TNO innovation for life

An overview of relevant European legislation for MSMEs engaged in Data Sharing

TNO Public ⟩ TNO 2024 R12799
22 november 2023

ICT, Strategy & Policy
www.tno.nl

TNO 2024 R12799 – 22 november 2023

An overview of relevant European legislation for MSMEs engaged in Data Sharing

Auteurs	K. (Kartik) Chawla
Rubricering rapport	TNO Public
Titel	TNO Public
Rapporttekst	TNO Public
Aantal pagina's	22 (excl. voor- en achterblad)
Aantal bijlagen	0
Projectnaam	Centre of Excellence for Data Sharing and Cloud
Projectnummer	060.54832

Table of Contents

1 Introduction

Navigating intricate and shifting legislative landscapes can be daunting for any organisation, but it is perhaps especially so for **Micro, Small and Medium-sized enterprises (MSMEs)**. This is particularly true for many legislations released under the EU's new Digital Package. But knowing the rules, especially those affecting digital businesses and data sharing, can give such MSMEs an important edge in complying with and benefitting from them.

This document provides an introductory summary highlighting four key new instruments which are part of the European Commission's '*A Europe fit for the Digital Age*' package and impact data sharing within the EU. Specifically, this document discusses the **Data Act (DA)**, the **Data Governance Act (DGA),** the **Digital Services Act (DSA)** and the **Digital Markets Act (DMA)**.

The intended audience of this document are Dutch and European Micro, Small and Medium enterprises (MSMEs) that are already participating in data sharing activities or will do so in the near future. These legislations can apply differently to MSMEs than they do to other organisations, for instance due to exemptions, incentives or discounts provided for MSMEs. It is therefore crucial that SMEs that engage in data sharing are aware of their contents so that they can avoid potential non-compliance and the corresponding penalties, and also make the best use of available rights and remedies. Some highlights are specifically applicable t**o Micro and Small Enterprises (MSEs*)**, and some are specifically applicable to **Micro, Small and Medium Enterprises (MSMEs**)**. These have been annotated accordingly.

This work does not attempt to provide a detailed legal analysis of these instruments but instead highlights some of their essential obligations and opportunities, particularly from the point of view of MSMEs. Furthermore, these regulations are still rather new and will likely be clarified further in due course through their application and commentaries from the appropriate authorities. The summaries provided in this document are non-exhaustive, do not constitute legal advice and should not be considered a substitute for reading the instruments and talking to a lawyer.

1.1 Structure of this document

The following chapters provide an introductory overview of the Data Act, the Data Governance Act, the Digital Services Act and the Digital Markets Act, respectively. While reading this document, it is important to note that the **General Data Protection Regulation (GDPR)** remains in force, and these legislations function in addition to it. In cases of conflict, the GDPR has precedence.

Each chapter is structured as follows: first, it provides an overview of the 'roles' that the act in question regulates, along with checklists that the reader can use to evaluate whether these roles can be applicable to them.[1] This is followed by a fictional example that illustrates the roles in practice. In case a role seems applicable based on the checklist and the example, the reader should seek further guidance from a lawyer or a legal expert. The table below also provides a quick overview of these roles and their relevance to MSMEs. Second, each chapter then non-exhaustively highlights the main provisions of the Act applicable to each role; third, it discusses how the Act will be enforced. Finally, fourth, the chapter provides an idea of future updates to keep track of, and also provides additional links for further reading on the specific Act.

[1] These definitions are likely to receive further clarification for their applicability with passing time.

Legislation	Roles	Potentially applicable to MSMEs?	Benefits to MSMEs?
Data Act (DA)	IoT Product Manufacturers and Service Providers	Yes	Yes
	Data Holders	Yes	Yes
	Data Processing Service Providers (DPSPs)	Yes	Yes
	IoT Users	Yes	Yes
	Data Recipients	Yes	Yes
Data Governance Act (DGA)	Public Sector Bodies (PSBs)	No	Yes
	Data Intermediation Service Providers (DISPs)	Yes	Yes
	Data Altruism Organisations (DAOs)	Yes	Yes
	Data Users	Yes	Yes
Digital Services Act (DSA)	Intermediary Service Providers (ISPs)	Yes	Yes
	Online Platforms (OPs)	Yes	Yes
	Very Large Online Platforms (VLOPs) Very Large Online Search Engines (VLOSEs)	No	Yes
	Consumer	No	No
	Trader	Yes	Yes
Digital Markets Act (DMA)	Gatekeepers	No	Yes
	Business User	Yes	Yes
	End User	No	No

1. Data Act

Date Proposed	Date Adopted	Applicable from
February 2022	November 2023	12th September 2025

1.2 Whom does it apply to?

The recently adopted Data Act is a wide-ranging legislation that has potentially significant implications for various data-sharing activities within the EU. The Data Act is a sector-agnostic legislation that affects data sharing and digital services in various contexts and roles. Broadly, it seeks to empower individuals and businesses while ensuring responsible and ethical data handling in the digital era. It redefines rules and practices on data access and, in collaboration with other legislations, aims to foster data (re)use. The leading roles affected by the Data Act are discussed below.

Roles	Criteria
IoT Product Manufacturers, and Related Service Providers	✓ Do you produce or manufacture connected devices, such as a smart home appliance or smart industrial machinery? ✓ And, do these devices obtain, generate, or collect data concerning their use or environment? ✓ And, can they communicate product data, for instance via an electronic communications service? ✓ And, is their primary function **not** the storing and processing of data on behalf of a party other than the user? ➢ Then you may qualify as a product manufacturer. ✓ Do you provide a digital service, such as software? ✓ And, is this digital service integrated into a connected device at time of purchase, rent or lease? ✓ And, could the connected device not perform one or more of its services without your digital service? ✓ Or, is it connected to the device at a point later than its purchase to add to, update or adapt its functions? ➢ Then you may qualify as a related service provider.
Data Holders[2]	✓ Do you have a right or obligation to make specific data available under EU law or national legislation adopted in accordance with EU law? Such a right or obligation can be, for instance: o As an IoT manufacturer under the Data Act, or o A data holder receiving a request for data from a public body under exceptional need, or o A data holder making data available under the Digital Governance Act, or o A data holder making data available under the GDPR. ➢ Then you may qualify as a Data Holder. ➢ Please note that this is category is broader than obligations to make data available under the Data Act.

[2] It is important to note that data holders can also be data controllers under the GDPR if they hold personal data. In that case, they would still need to comply with the GDPR.

Data Processing Service Providers (DPSPs)	✓ Do you provide cloud or edge computing services? ✓ That is, do you enable ubiquitous and on-demand network access to a configurable, scalable and elastic pool of shareable computing resources that can be rapidly provisioned with minimal management? ➢ Then you may qualify as a Data Processing Service Provider.
IoT Users	✓ Do you own or use an IoT Product or a Related Service? ➢ Then you may qualify as a User under the Data Act.
Customers	✓ Do you use cloud or edge computing services? ✓ Do you have a contract for the provision of this service? ➢ Then you may qualify as a Customer under the Data Act.
Data Recipients	✓ Has a 'data holder' made data available to you, or is making it available to you? ✓ Is this in relation to your trade, business, craft or profession? ✓ Are you **not** the user of the relevant IoT product or related service? ➢ Then you may qualify as a Data Recipient.

Example

Consider, for instance, a fictional company called Wheezy. Wheezy manufactures and distributes wi-fi enabled smart bulbs that consumers can use in their smart home setups. These bulbs collect usage data, and also collect data about the temperature in their surroundings. Jane, an artist living in Amsterdam, purchases a few of Wheezy's smart bulbs for her home. Wheezy, in this case, is likely to be an IoT Product Manufacturer, and Jane is likely to be an IoT User.

Consider a second fictional company called Wheezy-Way. Wheezy-Way develops and maintains Wheezy-Way, a multi-platform app that allows users to connect to and manage their Wheezy smart bulb products. While the user could turn the bulbs on and off without the app, they couldn't modify the colour of the lamp without it. Wheezy-Way, in this case, is likely to be a Related Service Provider. Both Wheezy and Wheezy-Way would be likely to qualify as Data Holders as well, as they have an obligation to make available to Jane data generated by her use of the smart bulb.

Consider a third fictional scenario: Jane finds that one of the smart bulbs she bought starts malfunctioning. She finds that while Wheezy does offer a repair service, it is in a different town – but a third-party aftermarket service provider, RepairIT, is available in Amsterdam itself. Jane goes to RepairIT and shares the data from her smart bulb with them, making them likely to be a Data Recipient.

Further examples of IoT Product Manufacturers and Related Service Providers include manufacturers of or integrated digital service providers for smart vehicles, smart industrial devices such as tractors, smart home products, medical and health devices, and voice assistants. Further examples of Data Holders include internet access providers and content distribution networks. Further examples of data recipients include AI start-ups obtaining training data from other organisations, or directly from the users of IoT devices.

Consider a fourth and final fictional scenario, where a fictional company SkyVault provides its clients with access to elastic computing resources, but only to the servers and networks. That is, it provides its customers with access to the infrastructural elements but not to operating services or software stored on these servers. SkyVault would, here, be likely to be a Data Processing Service Provider under the Data Act as an IaaS provider. Clients of SkyVault would be likely to qualify as Customers. Further examples of DPSPs include PaaS, SaaS and edge computing service providers such as Amazon Web Services.

1.3 Highlights per Role

IoT Product Manufacturers and Related Service Providers*	Data Holders	Data Processing Service Providers (DPSPs)
IoT Product Manufacturers and Related Service Providers must design their products and services in such a way as to provide users with access to the associated readily available data and relevant meta-data by default, securely, easily, in a commonly used and machine-readable format, and free of charge. If the data cannot be accessed directly from the device or service, it must be made accessible through other (simple and electronic where feasible) means, without undue delay. They must also make this data available to third parties, other than parties designated as Gatekeepers under the DMA, upon user request, in compliance with further detailed requirements. IoT Product Manufacturers and Related Service Providers must also provide users with detailed pre-contractual information, including for instance information about the types and volume of data collected and how to access it. The Data Act also specifies detailed legal and economic protections for this data sharing, including for instance protection for the IoT Product Manufacturer or Related Service Provider's trade secrets and a prohibition on IoT Product Manufacturers and Related Service Providers' use of the in-scope data without an explicit contract with the user. Such data, generated by usage, is excluded from the protection of the *Sui Generis* rights under Directive 96/9/EC.	*For B2B interactions* Data holders legally obliged to make data available to data recipients are required to do so in compliance with detailed requirements. For instance, if EU rules mandate access to data, it is to be provided transparently with Fair, Reasonable and Non-Discriminatory (FRAND) terms, and non-exclusively. Data holders may apply appropriate technical and organisational protection measures where necessary, for instance for the protection of trade secrets. Data holders can also seek corrective measures in case such data is used to develop competing products.[3] Data holders can agree with data recipients about reasonable and non-discriminatory compensation for making data available, but the basis for the calculation must be specified**. Unfair contractual terms concerning data access unilaterally imposed by one enterprise on another shall be non-binding. The DA defines an unfair term as a term of "*such a nature that its use grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing.*" It also provides a grey and black list for unfair terms. If such non-binding terms can be separate from the rest of the contract, the separable part shall remain binding. *For B2G interactions** The Data Act also obligates Data Holders to make relevant data available to public sector bodies (PSBs) in cases of exceptional need. Such an exceptional need can be when the data is (a) necessary to respond to a public emergency or (b), only for non-personal data, where the lack of	DPSPs must enable customers to switch to another data processing service of the same type with another service provider, combination of providers, or on-premises services. They must not impose and, in fact must remove, commercial, technical, contractual and/or organisational barriers that prevent customers from, for instance, porting available data and assets and (for IaaS providers) maintaining functional equivalence.[4] They must specify the rights of customers concerning such switching in a written and reproduceable contract between the parties and provide information on available procedures for switching and porting data processing services. They must also implement technical measures in support, including establishing open interfaces where relevant and implementing compatibility with interoperability standards that still need to be drafted. The interoperability standards are also relevant for common European data space and smart contract service providers. Charges for such switching are to be gradually withdrawn, with no imposition of switching charges permitted from 12 January 2027. The Data Act also obliges DPSPs to prevent international transfers of or third-country governmental access to in-scope non-personal data held in the EU outside the EU, where such a transfer would conflict with

[3] This does not, however, extend to competing services.

[4] Data Act, Art. 2(14) defines functional equivalence as "*the maintenance of a minimum level of functionality in the environment of a new data processing service after the switching process, to such an extent that, in response to an input action by the user on core elements of the service, the destination service will deliver the same output at the same performance and with the same level of security, operational resilience and quality of service as the originating service at the time of termination of the contract*". Further clarification is also available in Recital 72-74.

	available data prevents the PSB from fulfilling a task in the public interest explicitly provided by law and the PSB has exhausted all other means to obtain such data.*	EU law or relevant national law. There are exceptions to this obligation, however, including, for instance, transfers based on international agreements such as a mutual legal assistance treaty.
Specifically for MSMEs		
*Micro and Small Enterprises are exempt from the requirements on making data accessible, unless (a) they have partner or linked enterprises[5] that do not qualify as Micro or Small Enterprises entities or (b) they are subcontracted to manufacture the device or provide the service in question. Micro- or small enterprises that scale up receive a one year grace period to bring their products and services into compliance.	**For B2B contexts where the data recipient is an MSME without a non-MSME partner or linked enterprise, the compensation for making data available cannot exceed the costs directly related to making the data available. *Micro and Small Enterprises entities are excluded from the application of the B2G provision regarding making data available in cases of exceptional need under option (b).	N/A.
For Users, Data Recipients and Customers		

[5] As per Annex Article 3 of the Annex to Recommendation 2003/361/EC,
"*2. 'Partner enterprises' are all enterprises which are not classified as linked enterprises within the meaning of paragraph 3 and between which there is the following relationship: an enterprise (upstream enterprise) holds, either solely or jointly with one or more linked enterprises within the meaning of paragraph 3, 25 % or more of the capital or voting rights of another enterprise (downstream enterprise).*

However, an enterprise may be ranked as autonomous, and thus as not having any partner enterprises, even if this 25 % threshold is reached or exceeded by the following investors, provided that those investors are not linked, within the meaning of paragraph 3, either individually or jointly to the enterprise in question:

- *a) public investment corporations, venture capital companies, individuals or groups of individuals with a regular venture capital investment activity who invest equity capital in unquoted businesses ('business angels'), provided the total investment of those business angels in the same enterprise is less than EUR 1 250 000;*
- *b) universities or non-profit research centres;*
- *c) institutional investors, including regional development funds;*
- *d) autonomous local authorities with an annual budget of less than EUR 10 million and fewer than 5 000 inhabitants.*

3. 'Linked enterprises' are enterprises which have any of the following relationships with each other:

- *a) an enterprise has a majority of the shareholders' or members' voting rights in another enterprise;*
- *b) an enterprise has the right to appoint or remove a majority of the members of the administrative, management or supervisory body of another enterprise;*
- *c) an enterprise has the right to exercise a dominant influence over another enterprise pursuant to a contract entered into with that enterprise or to a provision in its memorandum or articles of association;*
- *d) an enterprise, which is a shareholder in or member of another enterprise, controls alone, pursuant to an agreement with other shareholders in or members of that enterprise, a majority of shareholders' or members' voting rights in that enterprise.*

There is a presumption that no dominant influence exists if the investors listed in the second subparagraph of paragraph 2 are not involving themselves directly or indirectly in the management of the enterprise in question, without prejudice to their rights as stakeholders.

Enterprises having any of the relationships described in the first subparagraph through one or more other enterprises, or any one of the investors mentioned in paragraph 2, are also considered to be linked.

Enterprises which have one or other of such relationships through a natural person or group of natural persons acting jointly are also considered linked enterprises if they engage in their activity or in part of their activity in the same relevant market or in adjacent markets.

An 'adjacent market' is considered to be the market for a product or service situated directly upstream or downstream of the relevant market."

The Data Act aims to give Users more control over their data. Users (including business) receive a right to access their own data and even to share this data with or transfer it to third parties (as long as they're not gatekeepers). They also receive extensive protections, including the right to receive pre-contractual information about how their data will be processed and made accessible.	Data Recipients can expect gaining access to data to be easier as the Data Act is slowly implemented across the market. They can also expect their access to this data to be protected by law, for instance by being provided FRAND terms for this access.	Customers of DPSP services can expect switching between service providers to get easier and become more standardised as the Data Act becomes implemented more widely. They can also expect switching charges to first decrease and then be removed altogether.

1.4 How is it enforced?

The Data Act will be applied and enforced by authorities designated by the respective Member States. It is important to note that authorities already responsible under existing acts (such as the Autoriteit Persoonsgegevens (AP) under the GDPR) will retain their mandate – that is, the AP will continue to be the supervisor for the elements of the Data Act that govern personal data. The relevant authority for the Netherlands is yet to be designated. The penalties for its violations are also to be determined by the Member States, but are required to be 'effective, proportionate and dissuasive.' Users, data holders and data recipients can raise complaints with the competent authorities but are also required by the Data Act to have access to specialised dispute settlement bodies for relevant disputes. At the EU level, the European Data Innovation Board will support the consistent application of the Data Act.

1.5 What's next?

Crucially, the obligations created by the Data Act also create important rights for IoT Users and Data Recipients. The transparency and data access obligations for manufacturers and providers of related services, for instance, are also a right to transparency and data access for users. Users also receive the right to share such data with third parties, for instance for aftermarket repair service providers. How these rights and obligations are used in practice is important to keep track of.

As this relatively new legislation has only recently been adopted, we can expect quite a few updates in the coming periods. There is time to prepare for the Regulation until it starts applying from 12 September 2025. In the meantime, the first update to track would be the implementation of the Act into Dutch law. For instance, the designation of competent authorities and specification of the penalties are essential to keep track of.

Furthermore, the Data Act requires the Commission to develop and recommend non-binding model contractual terms on data access and use to assist parties in drafting contracts. The Commission is already working on developing such model terms. Such model clauses can assist parties in ensuring compliance with the Data Act. The Commission may also release open interface and interoperability standards for data spaces, data processing services, and smart contracts. These are also important to keep track of.

1.6 Further reading

WilmerHale, Details of the Data Act (1) – Access Rights and Obligations.
CiTiP, Data Act Series.
European Commission, Data Act – Questions and Answers.
European Commission, A Europe fit for the Digital Age.

2. Data Governance Act

Date Proposed	Date Adopted	Applicable from
November 2020	May 2022	September 2023

2.1 Whom does it apply to?

The Data Governance Act (DGA) follows in the footsteps of the Free Flow of Data Regulation (EU) 2018/1807 and the Open Data Directive (EU) 2019/1024 and addresses some of the remaining gaps in enabling the use of specific categories of protected data held by public organisations. The DGA mainly applies to public sector bodies, but also contains provisions relevant to data intermediation service providers and organisations engaged in data altruism.

Role	Definition
Public Sector Bodies (PSBs)	✓ Are you a state, regional, or local authority, such as a municipal organisation or a state associated utility company? ✓ And, are you governed by public law? ✓ Or, are you an association formed by a public authority? ➢ Then you may qualify as a Public Sector Body.
Data Intermediation Service Providers (DISPs)	✓ Do you provide a service that aims to enable data sharing between an undetermined number of data subjects, data holders and data users? ✓ And, do you aim to establish commercial relationships between these entities? ➢ Then you may qualify as a Data Intermediation Service Provider.
Data Altruism Organisations (DAOs)	✓ Does your organisation engage in the voluntary sharing of personal or non-personal data? ✓ And, does your organisation do so for objectives of general interest, provided by law? ✓ And, does your organisation do so at cost, without seeking compensation in addition to incurred costs (that is, as a non-profit organisation)? ➢ Then you may qualify as a Data Altruism Organisation.
Data Users	✓ Do you have a legal right to access certain personal or non-personal data, for instance from a PSB, a DISP, or a DAO? ✓ And, do you have a right to use that data for commercial or non-commercial purposes? ➢ Then you may qualify as a Data User. The obligations applicable to PSBs, DISPs and DAOs under the DGA may be good for you to know about.

Example

Consider, for instance, a fictional company, TellIsh, that offers a digital marketplace where participants can monetise and re-use non-personal data that they have a right to make available. TellIsh does not trade data itself but runs the platform that enables others to do so and develops and deploys tools to support such transactions. TellIsh, here, is likely to be a Data Intermediation Service Provider (DISP). Further examples of DISPs include data spaces and other orchestrators of data-sharing ecosystems, and data pools (established jointly by several legal or natural persons).
Consider a second fictional platform, VirusData, that allows its users to 'donate' anonymised data from their smart wearables. VirusData then makes this data available to researchers for free, to support them in identifying potential viral outbreaks before they are widespread. VirusData would then be likely to be a Data Altruism Organisation (DAO).
An individual or business utilising the services of TellIsh or Virus Data is likely to be a Data User.

2.2 Highlights per Role

Public Sector Bodies (PSBs)	Data Intermediation Service Providers (DISPs)	Data Altruism Organisations (DAOs)
The DGA does not obligate PSBs to allow the re-use of protected data. Rather, it gives a set of harmonised basic conditions under which such re-use of specific categories of protected data *might* be permitted for commercial or non-commercial purposes. This applies to data protected on the grounds of commercial confidentiality, statistical confidentiality, intellectual property rights protection, or personal data protection insofar as it is outside the scope of the GDPR. The DGA prohibits exclusive arrangements for the re-use of the in-scope data. It also requires the public availability of the conditions and procedure for allowing re-use, including through national and EU Single Information Points. Transfers to third countries that create a conflict with EU or national law are prohibited by the DGA as well, with some exceptions for instance in case of mutual legal assistance treaties or appropriate implementing acts.	DISPs must notify and register that they provide such a service to the relevant designated authority (for example, the ACM), establishing their compliance with the requirements of the DGA. They are subject to strict requirements aimed at guaranteeing their neutrality, for instance an obligation to not use the data they receive for purposes other than putting them at the disposal of a recipient and an obligation for data intermediation services to be provided through a separate legal person. Registered DISPS are allowed to use the label 'data intermediation services provider recognised in the Union' and a common logo. The restrictions on transfers to third countries apply to DISPs as well.	DAOs must also apply to be registered as providing such a service to the relevant designated authority (for example, the ACM), establishing their compliance with the requirements of the DGA. DAOs are subject to a variety of requirements and must implement specific safeguards to protect the rights and interests of data subjects and data holders. For instance, DAOs must operate on a non-profit basis and be legally independent from any entity that operates on a for-profit basis, and must carry out data altruism activities through a structure functionally separate from other activities. Registered DAOs can use the label 'data altruism organisation recognised in the Union' and use a common logo. Member States may create organisational or technical arrangements to facilitate data altruism. The Commission shall establish a Rulebook for facilitating data altruism, including technical, security and interoperability requirements and a standard European data altruism consent form. The restrictions on transfers to third countries apply to DAOs as well.

Specifically for MSMEs		
PSBs may charge fees for data re-use, but only to the extent of costs to make the data available, for instance in relation to the cost of reproducing, providing and disseminating the data. However, they may also offer data to MSMEs at discounted rates, or free of charge.	A subset explicitly included in the definition DISPs is 'Data Cooperatives', which refers data intermediation service offered by an organisational structure consisted of data subjects, ZZPers, or MSMEs. The main objective of this organisational structure should be to support its members in exercising their rights concerning specific data. Such Data Cooperatives are subject to the same requirements as other DISPs, and can potentially be quite helpful for MSMEs.	N/A.
For Users		
These provisions can be quite useful for entities that would like to obtain access to such protected data, for instance for research or AI training purposes.	Entities that rely on and utilise DISP services can, soon, expect to be able to check whether a company complies with the requirements of the DGA in the provisions of its services by checking for their registration, and the presence of the common label and logo.	For entities that would like to obtain access to data, for instance for research or AI training purposes, they can soon expect to be able to check for the existence of DAOs and the data they offer through the registers. They can also easily identify complying organisations with the presence of the common label and logo.

2.3 How is it enforced?

The DGA requires the designation of competent authorities by the Member States to assist PSBs in managing access to protected data and for monitoring DISPs and DAOs for compliance. In the Netherlands, the ACM will be designated as the supervisory authority and competent authority for DISPs and DAOs, with the Dutch DPA advising on the conditions of the regulation that relate to the protection of personal data.

The DGA also envisions the setup of a European Data Innovation Board to advise and assist the Commission in the continued implementation of the DGA. The Member States will also determine penalties for DISPs and DAOs. The Commission retains the power to adopt delegated acts, where deemed necessary, that lay down the criteria for, for instance, transfers to third countries or the Rulebook.

2.4 What's next?

You can track the progress of the DGA's implementation into Dutch law here. The reuse of protected categories of data encouraged by the DGA may be an opportunity for MSMEs that rely on data to access new types of data and consider new avenues of approach for their products and services. Establishing the Dutch National Information Point is pending and essential to keep track of. The European Commission shall also establish a European Single Access Point to be integrated into data.europa.eu.

While the DGA does not provide too much information about the functioning of Data Cooperatives, developments regarding the same may be worth keeping an eye out for. The registration requirements for DISPs and DAOs are also essential to track if they apply to you. The ACM has already called for DISs to register for the DGA. Finally, the Commission may also adopt model (but non-binding) contractual terms for transfers of data to third countries.

2.5 Further reading

Julie Baloup and Teodora Lalova-Spinks, CiTiP White Paper on the Data Governance Act
European Commission, Data Governance Act explained
ACM, Datadiensten

3. Digital Services Act

Date Proposed	Date Adopted	Applicable from
December 2020	October 2022	February 2024

3.1 Whom does it apply to?

The Digital Services Act (DSA) focuses on online content regulation and user protection. The DSA, among other things, adapts and supplements[6] rules for intermediary services providers – that is, rules about whether 'mere conduits', 'caching' or 'hosting' service providers are to be held liable for the legality of the data that goes through their infrastructure. These adaptations aim to address the challenges posed by digital platforms, and are aimed at ensuring a safer and more transparent online environment.

Role	Definition
Intermediary Service Provider (ISP)	✓ Do you allow your users to transmit information over a communication network as part of your service? ✓ Or, do you provide your users with access to a communication network as part of your service? ➢ Then you may qualify as a 'mere conduit' service provider. ✓ Do you allow automatic, intermediate and temporary storage of transmitted information as part of your service? ✓ And, do you do so for the sole purpose of making the transmission more efficient or more secure? ➢ Then you may qualify as a 'caching' service provider. ✓ Do you allow your users to store information as part of your service? ➢ Then you may qualify as a 'hosting' service provider. ➢ If you provide 'mere conduit', 'caching' or 'hosting' services, you may qualify as an intermediary service provider.
Online Platforms	✓ Do you qualify as a Hosting Service Provider? ✓ And, do you allow your service recipients to disseminate information to the public as part of your service? ✓ Is such dissemination **not** an or purely ancillary feature? ➢ Then you may qualify as an Online Platform Provider.
Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs)	➢ A subset of Online Platforms that meet specific criteria, including having more than 45 million average active monthly users in the EU, are designated as Very Large Online Platforms (VLOPs) or Very Large Online Search Engines Very Large Online Search Engines (VLOSEs) by the European Commission. 19 organisations have been designated as such so far.

[6] Articles 12 to 15 of the eCommerce Directive are deleted, and references to Articles 12 to 15 are to be construed as references to Articles 4,5,6 and 8 of the DSA respectively. All other rules of the eCommerce Directive remain valid. The Dutch implementation of the eCommerce Directive is available here.

Consumer	✓ Do you use the services of an ISP or an OP, outside your trade, business, craft or profession? ➢ Then you may qualify as a Consumer.
Trader	✓ Do you use the services of an ISP or an OP, for professional purposes, that is, for purposes related to your trade, business, craft or profession? ➢ Then you may qualify as a Trader.

Example

Consider, for instance, a fictional internet access service provider, AT&Viggo. AT&Viggo only provides its clients with a connection to the internet. AT&Viggo is, in this case, is likely to qualify as a 'mere conduit' Intermediary Service Provider (ISP). Further examples of 'mere conduit' ISPs can include Internet Exchange Points (IXPs) and Virtual Private Networks (VPNs).

Consider a second fictional company, Cloudly. Cloudly provides a Content Distribution Network (CDN) service – that is, it provides a geographically distributed network of proxy servers and data centres which (temporarily) store content such as video content which is requested individually my multiple users, in order to make it available to users more quickly. Cloudly, in this case, is likely to qualify as a 'caching' Internet Service Provider.

Consider, finally, a third fictional social-media start-up called YourSpace. YourSpace allow its users to store notes and files on their account, but these are only visible to the users themselves. YourSpace is likely to be considered a 'hosting' Intermediary Service Provider (ISP), or a Hosting Service Provider (HSP). Further examples of 'hosting' services include cloud computing, web hosting, and paid referencing services. Apple, for instance, provides hosting services for iCloud users.

Let's say that YourSpace expands its offerings to also allow its users to share the notes and other files linked with their account to other users and to the public. YourSpace will then be likely to qualify as an Online Platform (OP). Further examples of Online Platforms include social media, content-sharing, and streaming platforms such as Facebook, Instagram and YouTube.

A YourSpace user who only uses it for their personal communications would be likely to qualify as a Consumer, while a YourSpace user who, for instance, provides advertisements for their business on the platform is likely to qualify as a Trader.

3.2 Highlights per Role

The DSA retains the safe harbour rules with some modifications, and also adds additional protection for 'voluntary own-initiative investigations'. It also introduces a variety of new obligations in a 'tiered' system – all obligations of the lower tiers apply to the higher tiers as well, but not vice-versa.

All Intermediary Service Providers (ISPs)	Hosting Service Providers (HSPs)
All ISPs offering their services in the EU must designate a single point of contact, such as an e-mail contact, phone number, electronic contact form or chatbot, for authorities and recipients of their service respectively and make this information easily accessible.[7] A legal representative must be designated in writing for ISPs that do not have an establishment in the EU but do offer services in it. ISPs must also comply with detailed provisions regarding their Terms and Conditions, including transparency requirements and requirements about enforcing content restrictions. They must release regular (at least annual) public	HSPs must implement easy-to-access, user-friendly Notice-and-Action mechanisms to allow anyone to notify the HSP of information hosted by it that they consider illegal via sufficiently precise and adequately substantiated notices. Receiving such a notice may mean that the HSP can no longer claim to not have knowledge of such information. They must take timely and diligent action on such notices and notify relevant parties, including, if necessary, law enforcement authorities. Note: Per the tiered nature of the DSA, these provisions are also applicable to Online Platforms.

[7] See Recital 43 and 44 of the DSA.

reports about the content moderation actions they undertake.* Note: Per the tiered nature of the DSA, these provisions are also applicable to Hosting Service Providers and Online Platforms.	
Specifically for MSMEs	
* Micro and Small Enterprises are exempt from the annual content moderation reports requirement for ISPs as long as they are not VLOPs.	N/A.
For Consumers and Traders	
Users (that is, both Consumers and Traders) of all ISPs can expect increased transparency and contact accessibility from all complying ISPs. They can also, crucially, seek compensation for any loss suffered due to an infringement of the DSA by an ISP.	Users of Hosting Providers can expect filing complaints about potentially illegal content to get easier and more usable. They can also expect to receive clear information about restrictions imposed on their usage of the service and related information, such as out-of-court dispute settlement.
Online Platforms (OPs)	**Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs)**
OPs must implement an effective, easy-to-access, user-friendly, internal complaint-handling system, and must also ensure that they have qualified staff to judge the complaints. OPs must prioritise notices submitted by specifically recognised 'trusted flaggers', a new concept introduced by the DSA. They are also required take steps to counter abuses of such systems. Disputes can also be escalated to any appropriately certified out-of-court dispute settlement bodies. OPs are also obligated to follow reporting obligations, for instance about the number of disputes submitted to out-of-court dispute settlement bodies, are prohibited from using dark patterns, and must implement appropriate measures to ensure the safety of minors. If the OP presents advertisements or uses recommender systems[8], they must comply with additional obligations such as transparency about why an ad or recommendation is presented to a user and how to change the relevant parameters. OPs enabling distance contracts are further required to establish the traceability of traders before allowing them to trade on their platforms, including for instance a self-certification to only offer products or services that comply with applicable EU law. When a provider becomes aware of an illegal product or service offered through its services, it must remove them and inform consumers and relevant authorities accordingly. They must also design their interfaces in such a way as to encourage compliance by design, for instance by enabling traders to comply with their obligations regarding pre-contractual information.	Providers of VLOPs and VLOSEs must perform (at least annually) systematic risk assessments and implement reasonable, proportionate and effective risk mitigation measures tailored to the identified risks. VLOPs and VLOSEs must conduct independent compliance audits (at least annually) and implement an internal compliance function. They must also comply with additional provisions for transparency in advertising, recommender systems, and reporting, comply with crisis response requirements, data access and scrutiny, and paying a supervisory fee.

[8] DSA, Art. 3(s), defines a recommender system as "*a fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service or prioritise that information, including as a result of a search initiated by the recipient of the service or otherwise determining the relative order or prominence of information displayed*"

Specifically for MSMEs	
*Micro and Small Enterprises are exempt from most of the provisions applicable to OPs, with some exceptions such as the transparency obligations with respect to the Digital Services Coordinator, unless they qualify as VLOPs. In case a micro- or small enterprise scales up, they receive a 12 month grace period to comply.	N/A.
For Consumers and Traders	
Users can, therefore, expect an easier and more effective process for filing complaints against potentially illegal content online, though they can also expect to be penalised for misusing such systems. They can also expect the complaints process to include non-judicial options such as arbitration and mediation, making the process potentially less expensive and time-taking. At the same time, they can also expect more transparency about decisions taken based on their requests, and more transparency and control on advertisements and recommendations made by platforms. Traders specifically can also expect more scrutiny in their participation on online platforms that enable distance contracts.	Users can expect more responsibilities for VLOPs and VLOSEs, including more careful management of potential social risks. They can also expect more transparency from such companies, and more third-party scrutiny of their available reports through independent auditors and researchers.

3.3 How is it enforced?

Member States are required to designate national **Digital Services Coordinators (DSCs)** who shall be responsible for the supervision and enforcement of the DSA within that Member State (including registering trusted flaggers). DSCs are required to provide mutual assistance and cross-border cooperation. In the Netherlands, the ACM has been appointed as the DSC and as the supervisor for most of the DSA, with the Dutch DPA being appointed as the supervisor for the prohibitions on profiling for showing advertisements on online platforms. The subset of obligations relevant to VLOPs and VLOSEs will be supervised and enforced by the Commission itself.

For Micro and Small Enterprises that scale up and no longer qualify as Micro and Small Enterprises, the DSA provides a 12 month window to bring themselves into compliance with its provisions. During this 12 month period, the obligations of the DSA will not apply.

The penalties for violations of the DSA are to be specified by Member States. The maximum amount for fines for failure to comply with an obligation is 6% of the annual worldwide turnover of the intermediary service provider in the preceding financial year, and for supplying incorrect, incomplete or misleading information is 1% of the same.

3.4 What's next?

The Commission may also encourage and facilitate voluntary standards, codes of conduct and crisis protocols for compliance with the various requirements of the DSA and for online advertising and accessibility. Such standards are likely to be developed by ETSI, CEN, and CENELEC. National standards might simultaneously be developed by NEN as well. These developments are worth keeping an eye out for.

3.5 Further reading

European Commission, Questions and Answers – Digital Services Act
ACM, Online diensten aanbeiden
Overheid.nl, Uitvoeringswet digitaledienstenverordening
European Commission, Digital Markets Act (DMA) Legislation (including templates)

4. Digital Markets Act

Date Proposed	Date Adopted	Applicable from
December 2020	September 2022	May 2023

4.1 Whom does it apply to?

Tailored to foster fair competition and curb anti-competitive practices, the Digital Markets Act (DMA) sets the stage for a more level playing field within a digital ecosystem dominated by gatekeepers. It regulates companies that provide at least one of the so-called 'Core Platform Services' (CPSs) to a large number of end users in the EU. While the obligations under the DMA are mainly applicable to such specifically designated 'Gatekeepers', they may create significant opportunities for MSMEs.

Role	Definition
Gatekeepers	Gatekeepers are providers of Core Platform Services (CPSs) that have a significant impact on the EU market and enjoy (or will enjoy) an entrenched and durable position in the market. Gatekeepers are to be specifically designated as such by the Commission. The Commission designated six companies as Gatekeepers in September 2023: Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft. The designation of specific CPSs is still ongoing.
Business Users	✓ Do you use a CPS provided by a designated Gatekeeper? ✓ And, do you use it in a professional or commercial capacity? ✓ That is, do you use it in the course of providing or to provide goods or services to end users? ➢ Then you may qualify as a Business User.
End User	✓ Do you use a CPS provided by a designated Gatekeeper? ✓ And, are you **not** a business user? ➢ Then you may qualify as an End User.

Example

To continue our previous example of YourSpace, consider that YourSpace also makes available an app through the Google Play app store, a designated Core Platform Service (CPS) provided by a Gatekeeper. YourSpace, in this case, is likely to be a Business User. Simon, the CFO of YourSpace, also uses the Google Play app store on his Android smartphone to download apps for personal use, for instance to chat with his family or monitor his exercise. Simon, in this context, is likely to be an End User.

4.2 Highlights per Role

Gatekeepers and End Users	Gatekeepers and Business Users (including MSMEs)
Gatekeepers shall allow and enable end-users to easily uninstall any software on the gatekeeper's OS, unless essential for its functioning. End users shall also be entitled to easily change default settings that prompt them to the	The DMA implements a variety of provisions to create a level playing field for business users with a Gatekeeper's CPS. These provisions create quite a few useful rights for

gatekeeper's products or services. Gatekeepers are required to allow and enable the use of third-party software or app stores on its OS and CPSs, including setting them as default. Gatekeepers are prohibited from treating their own services more favourably when ranking or indexing and must conduct such ranking on FRAND terms. End users should be able to switch between and subscribe to different software accessed using the Gatekeeper's CPS, and will be provided the option to port their data free of charge and effectively, including real-time access. End users can, therefore, expect less unfair practices in the digital market, and potentially more innovative services and choices. They can also expect better interoperability among services and CPSs, more control over their usage of CPSs.	business users who use their CPSs, and can be especially useful for MSMEs. For instance: • The DMA requires gatekeepers to provide advertisers and publishers with detailed information about their advertising upon request free of charge, including the price and fees paid and the metrics used to calculate the price and fees. Advertisers and publishers are also allowed to request access to the gatekeeper's performance measuring tools and relevant data upon request, free of charge, so that they can carry out independent verification. • Gatekeepers cannot prevent business users from offering the same products or service to end users through alternative sales channels (third party or own) at prices or conditions different from those provided through the services of the gatekeepers. • Gatekeepers must also provide third-party online search engines with access to search query data on FRAND terms. • Business users should be allowed to communicate and promote offers to end users via the Gatekeeper's CPS or other channels, including under different conditions. • Gatekeepers shall allow other providers of services and hardware interoperability with its CPS as are available to itself. • Content purchased by end users from business users should be made accessible on the Gatekeeper's CPS even if the end-user did not acquire the content through the CPS. • Gatekeepers cannot impose their own identification services, web browser engines, payment services, etc. on their business users or end users. • Gatekeepers cannot require business users or end users to register or subscribe to one CPS to be able to use other CPSs. • Gatekeepers must provide access to their app stores, search engines and social networking services to business users on FRAND terms. • Gatekeepers are prohibited from using data that is not publicly available and is generated by business users' use of the relevant CPSs in competition with business users. • Business users are also to be offered high-quality, continuous and real-time access to their data on the CPS free of charge, upon request. • Basic functionalities of number-independent interpersonal communication services listed as CPSs are to be made interoperable with the services of other similar service providers.

4.3 How is it enforced?

The supervision and enforcement of the DMA is to be managed by the European Commission, though it may also initiate actions based on reports submitted by ACM. There is also room for third parties, including business users, competitors, or end-users, to bring complaints against gatekeepers directly to the ACM or the Commission.

4.4 What's next?

While the DMA's obligations are mainly on Gatekeepers, the level playing field it aims to create can be significant for MSMEs, especially if they utilise a Gatekeeper's CPS. For instance, the requirement on Gatekeepers to provide access to their app stores, to their CPSs, to allow interoperability to business users can be a substantial benefit for MSMEs. Similarly, the transparency requirements for advertisements can allow MSMEs to verify the effectiveness and costs of their advertising campaigns. A draft of the Dutch implementing act for the DMA is available here.

4.5 Further reading

European Commission, Digital Markets Act: Ensuring fair and open digital markets
Overheid.nl, Uitvoeringswet digitalemarktenverordening (Digital Markets Act)

5. Conclusions

This document has provided a high-level summary of four pivotal legislations: the Data Act, the Data Governance Act, the Digital Services Act, and the Digital Markets Act. These legislations represent a significant step forward in regulating the rapidly evolving digital market within the European Union. These are wide-ranging and interconnected legislations, and they create a complex web of obligations for a diverse set of actors participating in the digital market. Correspondingly, they also create a variety of new rights, presenting a transformative opportunity for various players in the digital ecosystem, especially MSMEs.

It is important to acknowledge that these legislations are still relatively new. As time progresses and these legislations are implemented, their true impact on the digital market in the EU will become clearer. It is therefore important to keep an eye out for further developments in these regulations and their application, including checking the implementation acts for the Netherlands where they are still pending.

To navigate this changing regulatory landscape effectively, MSMEs must determine which provisions apply to them, by identifying the roles they or other entities in their network fit into. This will help them understand not just the obligations they must comply with under the law, but also to recognize the rights they may be able to assert and claim, thereby harnessing the opportunities emerging from these legislations. One of the objectives of the vision for Europe's Digital Decade is to assist MSMEs, making it important to take advantage of the opportunities created by the legislations.

In conclusion, the EU's commitment to shaping a fair, competitive, and responsible digital landscape is evident through these legislations. As they are implemented into practice, we can anticipate their influence on digital businesses, data management practices, and market dynamics to become increasingly significant, ultimately shaping the digital landscape in the European Union, and even beyond, for years to come.

6. Glossary

DA	Data Act
DGA	Data Governance Act
DSA	Digital Services Act
DMA	Digital Markets Act
GDPR	General Data Protection Regulation
MSEs	Micro and Small Enterprises
MSMEs	Micro, Small and Medium Enterprises
AP	Autoriteit Persoonsgegevens
DPSPs	Data Processing Service Providers
FRAND	Fair, Reasonable and Non-discriminatory
PSBs	Public Sector Bodies
DISPs	Data Intermediation Service Providers
DAOs	Data Altruism Organisations
ISPs	Intermediary Service Providers
HSPs	Hosting Service Providers
OPs	Online Platform Providers
VLOPs	Very Large Online Platforms
VLOSEs	Very Large Online Search Engines
DSCs	Digital Service Coordinators
CPS	Core Platform Service

ICT, Strategy & Policy

www.tno.nl

TNO innovation for life