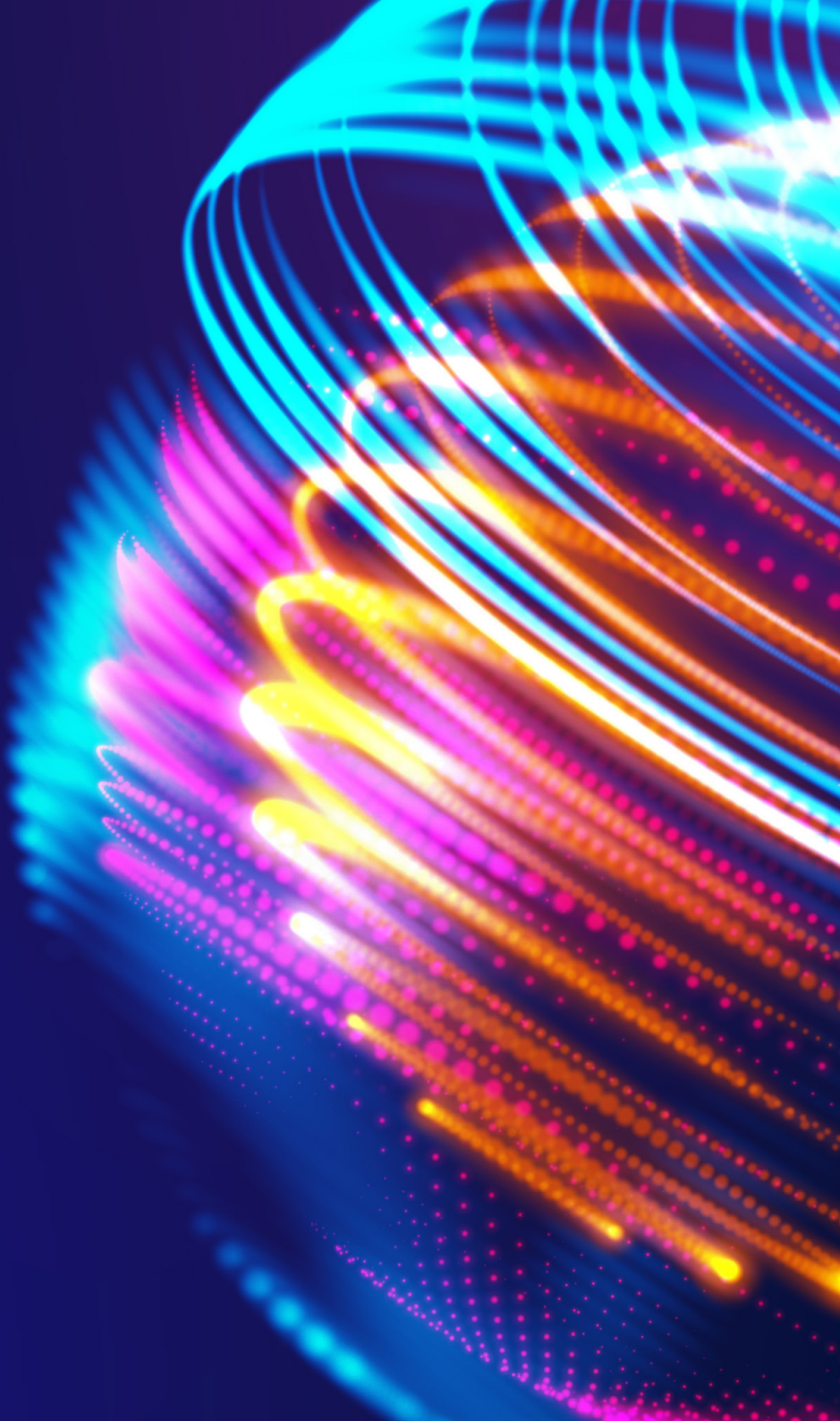
SQUIRE PATTON BOGGS

Local Connections. Global Influence.

Preparing for 2023 and Beyond

EU Digital Markets and Services Regulations



Introduction

The EU has adopted two new regulations for digital services and markets in the EEA:

- **The Digital Markets Act (DMA)**, which comes into force on 1 November 2022 and establishes a list of do's and don'ts that Big Tech companies and their trading partners will need to implement by mid-2023 in their daily operations to ensure fair and open digital markets.
- **The Digital Services Act (DSA)**, which comes into force on 16 November 2022 and establishes a list of do's and don'ts that most online intermediation companies and their trading partners will need to implement by mid-2024 in their daily operations to create a safer digital space and content moderation.

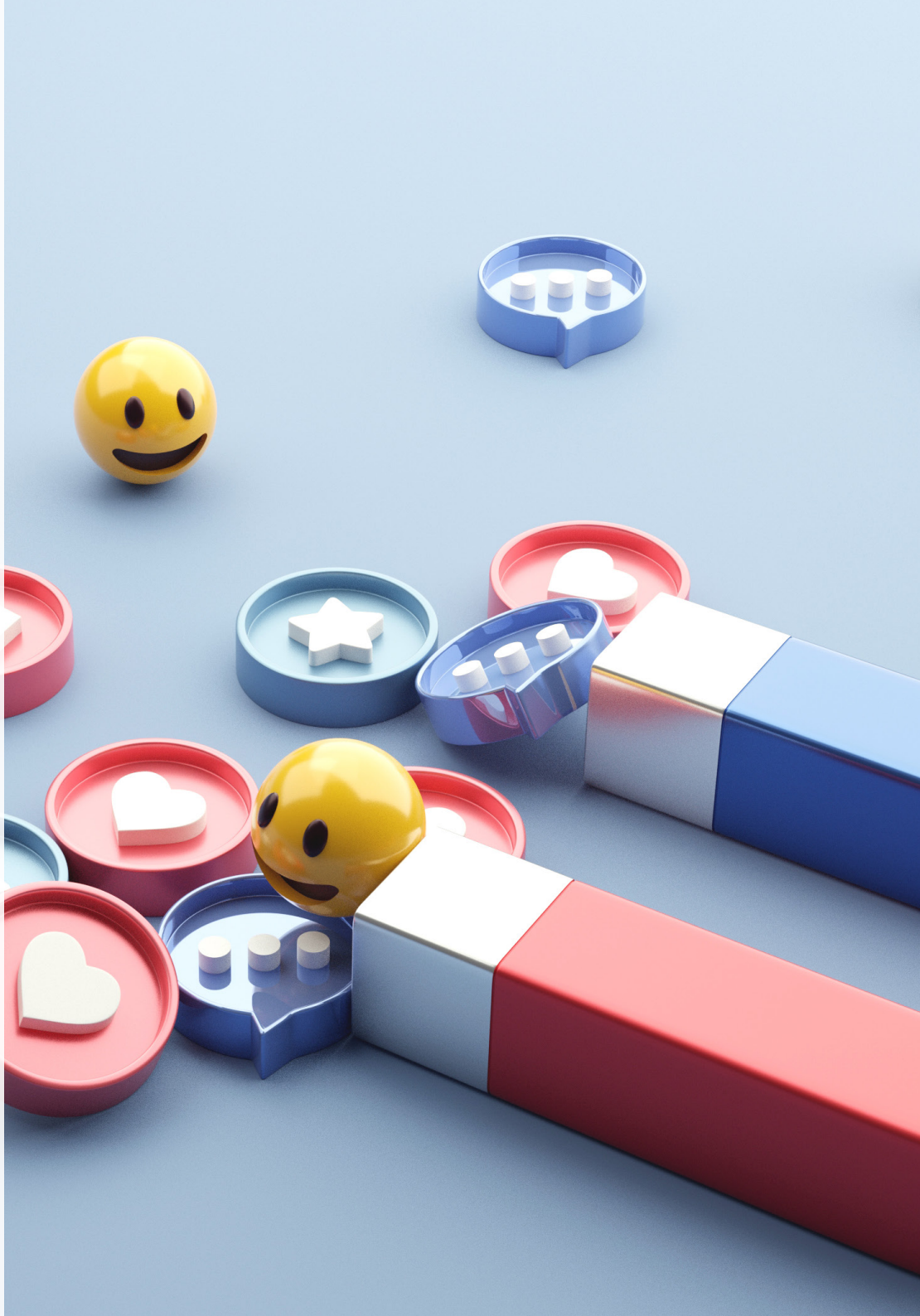
DMA – Who Does it Apply to?

The DMA applies to entities designated as "gatekeepers", which includes providers of "core platform services", such as:

- Online intermediation services,
- Online search engines,
- Online social networking services,
- Video-sharing platform services,
- Number-independent interpersonal communication services ("NI-ICS") – as defined in the EU Electronic Communications Code,
- Operating systems,
- Web browsers,
- Virtual assistants,
- Cloud computing services,
- Any online advertising services provided by a provider of the services listed above

A provider of a core platform service will only be designated as a gatekeeper under the DMA if it meets the following criteria:

- It has a significant impact on the internal market
  - This condition is presumed if the provider has had an EU turnover of €7.5 billion in the previous three financial years, or a market capitalisation of €75 billion in the previous financial year, and it provides its core platform service in at least three Member States
- Its core platform service constitutes an important gateway for business users to reach end users
  - This condition is presumed if the provider's core platform service has had, in the previous financial year, on average, 45 million monthly active end users and 10,000 yearly active business users in the EU
- It enjoys an entrenched and durable position in its operations, or it is foreseeable that it will do so in the near future
  - This condition is presumed where the thresholds relating to the number of users above have been met in the previous three financial years



DMA – Overview of Obligations

The DMA imposes a number of obligations on gatekeepers aimed at ensuring fair competition in digital markets and prohibiting digital business practices which are deemed unfair.

The main obligations imposed by the DMA on gatekeepers are rooted in EU competition law, in that they aim to ensure that gatekeepers cannot exploit the entrenched position of their core platform services in the internal market to the detriment of business users (i.e. persons acting in a commercial or professional capacity using core platform services in the course of providing goods or services to end users) and end users (i.e. any other users).

In particular, the DMA imposes obligations on gatekeepers related to:

- **Self-preferencing** – Preventing gatekeepers from using the entrenched position of their core platform services in the internal market to favour their other services against those of business users.
- **Access to Data and Services** – Regulating the availability and terms on which gatekeepers provide their services and access to the data they collect.
- **Restrictions on Users** – Preventing gatekeepers from restricting the ability of business users to deal with end users.
- **Advertising Transparency** – Regulating the terms on which the gatekeepers provide their services to advertisers and publishers.
- **Personal Data Protection** – Regulating the processing and use of end users' data by gatekeepers.
- **Interoperability** – Concerning the ability of business users to demand that their services be able to interact with those of the gatekeepers. The DMA also imposes interoperability obligations on gatekeepers which provide NI-ICS.

These obligations are divided in two types. The obligations contained in Article 6 are subject to further specification, meaning that the European Commission, following a dialogue with the gatekeeper concerned, can determine whether it complies with the relevant obligation and, if not, specify, within six months, the measures that the gatekeeper should adopt in order to comply. The obligations in Article 5 are not subject to this procedure and apply directly.

DMA – Self-preferencing Obligations

Article	Obligation	Direct Application*
5.7	Do not require users to use your identification service, web browser engine or payment service for services provided by business users using your core platform service.	✓
5.8	Do not require users to subscribe or register with any other core platform services to be able to use, access, sign up or register with your core platform service.	✓
6.1	Do not use, in competition with business users, any data which is not publicly available and is generated or provided by those business users, or their end users, by using your core platform service, including click, search, view and voice data.	X
6.5	Do not treat, in terms of ranking, your services and products more favourably than similar services or products of a third party. Do apply transparent, fair and non-discriminatory conditions to such ranking.	X
6.6	Do not restrict the ability of end users to switch between, and subscribe to, different software applications and services accessed using your core platform service, including as regards the choice of Internet access services for end users.	X

DMA – Access to Data and Services Obligations

Article	Obligation	Direct Application
6.10	Do provide business users at their request, free of charge, with access to, and use of, data that is provided or generated by those business users or their end users using your core platform service. If that data is personal data, do provide those business users with access and use of the data only where it is directly connected with the use made by the end users of the products or services offered by the business user through your core platform service, and subject to the end users' consent.	X
6.11	Do provide any third party providing online search engines, at their request, with access on fair, reasonable and non discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on your online search engines.	X
6.12	Do apply fair, reasonable and non-discriminatory general conditions of access for business users to your software application stores, online search engines and online social networking services. Do publish general conditions of access, including an alternative dispute settlement mechanism.	X
6.13	Do not apply general conditions for terminating the provision of your core platform service which are disproportionate. Do ensure that such conditions of termination can be exercised without undue difficulty.	X

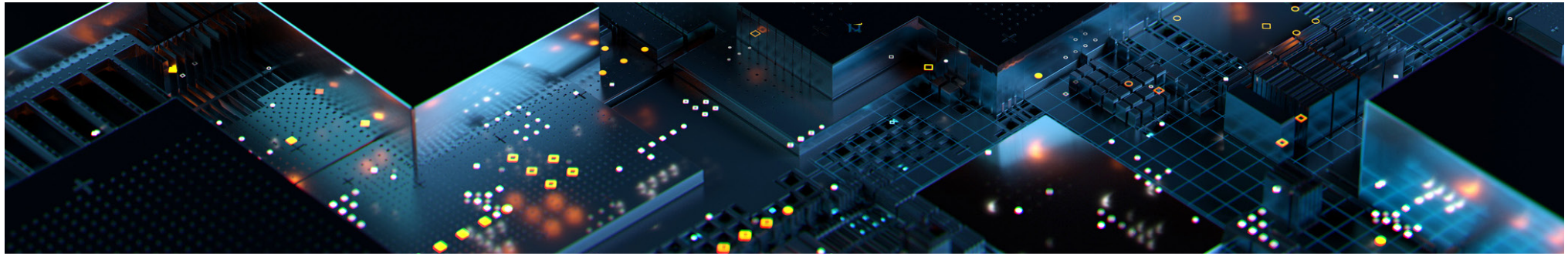
*A tick indicates that the obligation applies directly. A cross indicates that the obligation is subject to further specification by the European Commission following regulatory dialogue with gatekeepers.

DMA – Restrictions on Users Obligations

Article	Obligation	Direct Application
5.3	Do not prevent business users from offering the same products or services to end users through third-party online intermediation services, or their own online sales channel, at prices or conditions that are different from those offered through your core platform service.	✓
5.4	Do allow business users to promote offers to end users acquired via your core platform service or other channels, and to conclude contracts with these end users regardless of whether they use your core platform service.	✓
5.5	Do allow end users to access and use, through your core platform service, content, subscriptions, features or other items, by using the software application of business users, including where the end users acquired these items from the business users without using your core platform service.	✓
5.6	Do not prevent users from raising issues of non-compliance with EU or national law related to any of your practices with any relevant public authority, including national courts.	✓

DMA – Advertising Transparency Obligations

Article	Obligation	Direct Application
5.9	Do provide advertisers with daily, free of charge information concerning each of their advertisements, regarding the price and fees paid by them, the remuneration received by the publisher, and how those prices, fees and remuneration are calculated.	✓
5.10	Do provide publishers with daily, free-of-charge information concerning each advertisement displayed on their inventory, regarding the remuneration received and the fees paid by the publisher, the price paid by the advertiser, and how those prices and remuneration are calculated.	✓
6.8	Do provide advertisers and publishers, upon their request and free of charge, with access to your performance measures tools and data necessary for advertisers and publishers to carry out their independent verification of the advertisements inventory. Do provide such data in a manner that enables advertisers and publishers to run their own verification and measurement tools to assess the performance of your core platform service.	X



DMA – Personal Data Protection Obligations

Article	Obligation	Direct Application
5.2(a)	Do not process the personal data of end users, using third-party services which use your core platform service, for the purpose of providing online advertising services; unless the end user is presented with a specific choice and consents pursuant to the General Data Protection Regulation ("GDPR").	✓
5.2(b)	Do not combine personal data from your core platform service with personal data from any of your other services, or with personal data from third-party services.	✓
5.2(c)	Do not cross-use personal data from your core platform service with personal data from any of your other services and *vice versa*.	✓
5.2(d)	Do not sign in end users to any of your other services in order to combine personal data.	✓
6.9	Do provide end users, at their request and free of charge, with effective portability of data provided or generated by those end users through their use of your core platform service, including providing, free of charge, tools to facilitate the effective exercise of data portability and access to such data.	X

DMA – General Interoperability Obligations

Article	Obligation	Direct Application
6.2	Do allow end users to easily uninstall any software applications on your operating system; Unless the software applications are essential for the functioning of your operating system or of the device and cannot technically be offered on a standalone basis by a third party.	X
6.3	Do allow end users to easily change default settings on your operating system, virtual assistant and web browser that direct or steer them to your products or services.	X
6.4	Do allow users to install and use third-party software applications or software application stores using, or interoperating with, your operating system, and allow users to access them by means other than your core platform service; unless your measures are necessary to ensure that third-party software applications or software application stores do not endanger the integrity of your hardware or operating system. Do not prevent the downloaded third-party software applications or software application stores from prompting end users to decide whether they want to set it as their default; unless your settings (other than default settings) enable users to effectively protect security in relation to third-party software applications or software application stores.	X
6.7	Do allow providers of services and hardware, free of charge, effective interoperability with, and access to, the same hardware and software features accessed or controlled via your operating system or virtual assistant as are available to the services and hardware you provide. Do allow business users and alternative providers of services provided together or in support of your core platform service, free of charge, access to, and effective interoperability with, the same operating system and hardware or software features as you have available or use when providing such services; Unless your measures are strictly necessary and proportionate to ensure that interoperability does not compromise the integrity of your operating system, virtual assistant and hardware or software features.	X

DMA – Interoperability Obligations for Providers of NI-ICS

The DMA also imposes interoperability obligations specific to providers of NI-ICS, which is defined under the EU Electronic Communications Code as comprising emails, voice over the Internet, instant messaging, cloud communications and other Over The Top communications that do not connect with telephone numbers.

A gatekeeper must make the basic functionalities of its NI-ICS interoperable with the NI-ICS of other providers offering, or intending to offer, such services in the EU, by providing, free of charge, the necessary technical interfaces or similar solutions that facilitate interoperability.

These basic functionalities include:

- End-to-end text messaging between two individual end users, and within groups of individual end users
- Sharing of images, voice messages, videos and other attached files in end-to-end communication between two individual end users, and between a group chat and an individual end user
- End-to-end voice calls between two individual end users, and between a group chat and an individual end user
- End-to-end video calls between two individual end users, and between a group chat and an individual end user

This obligation is subject to the following two provisos:

- The gatekeeper is only required to collect and exchange, with the provider of NI-ICS that makes the request for interoperability, personal data of end users which is strictly necessary to provide effective interoperability, and subject to compliance with the GDPR
- The gatekeeper can take measures to ensure that third-party providers of NI-ICS requesting interoperability do not endanger the integrity, security and privacy of its services, if they are strictly necessary, proportionate and duly justified

Compliance with this interoperability obligation is likely to require product changes on the part of providers of NI-ICS.

DMA – Other Obligations

In addition to specifying those obligations to which gatekeepers are subject, the DMA includes a number of other important features which are relevant to gatekeepers:

- Gatekeepers must, within six months of their designation, provide the European Commission with a report describing the measures they have implemented to ensure compliance with those obligations
- Gatekeepers must, within six months of their designation, submit to the European Commission an independently audited description of any techniques for profiling of consumers that they apply to or across their core platform services
- Gatekeepers may, in circumstances where a specific obligation in relation to their core platform services would endanger, due to exceptional circumstances beyond their control, the economic viability of their operations in the EU, apply to the European Commission to suspend, in whole or in part, that obligation
- Gatekeepers may, on grounds of public health or public security, apply to the European Commission to exempt them, in whole or in part, from a specific obligation in relation to their core platform services
- Gatekeepers must inform the European Commission of any concentration where the merging entities or the target of the concentration provide core platform services or any other services in the digital sector or enable the collection of data
- Gatekeepers must introduce a compliance function, which is independent from their operational functions, and composed of one or more compliance officers, including the head of the compliance function

DMA – Enforcement

The European Commission will be solely responsible for enforcing the DMA and it has announced that this function will be conducted primarily by the Directorate for Competition (DG COMP) and the Directorate for Communications Networks, Content and Technology (DG CONNECT). The role of national competition authorities will be limited to assisting the European Commission in its enforcement functions.

The European Commission may exercise various investigative powers, similar to those it already has under EU competition law, with additional powers to be specified in a further regulation implementing the DMA:

- requesting that companies provide all necessary information, including any data and algorithms and information about testing
- interviewing any person, with their consent, for the purpose of collecting information
- conducting inspections of companies, which includes entering premises, examining and copying accounts, requiring explanations on algorithms, data-handling and business practices, sealing premises and requiring explanations on any document from the companies' staff

The European Commission may impose the following penalties on non-compliant gatekeepers:

- a fine of up to 10% of annual worldwide turnover for a first infringement
- fines of up to 20% of annual worldwide turnover for repeated infringements

Moreover, the European Commission will be able to impose:

- in cases of serious and irreparable damage, interim measures
- in cases of systemic non-compliance, behavioural or structural remedies

Furthermore, the direct application of the obligations in Article 5 of the DMA (which are not subject to further specification by the European Commission) could lead to enforcement through the national courts of Member States.

In practice, the EU has stated that Big Tech companies that are likely to be designated as gatekeepers by the European Commission should submit draft notification forms before the formal designation process begins, in order to enable meaningful pre-notification talks. Regulatory dialogue of this kind with gatekeepers is also likely to generate opportunities for complainants to act informally in the future.

DSA – Who Does it Apply to?

The DSA complements the DMA and applies to providers of "intermediary services", such as providers of:

- "Mere conduit" services, which consist of the transmission in a communication network of information provided by the recipient of said service, or the provision of access to a communication network
- "Caching" services, which consist of the transmission in a communication network of information provided by the recipient of said service, involving the temporary storage of that information, in order to make more efficient the information's onward transmission to other recipients upon their request
- "Hosting" services, which consist of the storage of information provided by, and at the request of, the recipient of such service

DSA – Categories of Intermediary Services

The DSA defines certain categories of providers of "intermediary services", in order to determine the obligations to which they are subject:

- Providers of "online platforms", which are hosting services that, at the request of a recipient of the services, store and disseminate information to the public
- Providers of online platforms that allow consumers to conclude distance contracts with traders
- Providers of "online search engines", which are providers of intermediary services that allow users to input queries in order to perform searches of all websites
- Providers of "very large online platforms", which are online platforms with at least 45 million average monthly active recipients of services and that have been designated by the European Commission
- Providers of "very large online search engines", which are online search engines with at least 45 million average monthly active recipients of services and that have been designated by the European Commission

DSA – Obligations on Providers of Intermediary Services

Article	Obligation	Further Specification
14	Do include in your terms and conditions information on any restrictions concerning the use of your service and information provided by the recipients.	Information includes policies, procedures, measures and tools used for content moderation, including algorithmic decision-making, human review and rules of procedure of the internal complaint handling system.
15	Do make publicly available, at least once a year, reports on any content moderation engaged in during the relevant period.	Reports include information on the number of orders to act against illegal content and to provide information received from national authorities, content moderation engaged in at your own initiative, the number of complaints received through your internal complaint-handling system and the use of automated means for content moderation.

DSA – Further Obligations on Providers of Hosting Services, Including Online Platforms

Article	Obligation	Further Specification
16	Do put mechanisms in place to allow the notification of specific items of information that the recipient considers to be illegal content.	Mechanisms must allow the recipient to notify an explanation of why the information is illegal, an indication of the information's electronic location, the recipient's name and email address and a statement confirming the belief that the notification is accurate and complete.
17	Do provide a statement of reasons to any affected recipients for restrictions imposed on the ground that the information provided by the recipient is illegal content or incompatible with your terms and conditions.	The statement of reasons must contain information on what the decision entails for the information (e.g. removal, demotion or suspension), its territorial scope and its duration, the facts and circumstances relied upon, the use of automated means in taking it, a reference to the legal or contractual ground relied upon and information on the possibilities for redress available to the recipient.
18	Do inform law enforcement or judicial authorities if you become aware of any information giving rise to suspicion of a criminal offence involving a threat to the life or safety of a person.	Notification must be made to the authorities of the Member State concerned or, if it cannot be identified, to the authorities of the Member State where the provider is established – or has its legal representative – or to Europol.

DSA – Further Obligations on Providers of Online Platforms

Article	Obligation	Further Specification
20	Do provide recipients for at least six months with access to a complaint handling system that enables the lodging of complaints against a decision that the recipient's information constitutes illegal content or is incompatible with the terms and conditions.	Decisions can include removing, disabling access to or restricting the visibility of the information, or suspending or terminating the provision of the service to the recipient, their account, or their ability to monetise the information in question.
21	Do allow recipients to select any out-of-court dispute settlement body certified to resolve disputes relating to decisions and complaints that have not been resolved through internal complaint handling systems.	Certification is granted by the Digital Services Coordinator of the Member State where the out-of-court dispute settlement body is established based on criteria of impartiality and independence, expertise, remuneration, accessibility and efficiency.
22	Do take necessary technical or organisational measures to ensure that notices submitted by trusted flaggers, acting within their designated area of expertise, are given priority.	Status of trusted flagger is granted by the Digital Services Coordinator of the Member States in which the applicant is established based on criteria of expertise, competence and independence.
23	Do suspend, for a reasonable period of time and after having issued a prior warning, the service to recipients that frequently provide manifestly illegal content. Do suspend, for a reasonable period of time and after having issued a prior warning, the processing of notices and complaints submitted by recipients that frequently submit notice or complaints which are manifestly unfounded.	Suspension decisions must consider all relevant facts and circumstances available, including the absolute number, the relative proportion and the gravity of the misuses, and, where it is identifiable, the intention of the recipient.

Article	Obligation	Further Specification
24	Do include in yearly reports on content moderation submitted pursuant to Article 15 information about the disputes referred to out-of-court dispute settlements bodies and the suspensions imposed. Do publish, at least once every six months for each online platform or online search engine, information on the average monthly active recipients in the EU.	Information includes the number of disputes, their outcome, the median time needed for their completion, the share of disputes where the provider implemented the decisions of the body and the number of suspensions imposed. Information on active recipients is to be communicated to the Digital Services Coordinator and the European Commission upon request.
25	Do not design, organise or operate online interfaces in a way which deceives or manipulates recipients or otherwise manifestly distorts or impairs their ability to make free and informed decisions.	The European Commission may issue guidelines on how the obligation applies to specific practices, including giving prominence to certain choices by recipient, repeatedly requesting recipient to make a choice and making procedure for termination of service more difficult than subscription.
26	Do allow recipients of advertisements to identify that the information is an advertisement, the person who paid for the advertisement and/or on whose behalf it is presented, and information about the parameters used to determine the recipient of the advertisement. Do not present advertisements to recipients based on profiling using special categories of personal data.	Recipients must be able to declare whether the content is or contains commercial communications, which must be made clear to other recipients.
27	Do set out in your terms and conditions, when using recommender systems, the parameters used and any options for recipients to modify those parameters.	Parameters must explain why certain information is suggested to the recipient, and include the criteria which are most significant in making that determination and the reasons for the relative importance of those parameters.
28	Do put in place appropriate and proportionate measures to ensure high level of privacy, safety and security of minors. Do not present advertisements based on profiling using personal data of the recipient, if you are aware with reasonable certainty that the recipient is a minor.	The European Commission may issue guidelines to assist in applying these obligations.

DSA – Further Obligations on Providers of Online Platforms Allowing Consumers to Conclude Distance Contracts with Traders

Article	Obligation	Further Specification
30	Do ensure that traders can only use the services to promote messages or offer products or services to consumers located in the EU if they have been provided with certain information. Do make best efforts to assess whether that information is reliable and complete, asking traders to remedy the situation if that is not the case, and suspending their services in case of non-compliance.	Information includes the name, address, telephone number and email address of the trader, a copy of its identification document or any other electronic identification, its payment account details, the trade register in which it is registered and its registration number or equivalent, and a self-certification committing to only offer products or services that comply with applicable EU laws.
31	Do ensure that your online interface is designed so as to enable traders to comply with EU law on pre-contractual information, compliance and product safety information, and provide certain information to consumers. Do make reasonable efforts to check in any official and freely accessible database or online interface whether products or services offered have been identified as illegal.	Information includes that necessary for the identification of the products or services promoted or offered to consumers in the EU, any sign identifying the trader (e.g. trademark, symbol or logo), and that concerning the labelling and marking under EU law on product safety and compliance.
32	Do inform, if an illegal product or service has been offered through your services in the EU, the affected consumers of that fact, the identity of the trader and any relevant means of redress.	If you do not have the contact details of all the affected consumers, information is to be made publicly available and easily accessible on your online interface.

DSA – Further Obligations on Very Large Online Platforms and Very Large Online Search Engines

Article	Obligation	Further Specification
34	Do identify, analyse and assess any systemic risks in the EU stemming from the design or functioning of your service and its related systems, including algorithmic systems, on a yearly basis. In doing so, consider the design of your recommender systems, as well as your content moderation systems, terms and conditions, systems for selecting advertisements and data related practices.	Risk assessment includes systemic risks such as the dissemination of illegal content, actual or foreseeable negative effects on the exercise of fundamental rights, on civic discourse, electoral processes and public security, and in relation to gender-based violence, the protection of public health and minors, and physical and mental well-being.
35	Do put in place reasonable and proportionate mitigation measures tailored to the assessment of systemic risks, such as adapting the design of your services, terms and conditions, content moderation processes, algorithms, advertising systems and reinforce your internal processes for the detection of systemic risk.	Measures include adjusting cooperation with trusted flaggers, adapting their online interfaces to give recipients more information, taking measures to protect the rights of the child and ensuring that any information resembling an existing person, object or place is distinguishable through prominent markings.
37	Do conduct yearly independent audits to assess compliance with the obligations imposed by the DSA, and provide the relevant auditors with access to data and premises and answer oral or written questions.	Audits must be conducted by an independent organisation, result in an audit report containing certain information, ensure an adequate level of confidentiality and professional secrecy, and, if not positive, lead to operational recommendations and an audit implementation report.
38	Do provide at least one option for each of your recommender systems which is not based on profiling.	
39	Do compile and make publicly available a repository containing certain information regarding advertisements on your online interface for one year after the advertisement was presented.	Information includes the content of the advertisement, the person who paid for it and/or on whose behalf it is presented, its period of presentation, whether it was intended for a particular group of recipients and on the basis of what parameters and the total number of recipients reached.
40	Do provide the Digital Services Coordinator of your place of establishment or the European Commission, at their reasoned request and within a reasonable period of time, access to data necessary to monitor and assess compliance with the DSA obligations.	Data accessed is only used to monitor and assess compliance with the DSA obligations, while ensuring the protection of personal data, confidential information and trade secrets.
41	Do establish a new compliance function to monitor compliance with the DSA obligations.	
42	Do publish the report on content moderation required by Article 15 every six months, rather than on a yearly basis. Do provide the Digital Services Coordinator of your place of establishment and the European Commission with your risk assessment, risk mitigation, audit and audit implementation reports.	Report must contain additional information, related to human resources dedicated to content moderation and information on the average monthly recipients for each Member State.

DSA – Enforcement

Each Member State will designate competent authorities, with one of them being a newly designated Digital Services Coordinator responsible for the supervision and enforcement of the DSA in that Member State. The European Commission will retain exclusive power to supervise and enforce the DSA in relation to very large online platforms and very large online search engines providers.

The Digital Service Coordinator may exercise various investigative powers for the purpose of enforcing the DSA:

- requesting that providers that may be aware of information relating to a suspected infringement provide such information
- inspecting premises in order to examine, seize, take or make copies of information relating to a suspected infringement
- asking providers or their staff for explanations in relation to such information

The Digital Services Coordinator may impose the following penalties on non-compliant providers:

- fines of up to 6% of annual worldwide turnover for non-compliance with an obligation
- fines of up to 1% of annual worldwide turnover for the supply of incorrect information
- periodic penalty payments of up to 5% of average daily worldwide turnover for failure to comply with an investigative order or an order for the cessation of an infringement

In cases of risk of serious harm, the Digital Services Coordinator may also impose interim measures

The Broader Picture

The DMA and the DSA form part of a broader framework of EU legislation governing competition, communications and data protection.

The table below provides an overview and comparison of some of the relevant pieces of this complex EU regulatory framework. The table shows that the obligations imposed under different legal instruments overlap with each other. While it remains to be seen if this overlap may lead to potential conflicts of jurisdiction, the EU Court of Justice has found in the past that where there is overlap between two or more of different instruments of EU legislation, it will be possible for enforcement to proceed in parallel under each of them, provided that they pursue different (and sometimes complementary) objectives. Moreover, the same case law has also confirmed that a determination made under one legal instrument could be used as a presumption in an enforcement case under a different legal instrument relating to the same facts. For example, a determination of being a gatekeeper and of an obligation to provide access to certain essential input on its core platform could be used as a presumption that that company is dominant and its input is essential for the purpose of the application of EU competition law.

Obligations	Digital Markets Act	Digital Services Act	EU Competition Law	EU Merger Regulation	European Electronic Communications Code	General Data Protection Regulation	E-Privacy Regulation	EU Data Act
Self-preferencing Ban	✓		✓					
Access to Data and Services Requirements	✓		✓					
Restrictions on Users' Rights Ban	✓		✓		✓			
Transparency Obligations	✓	✓			✓			
Personal Data Protection and Data Mobility Obligations	✓	✓	✓		✓	✓	✓	✓
Interoperability Obligations	✓		✓		✓			✓
Merger Reporting Obligation	✓			✓				

International Cooperation

Digital services and markets are inherently global.

Due to the cross-border nature of digital platforms and the international scope of modern technology, competition authorities elsewhere in the world are also addressing how to ensure end users continue to benefit from new opportunities in digital markets, while promoting innovation and protecting consumer rights.

In the UK, for example, two draft bills are expected to be adopted in the near future, which aim to tackle the same issues as the DMA and the DSA:

- Similar to the DMA, the Digital Markets, Competition and Consumer Bill will empower the Digital Markets Unit (DMU) – which is already set up within the Competition and Markets Authority – to oversee the digital firms to be designated as having Strategic Market Status (SMS). The DMU will set and enforce a code of conduct and implement pro-competitive interventions regarding access to data and interoperability
- Similar to the DSA, the Online Safety Bill (OSB) will impose obligations on providers of internet services which allow users to upload or share content that may be encountered by others on their services, or include a search engine.

In the US, following a sixteen-month investigation of competition in digital markets, the US House of Representative subcommittee on antitrust, commercial and administrative law introduced in 2021 various antitrust bills targeting search, marketplace and user-generated content platforms, dealing with many of the same issues as the DMA.

As the OECD noted in this respect, "*Governments may need to enhance co-operation across national competent agencies to address competition issues that are increasingly transnational in scope or involve global firms.*" Against this backdrop, the US, EU and UK competition agencies have recently issued joint statements to re-affirm their commitment to cooperate in this area.

Conclusion and Contacts

Enforcement and compliance efforts in digital markets are becoming ever more complex. The DMA and DSA have been adopted while recent court rulings, investigations and hearings, policy reports and studies on how to address competition as well as wider data issues in digital markets keep proliferating around the globe.

We keep monitoring these issues through our webpage dedicated to Digital Markets Regulations around the world, which can be accessed here. We have extensive experience in advising clients on their potential regulatory risks in digital markets and options on how to mitigate them.

If you have any questions on the DMA, DSA or any other developments in this new and evolving area, please contact the author of this client briefing using the contact details below or your usual Squire Patton Boggs contact.

Francesco Liberatore
Partner, London, Brussels, Milan
T +44 207 655 1505, +322 627 11 11, +39 02 72 74 2001
E francesco.liberatore@squirepb.com

The author thanks Ruggero Chicco and Eben Kurtz for their assistance in preparing this client briefing.

SQUIRE PATTON BOGGS

squirepattonboggs.com

60254/10/22