A&L Goodbody

COMMERCIAL & TECHNOLOGY

European Regulation of Digital Services – the DSA

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act or **DSA**).

The DSA is a legislative initiative originally designed by the European Commission with the goal of enhancing the safety, trustworthiness and predictability of online environments.
The DSA is now in force and for the majority of in-scope service providers its provisions will apply from 17 February 2024.

18 MIN READ

Table of contents

Introduction

The DSA imposes new obligations on online intermediary services with the aim of increasing the transparency and safety of online environments. These obligations apply to all intermediary services. However, certain intermediary services, such as hosting services and online platforms, must comply with additional obligations. This tiered approach recognises the more significant role certain intermediaries play in society, in terms of their impact on digital safety. Additionally, the European Commission (**Commission**) has the power to designate certain services as Very Large Online Platforms (**VLOPs**) and Very Large Online Search Engines (**VLOSEs**) that are deemed to have a larger reach and greater impact than other intermediary services and are therefore tasked with more significant due diligence obligations. In this way, the obligations set out by the DSA are dependent on the functionality and reach of the relevant intermediary service.

The DSA focuses on increasing transparency, through the imposition of reporting obligations and/or prescriptive requirements in relation to an intermediary's terms and conditions and the functionality of its online interface. Intermediaries are also tasked with greater content moderation obligations, as the DSA requires intermediaries to implement notice and action mechanisms allowing for notification of illegal content, to implement complaint handling systems, and to participate in out of court settlement procedures in relation to content that has been flagged. In view of the greater risk arising for their services, VLOPs and VLOSEs are required to undertake detailed risk assessments and external audits.

Importantly, the DSA retains the liability exemption for content hosted, stored or transmitted that meets the test originally set out in the e-Commerce Directive. The DSA also introduces a 'good Samaritan' protection which allows intermediary services to carry out own-initiative investigations to identify and remove illegal content without losing their liability exemption.

Enforcement of the DSA is shared between national authorities and the Commission, with the Commission and national authorities having shared powers of enforcement of the DSA against VLOPs and VLOSEs with a more prominent role for the Commission in regulating such entities. Each Member State is required to designate a national authority as its Digital Services Coordinator (**DSC**), who will bear primary responsibility for overseeing the supervision and enforcement of the DSA in that Member State. The Commission and DSCs are expected to cooperate closely and provide each other with mutual assistance, creating a unified enforcement framework.

Both the Commission and DSCs are granted investigative and enforcement powers. The Commission has the power to request information, take interviews and conduct inspections, even before any proceedings are initiated. DSCs are granted similar powers of investigation, including requests for information and conducting inspections, however these powers will depend to some extent on how they are practically implemented by Member States. An infringement of the DSA has the potential to expose intermediaries to significant fines. Indeed, fines for non-compliance of up to 6% worldwide turnover can be imposed by the Commission or by a DSC of establishment.

The DSA also provides for an independent advisory group of DSCs – the European Board for Digital Services (the **Board**). The Board is intended to advise and provide guidance on issues falling within the scope of the DSA as well as assisting in joint investigations of DSCs.

The DSA will impact a variety of stakeholders, most significantly intermediary services who now face a heightened compliance burden. This compliance burden will vary for each intermediary service, with VLOPs and VLOSEs bearing the greatest compliance burden due to their nature and size. At the same time, consumers and businesses using these intermediary services are expected to benefit from the DSA and operate in safer, more trusted digital worlds.

The following Q&A provides further details on the core aspects of the DSA.

Q&A

1. Scope

(a) What is the scope of the DSA?

The DSA applies to "intermediary services" offered to recipients who are located in the EU, regardless of whether the recipient is a business or consumer. Similar to the GDPR, the DSA has an extra-territorial scope and applies to intermediary service providers, irrespective of their place of establishment, provided the services they offer are "substantially connected" to the EU. A "substantial connection" will exist where the intermediary service provider has:

- an establishment in the EU; or
- has a significant number of users in a Member State; or
- targets its activities towards a Member State. Relevant factors in determining whether a provider is targeting activities towards a Member State may include using a language or currency used in that Member State, the ability to order products to that Member State or using a relevant top-level domain.

(b) What is an intermediary service?

The DSA builds on and updates the existing legal framework for intermediary services laid down in Directive 2000/31/EC on Certain Legal Aspects of Information Society Services in Particular Electronic Commerce in the Internal Market (the **e-Commerce Directive**). Pursuant to Article 2(a) of the e-Commerce Directive, Information Society Services (**ISS**) are those defined by Article (1)(1)(b) of Directive 2015/1535, namely "any service provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".

The DSA applies to intermediary services, defined and categorised in the DSA as 'mere conduit', 'caching' and 'hosting' services:

- **Mere Conduit services** consist of the transfer of information provided by a service recipient over a communication network. Examples of such a service include internet service providers, top-level domain name registries, voice over IP, virtual private networks, domain name systems, and direct messaging services.
- **Caching services** have the sole purpose of storing information from a communications network to improve the efficiency of the subsequent transmission of the information to other recipients upon their request. Examples include content delivery networks, content adaptation proxies, or reverse proxies.
- **Hosting services** such as app stores, online marketplaces, cloud service providers and social media platforms that involve the storage of information provided by, and at the request of, a recipient of the service.

In addition to the above, there are specific categories of intermediary services which the DSA imposes more significant obligations. These include **Online Platforms** that:

- are hosting services that, at the request of a recipient of the service, **store and disseminate information to the public**, unless that activity is deemed a minor and purely ancillary feature of another service.
- allow consumers to conclude **distance contracts** with traders.

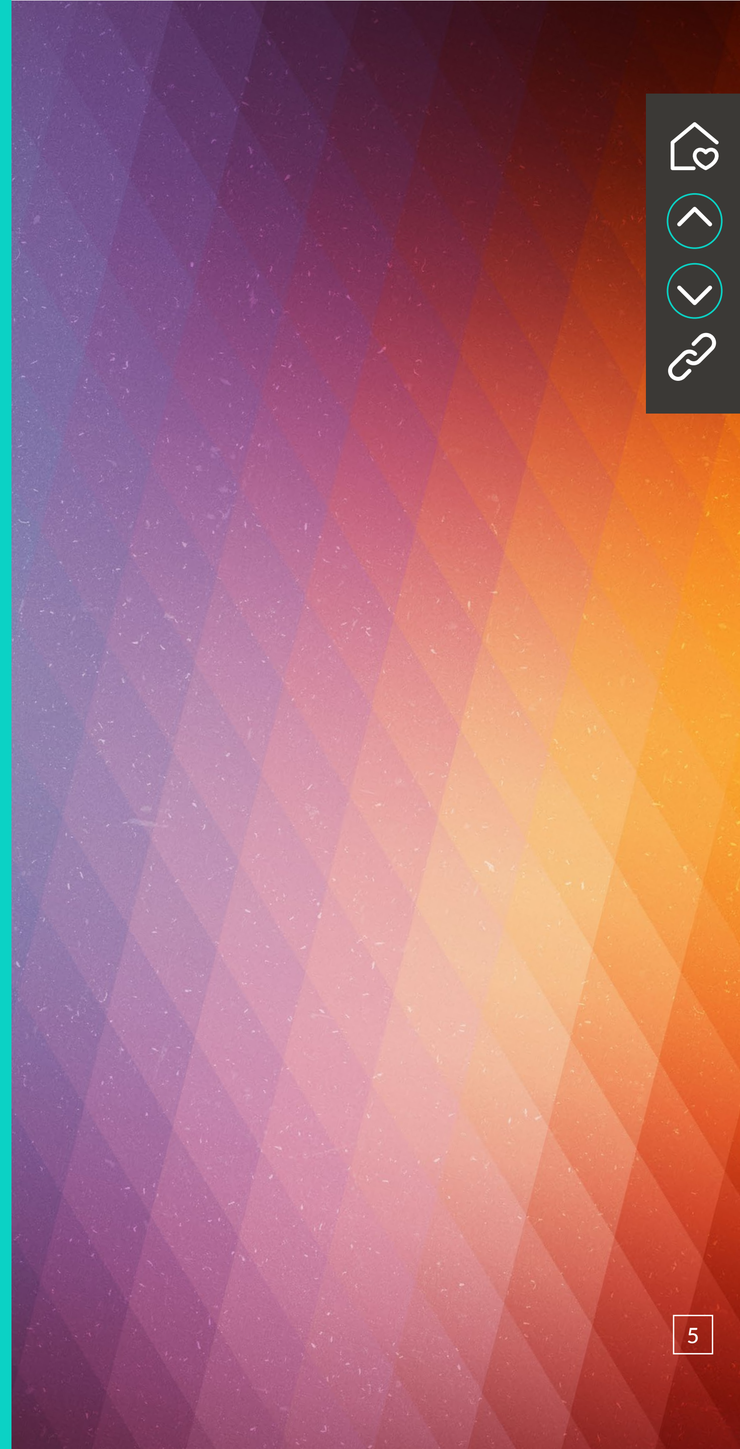
(c) Very Large Online Platforms and Very Large Online Search Engines

The DSA also empowers and requires the Commission to designate certain platforms and online search engines that have a number of average monthly active recipients of the service in the EU that is equal to or higher than 45 million as being a VLOP or VLOSE. Unlike the intermediary services listed above, a service will not be deemed a VLOP or VLOSE unless designated as such by the Commission. When deciding whether to designate a VLOP or VLOSE, the Commission will have regard to the number of average monthly active recipients published by the provider in question, as they are required to publish this information (so that the Commission can make this decision).

On 25 April 2023, the Commission adopted the first designation decisions under the DSA, designating 17 entities as VLOPs and 2 entities as VLOSEs. The entities were designated based on the user data they were required to publish by 17 February 2023. The **VLOPs** are: Alibaba AliExpress; Amazon Store; Apple AppStore; Booking.com; Facebook; Google Play; Google Maps; Google Shopping; Instagram; LinkedIn; Pinterest; Snapchat; TikTok; Twitter; Wikipedia; YouTube; and Zalando. The **VLOSEs** are: Bing; and Google Search.

(d) Is there a different DSA regime for SMEs?

Small and micro enterprises (**SMEs**) are subject to less onerous regulatory requirements than larger platforms, as the DSA recognises the different capacities and needs of businesses of different sizes. SMEs have also been given more time than larger businesses to become DSA compliant.



2. Obligations imposed under the DSA

(a) Are new obligations imposed on intermediary services?

One of the key objectives of the DSA is to create a safer online environment by setting out clearly rules and responsibilities for providers of intermediary services. The DSA introduces a broad range of new obligations applicable to providers of intermediary services, including obligations relating to content moderation practices and user redress, which we set out in more detail below. For recipients of such services, the obligations are intended to provide increased clarity about the rules governing content on these services and to boost the reliability and safety of online services.

(b) Is everyone subject to the same obligations?

As highlighted above, the DSA identifies four categories of intermediary service providers and determines what obligations apply to them. Although there are general obligations applicable to all intermediary services, there are more onerous obligations for specific categories of intermediary service providers.

We set out below each category of intermediary services and a summary of their respective obligations:

i. Intermediary Services

ii. Hosting Services

iii. Online Platforms

iv. VLOPs and VLOPEs

The obligations are cumulative in nature and services which fall under a number of these categories will be obligated to comply with the obligations set out in each e.g. a VLOP may be required to comply with the obligations set out in each of (i) - (iv).

(i) Intermediary Services

Under the DSA, all intermediary services are subject to the following requirements/ obligations:

INTERMEDIARY SERVICES	
Obligation	**Summary of Requirements**
Removal of illegal content *(Article 9 and 10)*	Upon receipt of an order to act against illegal content/provide information, inform relevant authorities of any effect given to the order without undue delay, specifying if and when effect was given to the order. 'Illegal content' is defined broadly under the DSA, to include any information or activity, including the sale of products or provision of services, which is not in compliance with EU law or the law of a Member State, which includes hate speech, defamation, the non-authorised use of copyright protected material and incitement to violence.
Designate a point of contact *(Article 11 and 12)*	Designate single points of contact, one for supervisory authorities and another for users, and make information publicly available to facilitate communication with those points of contact.
Appoint a legal representative *(Article 13)*	Appoint a legal representative in the EU, if an intermediary service provider without an establishment in the EU who offers their services to users in the EU. The legal representative may be held liable for non-compliance with obligations under the DSA.
Ensure compliant terms & conditions *(Article 14)*	Comply with the obligations regulating the form and content of terms and conditions applicable to their own services. The terms must include the steps a user can take to terminate services. The terms must also set out any restrictions imposed on information permitted on the services and those restrictions must be applied in an objective and proportionate manner. It is also necessary that the terms include information on the use made of any algorithmic tools for content-moderation and the internal complaints system in place. Services that are primarily used by/ predominantly directed at minors must explain the conditions for, and any restrictions on, the use of their service in a way that minors can understand.
Publish an annual report *(Article 15)*	Publish a 'clear' and 'easily comprehensible' annual report detailing content moderation activity. The Report should include the specific information elements listed in Article 15, including: the number of orders received from supervisory authorities and their response times; information on their own-initiative content moderation practices, whether this be their use of automated tools and the restrictions they applied, and information about the training and assistance provided to content moderators; and the number of complaints received through the internal complaint-handling systems. The transparency obligations do not apply to SMEs.

(ii) Hosting services

Hosting Services involve the storage of information provided by, and at the request of, a recipient of the service. Some examples include app stores, online marketplaces, cloud service providers and social media platforms. Intermediary service providers that are hosting services will be subject to the following additional requirements:

HOSTING SERVICES	
Obligation	**Summary of Requirements**
Enhanced reporting *(Article 15)*	Hosting services transparency reports must include extra information including the number of reports that were submitted by trusted flaggers and these should be organised by the type of illegal content concerned. They must specify the action taken and the number processed by automated means and the median response time.
Establish a notification system *(Article 16)*	Have an established notification system in place that allows users to notify of content they believe to be illegal. Those measures must ensure a user is capable of facilitating precise notices to accurately identify the illegal content. The DSA codifies the position provided for in EU case law that where such a notice provides a provider with sufficient knowledge as would allow a diligent provider to identify illegality this would be deemed to give rise to actual knowledge or awareness which would in turn reverse the hosting liability exemption. Users must also be informed of the decision taken on their notice and the further redress mechanisms available to them.
Provide reasons to users *(Article 17)*	Provide a statement of reasons to a user if content is removed, disabled or if services are terminated. The DSA requires for the statement to include the facts relied upon in the decision, the legal rule or the contractual term that was breached and the available redress mechanisms. Law enforcement authorities may intervene and ask that no explanation is given to the user.
Report criminal offences *(Article 18)*	Alert law enforcement authorities if the provider of hosting services believes that a serious criminal offence involving a threat to life or safety of persons is taking place or is planned.

(iii) Online platforms

Online platforms are hosting services which also disseminate information to the public at the user's request, such as online marketplaces and social media platforms. The obligations in this section do not apply to micro or small enterprises. It is possible for intermediary services to apply to be exempted from the requirements of this section of the DSA.

Intermediary services which qualify as online platforms are subject to the following additional requirements/obligations:

ONLINE PLATFORMS	
Obligation	**Summary of Requirements**
Establish an appeal process *(Article 20)*	Put in place an internal complaint-handling process allowing users to appeal the decision to remove/restrict access to content determined to be illegal or in breach of the terms and conditions of the platform or to suspend/terminate a user's use of the service. The decision must be taken under the supervision of qualified staff (and not solely on the basis of automated means) and the relevant user has six months to appeal their decision. The online platform is also required to have a clear and free complaint mechanism in place.
Out-of-court settlement of disputes *(Article 21)*	Users to be given the opportunity to refer any decision they disagree with to an out-of-court dispute settlement body certified by the Digital Services Coordinator of the relevant Member State. This information must be available on the service's interface.
Prioritise "trusted flaggers" *(Article 22)*	Any content that is reported by 'trusted flaggers' is to take priority and should be processed without delay. The necessary criteria for an entity to become a trusted flagger is set out in the DSA and interested parties can apply to the Digital Services Coordinator to become one. Trusted flaggers must publish public reports on the notices that they have filed and the effect given to these notices by the different providers.
Suspend repeat offenders *(Article 23)*	If users repeatedly upload illegal content after a prior warning, they may be suspended for a reasonable time. Repeatedly submitting unfounded complaints shall also result in suspension.
Publish monthly active users *(Article 24)*	Publish the average monthly active users in the EU over the last six months on their online interface. Online platforms were first required to publish this by 17 February 2023 and are required to update this at least once every six months.
Avoid dark patterns *(Article 25)*	A prohibition in relation to the use of "dark patterns" on online platforms which prohibits the design or operation of the user interface in a manner that manipulates or deceives users.
Identify advertising *(Article 26)*	The fundamental parameters of the online platforms' recommender systems, along with options to change those parameters should be evident in the platform's terms and conditions. These are systems that suggest and rank the information shown to a platform's users.
Publish recommender systems *(Article 27)*	The fundamental parameters of the online platforms' recommender systems, along with options to change those parameters should be evident in the platform's terms and conditions. These are systems that suggest and rank the information shown to a platform's users.
No targeting of minors *(Article 28)*	Targeting advertising techniques that involve the processing of personal data of minors or sensitive personal data (as defined under the GDPR) are prohibited.
Commercial communications functionality *(Article 26)*	Online platform providers are obligated to give users functionality that allows them to declare that their content is a "commercial communication".

(iv) Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs)

VLOPs and VLOSEs are service providers that have to comply with stricter obligations under the DSA because of their more significant user reach. Platforms and services fall within this category when they provide their services to 45 million or more monthly active users in the EU. The rationale behind this category is that large platforms and search engines are deemed to pose a greater risk in terms of exposure to harmful content by virtue of their larger user base and the fact that they facilitate the sharing of user generated content publically. The obligations aim to empower and protect user's online (including minors) by requiring the VLOPs and VLOSEs to assess and mitigate their systemic risks and to provide robust content moderation tools.

Designated VLOPs and VLOSEs must comply with **additional obligations** from four months of their date of designation, in addition to the obligations set out above.

VLOPS AND VLOSES

Obligation	Summary of Requirements
Accessibility of terms & conditions *(Article 14 and 33)*	Publish terms and conditions in the official languages of each Member State that their services are offered. Also required to provide a machine-readable summary of the terms and conditions, including available remedies and redress mechanisms.
Perform risk assessments *(Article 34)*	Perform risk assessments to assess the "significant systemic risks" that stem from the provision of their services. This centres on risks in relation to the dissemination of illegal and other harmful content through their services.
Introduce risk mitigation measures *(Article 35)*	Put in place reasonable, proportionate, and effective mitigation measures, tailored to the specific systemic risks identified in their risk assessment, with particular consideration for the impacts of such measures on fundamental rights.
Take action in crisis *(Article 36 and 48)*	Take certain specified actions in case of a public (security or health) crisis. This may include conducting an assessment or taking active measures to prevent, eliminate or limit their contribution if their service could contribute to it. This includes content moderation.
Conduct independent audits *(Article 37)*	Conduct independent audits which assess the provider's compliance with certain obligations arising under DSA, as well as any commitments to the codes of conduct. The audits are to be carried out at least once a year, by independent firms, free of any conflict of interest. The recommendations in the audit report must be either adopted or the platform must justify their reasons for not doing so within one month.
Alternatives to recommender systems *(Article 38)*	Where they employ recommender systems, they must provide at least one option to users that is not based on profiling.

VLOPS AND VLOSES	
Obligation	**Summary of Requirements**
Advertising transparency reporting *(Article 39)*	Additional advertising transparency requires information such as whether the advertisement was targeted, or the relevant parameters and the total number of recipients reached to be available and searchable on the platform.
Information sharing with regulators *(Article 40)*	There is a requirement to share data with authorities to monitor their compliance with the DSA. Examples of information that may be shared includes; explanations on algorithm systems. "Vetted researchers" may also be granted access to data by regulators for the purpose of conducting research that contributes to the identification of systemic risks.
Establish a compliance function *(Article 41)*	Establish an independent compliance function that monitors compliance with DSA obligations and reports directly to the management body of the provider and can raise concerns and warn the management body of non-compliance risks.
Pay an annual supervisory fee *(Article 43)*	Pay the Commission an annual supervisory fee to cover the estimated costs of the Commission, calculated according to the relevant delegated act.
Create a public ads repository *(Article 39)*	Establish a publicly accessible repository of all online advertisements that have been displayed on their platform. The repository must include information on the period during which the advertisement was/is being presented to recipients of the service, and for one year after the ad's final exposure. The repository must also contain additional information relating to ads, including the parameters used to specifically display the ad to one or more particular groups of recipients and the total number of service recipients reached (with aggregate numbers broken down by Member State, if applicable).

(c) How will the DSA impact online advertising practices?

(i) Rules for advertising

The DSA introduces specific rules for online platforms and VLOPs and VLOSEs that engage in online advertising practices. Their objective is to increase transparency, accountability, and consumer rights.

Under the DSA, online platforms that present advertisements on their interfaces must provide recipients with concise and unambiguous information about the advertisement in real time, including prominent markings and information about the advertiser, the product or service being advertised, and if there was any payment for the placement of the content. Targeting advertising techniques that involve the processing of personal data of minors or sensitive personal data (as defined under the GDPR) are prohibited.

VLOPs and VLOSEs must comply with additional online advertising transparency obligations, and make publicly available a repository of the information about online advertisements for a period of one year after the advertisement was last presented.

(ii) Additional rules for online marketplaces

The DSA imposes special obligations on online platforms that allow consumers to conclude distance contracts with traders. Some of these obligations include:

- Implementing a Know-Your-Trader program. This consists of obtaining specific information from traders, including contact details, identification, payment details, and a certification from the trader to only offer products or services that comply with EU law. Online marketplaces must then make their best efforts to assess whether the information is reliable.
- Performing due diligence checks on the products and services provided on their site by traders. This includes making sure traders have provided information necessary for the identification of the products or the services and where applicable, information concerning the labelling and marking in compliance with rules of EU law on product safety and product compliance. Providers must also randomly check the potential illegality of offered products and services.
- Informing consumers that they have bought an illegal product or service on the online marketplace, within six months of the moment the provider became aware of the illegality.

3. Enforcement

(a) Who will be enforcing the DSA?

Enforcement of the DSA is shared between national authorities and the Commission. The Enforcement regime will depend on the provider on whom provisions of the DSA are being enforced against.

On a national level, the DSA allows Member States to designate one or more national authorities with responsibility for the supervision and enforcement of the DSA, recognising that the DSA touches on multiple issues which may already come within the framework of current national authorities such as consumer protection, media regulation and data protection. However, one of these national authorities must be designated the DSC, which is the body tasked with primary responsibility for enforcing and supervising the DSA. The DSC will be the single body that pulls the national authorities together and acts as the primary entity that oversees compliance with the DSA. In Ireland, the DSC has been announced to be An Coimisiún na Meán (in English, the Media Commission, but we understand it plans to adopt and use its official Irish name). However, the powers of DSC have not been formally granted to An Coimisiún na Meán as yet, although it is proposed that this will be done through an amendment to the Online Safety and Media Regulation Act.

The revisions to the Online Safety and Media Regulation Act are intended to specify the enforcement powers of An Coimisiún na Meán as Ireland's DSC and set out national procedures for other provisions of DSA such as:

- complaints mechanisms for users;
- vetting of researchers to allow data access to platforms; and
- certification of out-of-court dispute resolution bodies.

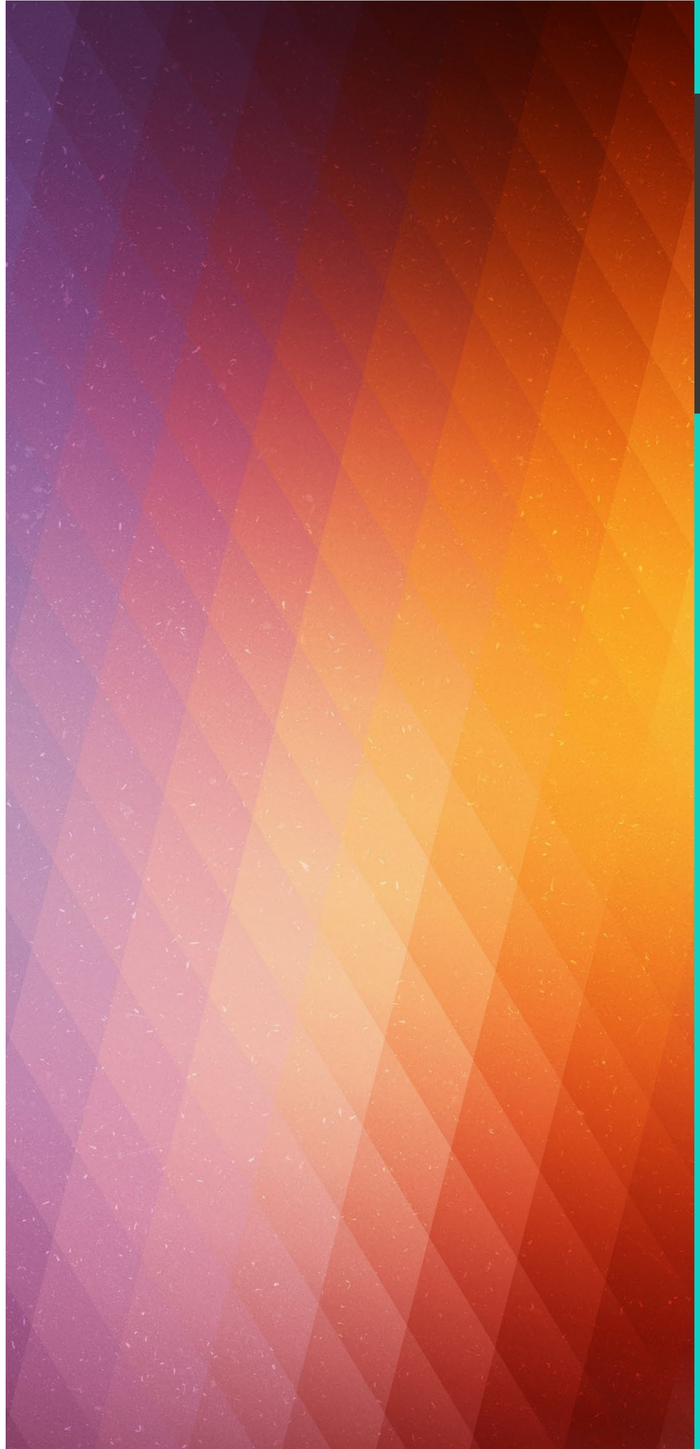
(i) Digital Service Coordinator

The DSA is based on the country-of-origin principle. The DSC where the main establishment of a provider is located shall have exclusive powers to supervise and enforce the provisions of the DSA in respect of that provider (subject to exceptions below).

(ii) EU Commission

The Commission is responsible for supervising and enforcing the enhanced obligations specific to VLOPs and VLOSEs. Member States have residual supervision and enforcement powers against VLOPs and VLOSEs for the other sections of the DSA, only to the extent the Commission has not initiated proceedings. If the Commission initiates proceedings against the VLOP or VLOSE, then the relevant Member State is relieved of its supervision and enforcement powers.

The Commission has a variety of investigative powers which it can exercise even before initiating any formal proceedings, such as requests for information, power to take interviews and statements, and power to conduct inspections. The Commission will similarly have the power to impose fines and require immediate actions where necessary to address very serious harms.



(b) What actions can be taken by DSCs in relation to non-compliance with the DSA?

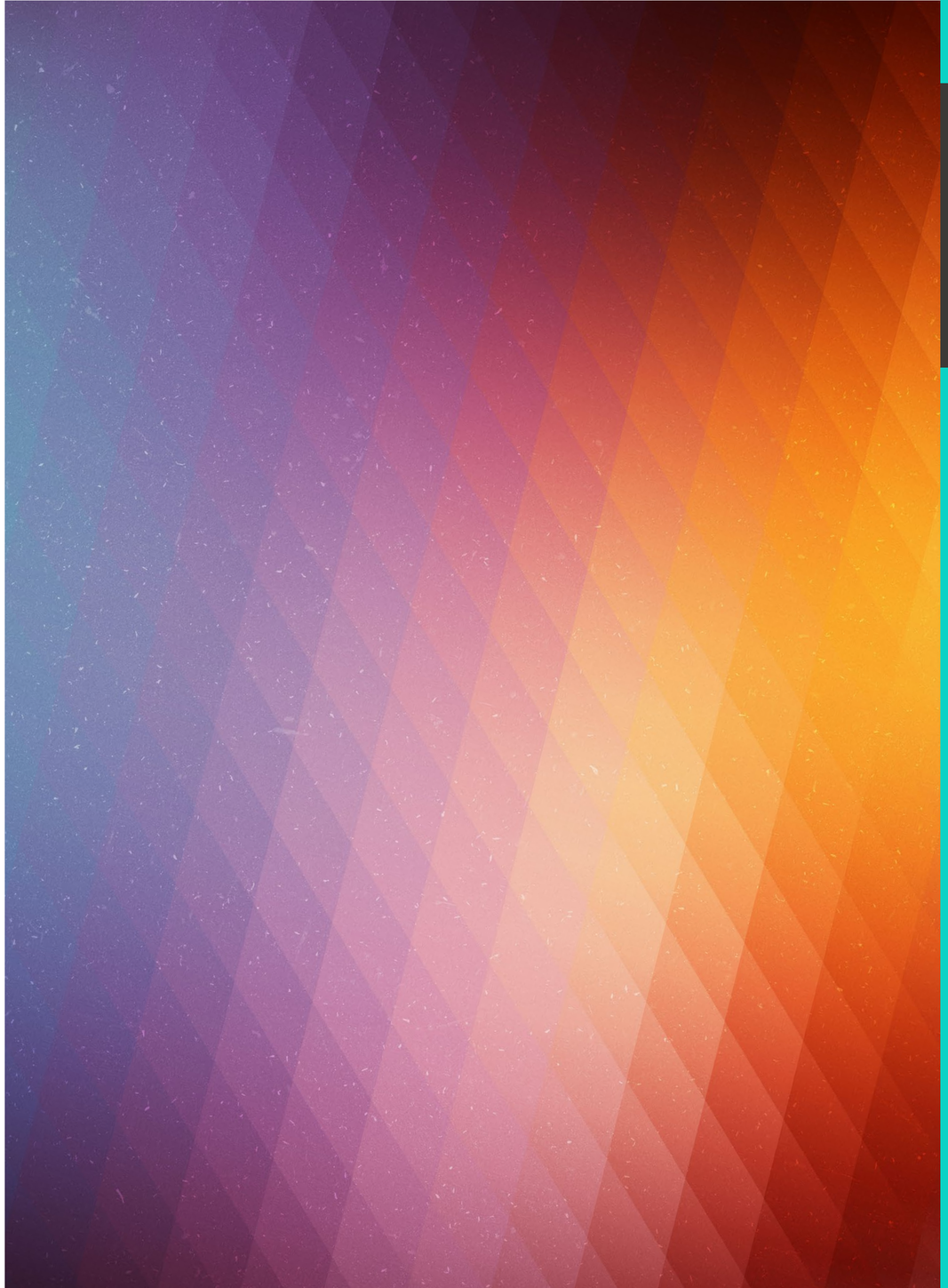
The DSC will be capable of imposing sanctions on digital service providers for non-compliance with the DSA, including fines, penalties, and even the suspension or blocking of services in extreme cases.

(i) Fines

The DSA specifies that the maximum fine possible under the act is 6% of the annual worldwide profits of the intermediary services in the preceding financial year. The maximum amount for a periodic penalty payment shall not exceed 5% of the average daily turnover of the provider in the previous financial year per day. If intermediaries fail to rectify or inspect misleading information on their service the maximum fine will be 1% of the annual income of the provider of intermediary services. Fines under the DSA must be proportionate and effective.

(ii) Temporary Access Restrictions

Where enforcement measures are exhausted, and the service provider is causing persistent and serious harm, the DSC may request that the competent judicial authority of the Member State order the temporary restriction of access to the infringing service or to the relevant online interface.



4. Timeline

(a) From when will the DSA apply and what are the key dates under the DSA?

The DSA entered into force on **16 November 2022** and will apply to all intermediary services from **17 February 2024**, subject to certain exceptions. If the Commission has designated an entity as a VLOP or VLOSE, the whole of the DSA will apply to that VLOP or VLOSE four months after notification of the designation from the Commission. This means that designated VLOPs and VLOSEs will be subject to the DSA before other intermediary services.

On **25 April 2023**, the Commission made its first designation decision under the DSA, designating 17 VLOPs and 2 VLOSEs. The designated VLOPs and VLOSEs will be required to comply with all applicable obligations of the DSA from **late August 2023**.

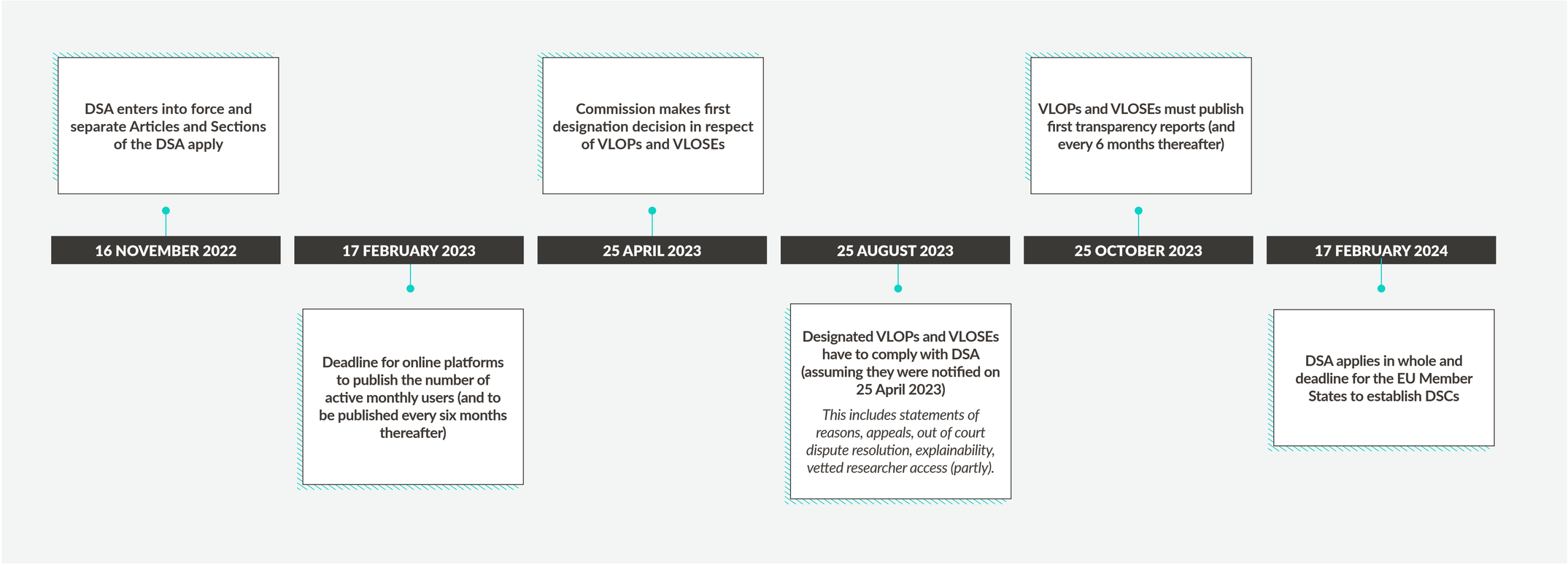
(b) What other provisions of the DSA apply from 16 November 2022?

Whilst the DSA will not apply to other providers until **17 February 2024**, certain provisions (some of which have already been mentioned above) have been applicable since **16 November 2022**. These provisions are intended to allow the Commission to prepare for the implementation and enforcement of the DSA, as well as other interim measures. They include:

- Transparency reporting obligations of online platforms: Online platforms and online search engines had until 17 February 2023 to publish information, in their publicly available online interfaces, on the average monthly active users of their services in the EU. They will be obliged to repeat this exercise at least once every six months thereafter.
- Delegated acts and implementing acts: The Commission can start adopting delegated acts to supplement the DSA by laying down: methodology for calculating the number of average monthly active recipients of the service in the Union; rules for performance of independent audits of VLOPs or VLOSEs compliance with certain DSA obligations (the entry into force of this act is expected in July 2023); technical conditions under which VLOPs or VLOSEs will share data with researchers and the purposes for which the data may be used; and methodology and procedures for determination of annual supervisory fees.

The Commission may also adopt implementing acts concerning templates of transparency reports and practical arrangements for: functioning of the information sharing system that supports communications between Digital Services Coordinators, the Commission and the Board; inspections in the premises of VLOPs or VLOSEs conducted by the Commission; monitoring the effective implementation and compliance with the DSA of VLOPs or VLOSEs by the Commission; hearings of VLOPs or VLOSEs by the Commission before adopting enforcement decision; and negotiated disclosures of information stored in the Commission's file to VLOPs / VLOSEs.

(c) Timeline of Key Dates



A&L Goodbody

Key contacts

John Whelan
Partner
+353 1 649 2234
jwhelan@algoodbody.com

John Cahir
Partner
+353 1 649 2943
jcahir@algoodbody.com

Chris Bollard
Partner
+353 1 649 2328
cbollard@algoodbody.com

Andrea Lawler
Partner
+353 1 649 2351
alawler@algoodbody.com

Andrew Sheridan
Partner
+353 1 649 2766
asheridan@algoodbody.com

Mark Ellis
Partner
+353 1 649 2885
mellis@algoodbody.com

© A&L Goodbody LLP 2023. The contents of this document are limited to general information and not detailed analysis of law or legal advice and are not intended to address specific legal queries arising in any particular set of circumstances.