2021, 1000; *von Lewinski K., Rüpke G., Eckhardt J. (eds.)*, Datenschutzrecht - Grundlagen und europarechtliche Umgestaltung, 2022, 256.

- Booking.com
- Bing
- Google Maps
- Google Play
- Google Shopping
- Instagram
- LinkedIn
- Meta (Facebook)
- Temu
- TikTok
- Wikipedia
- X (Twitter)
- YouTube and
- Zalando.

A large number of these platforms not only exert a major influence on the opinion-forming and purchasing behaviour of users via news feeds, advertising measures and online shops, but are also at risk of using personal data in an uncontrolled manner.

4.3. The Instruments of the DSA for Enforcing the Law

The DSA has established a two-tier structure for law enforcement:[18]

4.3.1. Complaints Management and User Protection

The DSA gives users specific rights to defend themselves - for example, against breaches of data protection law.

If illegal content or breaches of data protection law are reported, online platforms must examine these reports carefully. They must provide a complaints procedure.[19] This must be easily accessible to users. Users have the right to a transparent redress procedure. For example, decisions by online platforms to delete or not to delete content or when users are denied access to a platform can be challenged. In future, providers will have to explain

[18] On this see *Verbraucherzentrale*, Digitale Dienste: Was regelt der Digital Services Act? <https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinedienste.pdf> [15.11.2024].
[19] See Art. 20, 53 of the "DSA".

openly and comprehensibly how they came to their respective decision and users will be able to have this decision-making process reviewed by means of legal remedies.[20]

E-Commerce and online advertising are particularly affected by the DSA. For example, targeted advertising for minors is prohibited. Likewise, adverts may not target religion or sexual orientation. All adverts must also be labelled as such. It must also be possible to identify who has paid for the advert in question; these transparency regulations also simplify cooperation between the platforms and law enforcement authorities. In short, online platforms must clearly disclose a) that the adverts on their website are advertisements, b) who placed them and c) what factors were decisive for a user to see this particular advert.[21] Intermediary services must also set up a central contact point for electronic communication.[22]

4.3.2. Enforcement by National Supervisory Authorities

The DSA obliges the EU Member States to designate bodies for official law enforcement that independently take action against provider violations - especially in the area of data protection law - and sanction them. Only the monitoring of “very large online platforms" is carried out by the *European Commission* itself.[23]

Because the DSA protects different legal interests, several authorities may be responsible as “DSA-coordinators" in the EU Member States.[24] This also includes the data protection authorities. However, the responsibility of the authorities must be clearly regulated; it must be ruled out that user complaints are lost in a „ping-pong of authorities". [25]

The central complaints and coordination centre in Germany is the so-called *Bundesnetzagentur*. It is the point of contact during the entire period of a complaint procedure. In Germany, however, supervision is also exercised by the so-called *Bundeszentrale für Kinder- und Jugendmedienschutz*. Consumer protection organisations are also of particular importance from a consumer

[20] Art.81 et seq. of the “DSA”.
[21] *Marx L*., Der Digital Services Act der Europäischen Kommission, AnwaltZertikat IT-und Medienrecht (AnwZert ITR), №4, 2021, margin note 2.
[22] Art. 11 et seq. of the “DSA”.
[23] *Verbraucherzentrale*, Digitale Dienste: Was regelt der Digital Services Act? <https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinedienste.pdf> [15.11.2024].
[24] See Art. 3 of the “DSA”.
[25] For more information see *Verbraucherzentrale*, Digitale Dienste: Was regelt der Digital Services Act? <https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinedienste.pdf> [15.11.2024].

protection perspective. These are naturally very „close to the ear" of consumers due to their counselling activities and their role as a complaints receiving body.

5. Related German Law: The „Digitale-Dienste-Gesetz"

Because the DSA is a European regulation, it is directly applicable in the Member States of the EU. Unlike a European directive, it no longer needs to be transposed into national law. Nevertheless, the DSA must of course be "flanked" by national law. The EU Member States themselves are responsible for enforcing its provisions. They must harmonise their national law accordingly. In Germany, the DSA is "flanked" by the national "Digitale-Dienste-Gesetz (DDG)" of 6 May 2024[26]. It highlights the difficulties that can arise when implementing the DSA in the EU Member States.

5.1. Supplementation of the DSA by the German DDG

The German DDG of 6 May 2024 largely supplements the DSA. In this context, it replaces existing national digital law.[27]

Of particular note are regulations on the liability of online platforms for content, on the setting of cookies and on fines for legal violations. The DDG deals with liability for "hosting", "caching" and "transmission" as so-called "fault-based liability". Regulations on this and on the liability of WLAN operators are specified in § 7 and § 8 DDG. Anyone who sets or reads cookies requires the explicit consent of the user. In this respect, an explicit "cookie opt-in regulation" is indispensable.

Finally, at the end of the law there are provisions on the fines that can be imposed for violations of the DDG. For example, there is a fine of up to 50,000 euros if the so-called imprint obligation is violated. In the case of commercial

[26] Gesetz zur Durchführung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19.10.2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinien 2000/31/EG sowie zur Durchführung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20.6.2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Onlinevermittlungsdiensten und zur Änderung weiterer Gesetze vom 6.5.2024 (Digitale-Dienste-Gesetz), Federal Law Gazette 2024 I, 1.

[27] *Lorenz B.*, Die Anbieterkennzeichnung nach dem DDG, AnwaltZertifikat IT- und Medienrecht (AnwZert ITR), №14, 2024, margin note 3.

communication, especially if correct sender information is concealed or hidden, the fine can even be up to 300,000 euros.

5.2. The so-called Imprint Obligation

One focus of the DDG is the so-called imprint obligation. It is an obligation to identify the service provider.[28] The so-called imprint obligation is regulated in § 5 DDG and applies to commercial digital services that are generally offered for a fee. § 5 DDG not only covers paid services, but can also apply to free services. The characteristic of payment only requires a commercial purpose of the offer.[29]

Against this background, influencer websites are also included if they advertise products or services. This does not only include monetary income that a company pays the influencer for displaying adverts. It also includes income in kind, for example if an influencer is provided with the advertised products or services free of charge by a company and is allowed to keep them.[30]

With regard to their obligation under § 5 DDG to identify the service provider, website operators must provide an imprint. The imprint must include the following informations:

- the name and address at which the service provider is established,
- in the case of legal entities, the legal form, the authorised representative, any share capital or share capital including contributions, and
- contact details, i.e. e-mail, telephone and, if applicable, fax number.

In addition, service providers may have to provide further information, such as the competent regulatory or supervisory authority, the commercial register, professional regulations and how these regulations can be accessed, as well as the tax number.

Finally, it is a requirement that the legal notice on the website is accessible via a maximum of two clicks.

[28] For more information see *Lorenz B.*, Die Anbieterkennzeichnung nach dem DDG, AnwaltZertifikat IT- und Medienrecht (AnwZert ITR), №14, 2024, margin note 3.

[29] See *Oberlandesgericht Hamburg*, decision of 3 April 2007 - 3 W 64/07, margin note 7; *Lorenz B.*, Die Anbieterkennzeichnung nach dem DDG, AnwaltZertifikat IT- und Medienrecht (AnwZert ITR), №14, 2024, margin note 3.

[30] On this see *Lorenz B.*, Die Anbieterkennzeichnung nach dem DDG, AnwaltZertifikat IT- und Medienrecht (AnwZert ITR), №14, 2024, margin note 3.

6. Conclusion

The coming years will show whether the DSA can fulfil its promises - including in terms of data protection law. The evaluation will take place by the beginning of 2027. The success of the DSA will largely depend on how well the EU Member States clarify the remaining details: They are responsible for large parts of the supervision.

Whether the DSA (together with its sibling, the DMA) has actually triggered a revolutionary development in the area of digital services,[31] will largely depend on the design of the enforcement and sanction regime, which in principle remains the preserve of the EU Member States.[32] Due to the country of origin principle, the jurisdiction of the supervisory authority is based on the location of the main establishment of the intermediary service concerned. In the context of the GDPR, for example, this decentralised principle is criticised by many experts because different national authorities sometimes act with varying degrees of speed and consistency.

In substance, however, the DSA was long overdue. After all, as technology develops, online platforms will increasingly gain market power and weaken data protection, competition and consumer protection.

Bibliography:

1. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (DSA) and amending Directive 2000/31/EC, OJ 2022 L 277.
2. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector (DMA) and amending Directives (EU) 2019/1937 and (EU) 2020/1828, OJ 2022 L 265.
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data and repealing Directive 95/46/EC (GDPR), OJ 2016 L 119.
4. Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a Procedure for the Provision of

[31] The *Economist* of 15.12.2020, <https://www.economist.com/business/2020/12/15/the -eu-unveils-its-plan-to-rein-in-big-tech.html> [15.11.2024].
[32] See Recital No. 79 of the "DSA".

Information in the field of Technical Regulations and of the Rules of Information Society Services, OJ 2015 L 241.
5. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce, in the Internal Market (E-Commerce Directive), OJ 2000 L 178.
6. *Verbraucherzentrale*, Digitale Dienste: Was regelt der Digital Services Act? <https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinedienste.pdf> [15.11.2024].
7. *Beck W.*, Der Entwurf des Digital Services Act – Hintergrund, Ziele und Grundsätze künftiger Regulierung des virtuellen Raums in der EU, Deutsches Verwaltungsblatt (DVBl), 2021, 1000.
8. *Brauneck J.,* Das Verantwortungsbewusstsein der Plattformbetreiber im Digital Services Act, Neue Zeitschrift für Verwaltungsrecht (NVwZ), 2024, 377.
9. *Brorsen H., Falk R.*, Neue Compliance-Pflichten nach dem Digital Services Act, Zeitschrift für IT-Recht und Recht der Digitalisierung (MMR), 2024, 32.
10. *Buchheim J., Schrenk M.*, Der Vollzug des Digital Services Act, Neue Zeitschrift für Verwaltungsrecht (NVwZ), 2024, 1.
11. *Legner S.*, Der Digital Services Act – Ein neuer Grundstein der Digitalregulierung, Zeitschrift für Urheber- und Medienrecht (ZUM), 2024, 99.
12. *Lorenz B.*, Die Anbieterkennzeichnung nach dem DDG, AnwaltZertifikat IT- und Medienrecht (AnwZert ITR), №14, 2024, margin note 3.
13. *Marx L.*, Der Digital Services Act der Europäischen Kommission, AnwaltZertifikat IT- und Medienrecht (AnwZert ITR), №4, 2021, margin note 2.
14. *von Lewinski K., Rüpke G., Eckhardt J. (eds.)*, Datenschutzrecht – Grundlagen und europarechtliche Umgestaltung, 2022.