DIGITAL SERVICES ACT and ACCESS TO INFORMATION HELD BY SERVICE PROVIDERS

Communication channels

Orders to provide information

User notification

Data retention obligations

The Digital Services Act ("DSA") is a European Union ("EU") law that introduces new and harmonised rules for providers of digital services. As regards access to electronic evidence, especially in a cross-border context, the DSA importantly harmonises rules on disclosure orders addressed by authorities directly to digital service providers, including the obligation to notify the user, sets out new communication channels and introduces specific data retention obligations.

This document, which was prepared in the framework of the **SIRIUS Project**, aims to raise awareness of the EU Member States' authorities on the toolbox put in place by the DSA and assist them in the process of accessing information held by service providers, in particular in criminal investigations and proceedings.

The SIRIUS project has received funding from the European Commission's Service for Foreign Policy Instruments (FPI) under contribution agreement No PI/2020/417-500. This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

TABLE OF CONTENTS

What is the Digital Services Act? 3

Relation between the DSA and other EU and national laws on digital services 3

DSA vs. the EU Electronic Evidence legislative package 3

DSA vs. the General Data Protection Regulation 3

DSA vs. national laws 3

Who does the DSA apply to? 4

Where does the DSA apply? 5

Substantial connection criterion 5

Targeting of activities 5

Orders to provide information 6

Who can issue the order? 7

What data can be requested? 7

GDPR 7

What are the minimum conditions for issuing the order? 8

Transmission of the order 9

User notification 9

Digital Services Coordinator 9

What are providers of intermediary services obliged to do? 10

Transparency obligations 10

What about data retention? 11

Data retention obligation in the DSA 11

To whom does the data retention obligation apply? 11

What data is collected and retained? 11

What is the retention period? 11

Proactive notification 12

Member State concerned 12

Nature of the offences 12

Communication channels 13

Single points of contact 13

Legal representatives 13

Enforcement of the DSA 14

Enforcement structure 14

Sanctions 14

When will the DSA apply? 15

WHAT IS THE DIGITAL SERVICES ACT?

The DSA is an EU regulation which is **directly applicable to providers of digital services**, such as online platforms, cloud services, social networks, app stores and content-sharing platforms, across the EU. It seeks to establish a **harmonised regulatory framework** for all categories of content, products, services, and activities on digital services. It aims to provide for a predictable and trusted online environment that promotes innovation in the EU internal market while ensuring online safety and protection of fundamental rights of the recipients of digital services (i.e. the users).

RELATION BETWEEN THE DSA AND OTHER EU AND NATIONAL LAWS ON DIGITAL SERVICES

The DSA applies to digital services (intermediary services) in all the sectors in the EU (i.e. horizontal application). It **addresses the gaps** of **EU sector-specific legislation** and **complements the existing and envisaged EU legislation** (e.g. Terrorist Content Online Regulation, and Regulation laying down rules to prevent and combat child sexual abuse).

DSA vs. the EU Electronic Evidence legislative package

In the field of direct cooperation between the authorities and providers of intermediary services active on the EU territory, the DSA recognises the **potentially overlapping scope of application** of the EU Electronic Evidence legislative package.

According to Article 2(4), the DSA is **without prejudice** to a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters ("Electronic Evidence Regulation") and a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings ("Electronic Evidence Directive").

The DSA considers the Electronic Evidence Regulation to be a ***lex specialis.*** → When both apply, the **rules of the Electronic Evidence Regulation should prevail** either as a specific application of or exception to the DSA.

DSA vs. the General Data Protection Regulation

The protection of individuals with regard to the processing of personal data in the EU is governed by the General Data Protection Regulation ("GDPR") and Directive on privacy and electronic communications ("ePrivacy Directive"). The measures introduced by the DSA do not amend but complement the existing rules on the processing of personal data by imposing additional obligations (e.g. transparency obligations) towards recipients of intermediary services.

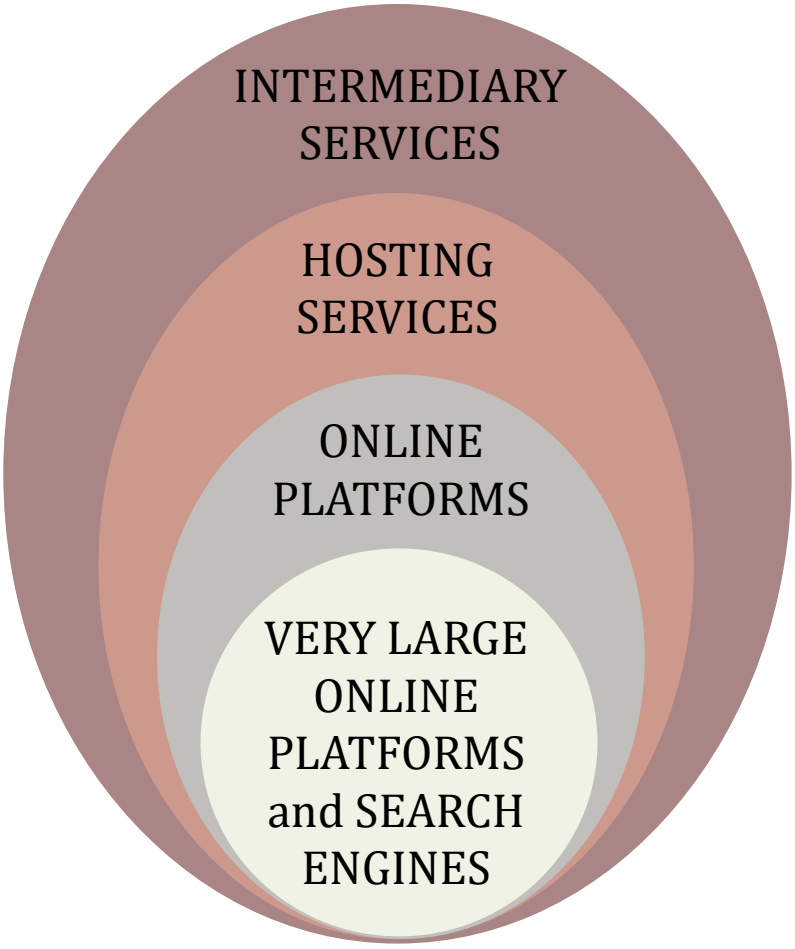
DSA vs. national laws

Unless explicitly provided otherwise like in the case of orders for information under Article 10 of the DSA, **Member States (MSs) must not introduce additional or keep in place conflicting national provisions** for matters which fall within the scope of the DSA.

WHO DOES THE DSA APPLY TO?

The DSA applies to **intermediary services**, i.e. one of the following information society services: "mere conduit", "caching" and "hosting" services. The distinction between them is purely technical.

For the purposes of the DSA, it is more important to determine under which of the **four categories** a particular intermediary service falls (the largest category being "intermediary services" and the most restricted in terms of qualifying factors being "very large online platforms and search engines") and what is the level of corresponding obligations for the provider of such services under the DSA.



online search engines, wireless local area networks, domain name system (DNS) services, top-level domain name registries, registrars, virtual private networks, voice-over-IP, cloud infrastructure services, messaging apps, and web-based email service providers

cloud storage services, web hosting, paid referencing services or services enabling sharing information and content online, including file storage and sharing

social networks, app stores, content-sharing platforms, online marketplaces, and online travel and accommodation platforms

online platforms and search engines with at least 45 million monthly active users in the EU (equivalent to 10% of the EU population) designated as such by the European Commission

Harmonised due diligence obligations under the DSA apply to intermediary services providers **cumulatively**, commensurate with their nature, size and impact. Each following category of intermediary services providers is subject to a specific set of obligations in addition to all the obligations applicable to the preceding categories. Accordingly, **all intermediary services providers must comply with certain basic obligations**, such as the obligation to create a point of contact. Providers of hosting services and online platforms are bound by a more advanced set of obligations, including specific data retention obligations for providers of online platforms. Very large online platforms (VLOPs) and very large online search engines (VLOSEs) must respect the most stringent requirements, such as the risk management obligations.

The **Electronic Evidence Regulation** does not distinguish between different categories of service providers. It applies to providers of electronic communications services, internet domain name and IP numbering services, and providers of other information society services that do not qualify as electronic communications service providers but offer users the ability to communicate with each other or offer their users services that can be used to store or otherwise process data on their behalf. Notwithstanding different terminology, its scope of application thus appears to be virtually the same as under the DSA.

WHERE DOES THE DSA APPLY?

The DSA applies to intermediary services that are **offered in the EU irrespective of the place of establishment or location of the provider of such services**. The DSA thus covers providers of intermediary services established in the EU, as well as those established outside the EU but offering their services in the EU, as evidenced by a **substantial connection** to the EU.

Providers of intermediary services offer their services in the EU when they **enable natural or legal persons in one or more MSs to use their services** and do not block access to such services (e.g. by geo-blocking the entire EU market).

Substantial connection criterion

1. Considered to be fulfilled where the service provider is **established in the EU**.
2. If the service provider is **established outside of the EU**, the substantial connection criterion should be based on specific factual criteria, such as:

- A significant number of recipients of the service in one or more MSs in relation to the population thereof,
- The **targeting of activities** towards one or more MSs.

Targeting of activities

Determined on the basis of all **relevant circumstances**, such as:

- The use of a language or a currency generally used in a particular MS,
- The possibility of ordering products or services in one or more MSs,
- The use of a relevant top-level domain (e.g. *intermediaryserviceprovider.be* , whereas *.be* is a top-level domain for Belgium),
- The availability of an application in the relevant national application store,
- The provision of local advertising or advertising in a language used in the targeted MS,
- The provision of customer service in the language generally used in the targeted MS.

The **Electronic Evidence Regulation** also has an extraterritorial scope of application and applies to service providers "offering services in the Union" even if they do not have physical presence in the EU. In order to qualify as a provider that offers services in the EU, it must a) enable natural or legal persons in a MS to use the services, and b) have a substantial connection to the EU. The criteria for assessing such connection are aligned with the criteria set out in the DSA.

ORDERS TO PROVIDE INFORMATION

Using judicial cooperation channels to obtain data (and electronic evidence) from service providers located in a foreign jurisdiction often takes too long which can lead to the loss of data in criminal investigations.

In order to facilitate and accelerate the process of obtaining data directly from foreign service providers, MSs have been increasingly using voluntary direct cooperation channel and applying different national tools, conditions and procedures in the process. This has led to a rather fragmented legal framework and to additional challenges for law enforcement and judicial authorities as well as service providers on the receiving end of the data disclosure requests made on a voluntary basis and production orders under Article 18(1)(b) of the Convention on Cybercrime.

Article 10 of the DSA addresses part of the concerns on the lack of harmonisation of the rules surrounding (cross-border) requests for data disclosure directed to service providers.

ARTICLE 10

DSA establishes **common rules** on the **content and format of orders** to provide information (**data disclosure orders**) issued by competent authorities directly to providers offering intermediary services in the EU

NATIONAL ORDERS

Disclosure orders directed to an intermediary services provider established or represented in the MS of the authorities issuing the order.

CROSS-BORDER ORDERS

Disclosure orders directed to an intermediary services provider established or represented in the territory of another MS.

Article 10 of the DSA does not give **any new powers to national authorities**. It **does not provide itself the legal basis** for the issuing of data disclosure orders, which must exist under EU laws (e.g. Electronic Evidence Regulation) or national law and in compliance with EU law.

Brief overview of the most important elements of data disclosure orders under Article 10 of the DSA can be found here.

The DSA puts in place a harmonised framework for the **exercise of powers by national judicial (or administrative) authorities that already exist** under national or EU laws laying down:

- **Specific minimum conditions** that such orders must meet in order to give rise to the obligations of the provider of intermediary services under Article 10 of the DSA; and
- **Complementary procedural requirements** relating to the processing of those orders.

The **Electronic Evidence Regulation** creates two new legal instruments, European Production Order and European Preservation Order. It lays down the rules under which an authority of a MS, in a criminal proceeding, may order a service provider established or represented in another MS to produce and preserve electronic evidence. It applies only in cross-border cases.

WHO CAN ISSUE THE ORDER?

Authorities of any MS as determined by the relevant national or EU laws.

Depending on the legal system of each MS and the relevant field of law at issue, **national judicial, but also administrative authorities**, including law enforcement authorities may have the competence to issue such an order in a particular MS.

The **Electronic Evidence Regulation** restricts the pool of possible issuing/validating authorities. European Production Orders may only be issued or, if issued by another competent authority (including law enforcement authorities), validated by a competent judicial authority. Depending on applicable national law, this may be a judge, a court, an investigating judge (or a public prosecutor in case of a European Production Order for subscriber data or traffic data requested for the sole purpose of identifying the user) competent in the case concerned.

The **Electronic Evidence Regulation** covers subscriber data, traffic data and content data. It regulates the gathering of data stored by the service provider at the time of receipt of a European Production Order. It does not authorise interception of data or obtaining data collected after the receipt of the European Production Order.

WHAT DATA CAN BE REQUESTED?

Specific information (data) about **specific individual recipients** (users) **of the intermediary service** concerned who are identified in the order for the purposes of determining their compliance with applicable EU or national rules.

The requested information should be aimed at **enabling the identification of the recipients** of the service concerned (Recital 37 of the DSA).

Data that is **already collected**. No real-time collection of data.

Data within **control of the provider** (not necessarily physical possession).

GDPR

If the information requested by an order to provide information includes any personal data – which will virtually always be the case with the recipients of services that are natural persons – providers of intermediary services must justify any disclosure of such information to the authorities on one of the **legal grounds in Article 6 of the GDPR**.

The disclosure of personal data by the provider of intermediary services in the context of Article 10 orders could be in line with the legal basis set out in Article 6(1)(c) of the GDPR, in particular the need for the provider to comply with a legal obligation (as laid down in national laws of MSs that give competence to domestic authorities to issue such orders).

WHAT ARE THE MINIMUM CONDITIONS FOR ISSUING THE ORDER?

At the moment the order is sent to the provider of intermediary services, all orders must at minimum **include**:

- Reference to the **legal basis** for the order (relevant EU or national law);
- Identification of the **issuing authority** (including the contact details of a contact point within that authority where appropriate);
- Information enabling the provider of intermediary services to **identify the recipient** of the service concerned (e.g. account name, email address);
- **Statement of reasons**, including the objective for which the information is required and why the requirement to provide the information is necessary and proportionate to determine compliance by the recipients of intermediary services with applicable EU or national law;
- Information about **redress mechanisms** for the provider of intermediary services and the users concerned; and
- Information about the **authority to receive the follow-up** from the provider of intermediary services, if different from the issuing authority.

Statement of reasons should not be included (or should be adapted) when this information must be kept confidential under the applicable law for reasons of prevention, investigation, detection and prosecution of criminal offences.

Under the **Electronic Evidence Regulation**, the European Production Order must be necessary and proportionate for the purpose of the criminal proceedings. It may only be issued if it could have been ordered under the same conditions in a similar domestic case. Depending on the type of data requested, the Regulation sets out minimum threshold for the criminal offences for which the order may be issued. It must not be issued if the requested data is protected by immunities and privileges under the law of the addressed MS, or subject to rules regarding freedom of press and expression. The European Production Order must include the following information:

- The issuing and, where applicable, the validating authority;
- The addressee (service provider);
- The user;
- The requested data category;
- If applicable, the time range requested to be produced;
- The applicable provisions of the criminal law of the issuing State;
- In case of emergency, the justification for it;
- If applicable, justification for addressing the order to the service provider processing the data on behalf of the controller;
- The grounds for the necessity and proportionality of the measure (this information is not to be sent to the service provider concerned); and
- A summary description of the case (this information is not to be sent to the service provider concerned).

TRANSMISSION OF THE ORDER

The order must be sent to the **electronic point of contact** designated by the provider of intermediary services.

It must be in one of the **official languages** of the MS in which the provider of intermediary services is established or represented as declared by such provider or in another official language of the MSs bilaterally agreed on by the issuing authority and the provider. The order may also be drafted in the language of the issuing authority. In that case, the order must be accompanied by a translation of its most significant elements into the above indicated official MS language.

Under the **Electronic Evidence Regulation,** a European Production Order must be transmitted to the addressed provider through a European Production Order Certificate (EPOC) using decentralised IT system.

Where needed, the EPOC must be translated into an official EU language accepted by the provider, which must include one of the official languages of the MS where the provider is established or represented.

USER NOTIFICATION

Providers of intermediary services must i**nform the recipient of the services concerned by the data disclosure order of the order itself and the effect given to it** at the latest when effect is given to the order, or, where applicable, at the time provided by the issuing authority in its order.

The notification must also include a statement of reasons and the possibilities for redress.

In the context of criminal proceedings, the user notification obligation can be delayed in accordance with applicable EU or national law.

Under the **Electronic Evidence Regulation,** it is the responsibility of the issuing authority to inform the person whose data is being sought without undue delay about the data production. The issuing authority may, in accordance with national law, delay, restrict or omit informing the person whose data are being sought.

The addressed provider must always refrain from informing the person whose data is being sought.

Authorities should specifically include **a non-disclosure order and confidentiality requirements** when the order must be kept confidential under the applicable law.

DIGITAL SERVICES COORDINATOR

The role of the Digital Services Coordinator is to supervise the application and, where necessary, whithout prejudice to the Commission's powers, enforce the DSA.

The issuing authority must **transmit the order and any information received** from the provider regarding the effect given to that order to the Digital Services Coordinator from the MS of the issuing authority who must then forward a copy of the order to all Digital Services Coordinators.

This obligation may not apply in the context of criminal proceedings or may have to be adapted in accordance with the applicable national criminal procedural law.

WHAT ARE PROVIDERS OF INTERMEDIARY SERVICES OBLIGED TO DO?

Upon receipt of an order, provider of intermediary services must **without undue delay inform the issuing authority of its receipt and any follow-up** (if and when effect was) given to the order.

Relevant national and EU laws which serve as the legal basis for issuing such orders may introduce specific deadlines for the production of the requested information.

Only the **obligation of the provider concerned to inform the relevant authorities about the effect given to the order/provide feedback** on the order is subject to the enforcement rules set out in the DSA.

DSA itself does not oblige the provider of intermediary services that receives the disclosure order to comply with it and to disclose the requested information to the authorities. **Disclosure orders may only be rendered binding and enforced** (in case of non-compliance) **through national laws or *lex specialis* EU legislation.**

Under the **Electronic Evidence Regulation,** the service provider addressed by the European Production Order must in principle comply with the order, preserve the required data and transmit the required data to the issuing authority at the latest within 10 days, 8 hours in emergency cases, upon receipt of the order.

The **Electronic Evidence Regulation** also sets out the enforcement procedure which applies when the service provider does not comply with a production order without valid reasons and the enforcing authority has not invoked any of the (limited) grounds for refusal. The issuing authority can then request enforcement by the competent authority in the enforcing State. If the service provider does not comply with a recognised order, the enforcing authority must be able to apply a pecuniary sanction.

TRANSPARENCY OBLIGATIONS

In accordance with Article 15 of the DSA, providers of intermediary services, with the exception of micro or small enterprises, must issue an **annual transparency report**, including:

- The number of Article 10 orders received, categorised by the MS issuing the order;
- The median time needed to inform the issuing authority, or any other authority specified in the order, of its receipt; and
- The median time needed to give effect to the order.

First transparency reports of VLOPs and VLOSEs have already been published, providing an insight into their different interpretations of and compliance with obligations under Article 10 of the DSA. While certain VLOPs and VLOSEs report that they have received a considerable number of orders under Article 10 of the DSA in the reporting period, others report that they have not received any, allowing the authorities themselves to make the choice of submitting their data disclosure requests under Article 10 of the DSA or as voluntary requests.

WHAT ABOUT DATA RETENTION?

The conditions and requirements that apply to orders to provide information under Article 10 of the DSA should have **no effect on the retention rules under applicable national law, in compliance with EU law** (Recital 34).

Article 30 of the DSA however introduces a specific **retention obligation.**

DATA RETENTION OBLIGATION IN THE DSA

To whom does the data retention obligation apply?

Providers of online platforms which allow consumers to conclude distance contracts with traders are bound by this special retention obligation.

Providers of online platforms that qualify as micro or small enterprises are not bound by it.

What data is collected and retained?

This retention obligation aims to ensure the traceability of traders. It therefore **concerns only the data of traders.**

What are traders under the DSA?

Natural or legal persons, privately or publicly owned, who are acting for purposes relating to their trade, business, craft or profession.

Before online platform providers allow the traders to use their platforms to promote messages on or offer products or services to consumers in the EU, they must **collect the following information**:

- The name, address, telephone number and email address of the trader;
- A copy of the identification document of the trader or any other electronic identification;
- The payment account details of the trader;
- The trade register in which the trader is registered and its registration number or equivalent means of identification in that register, if applicable;
- Self-certification by the trader committing to only offer products or services that comply with the applicable rules of EU law.

What is the retention period?

The online platform provider must store this information in a secure manner for the **duration of the contractual relationship with the trader concerned and six months after its termination**.

The online platform providers can only **disclose the information** to third parties (including law enforcement and judicial authorities) when so required by applicable law, including **orders under Article 10** of the DSA.

Information concerning the trader's name, address, telephone number and email address; trade register information; and self-certification must also be made publically available in a clear, easily accessible and comprehensible manner.

NOTIFICATION UNDER ARTICLE 18 OF THE DSA

Under **Article 18** of the DSA, a provider of hosting services that becomes aware, for example through a notice by any individual or entity or through its own voluntary measures (e.g. provider's internal automated flagging mechanism), of any information giving rise to a **suspicion that a criminal offence involving a threat to the life or safety of persons** has been committed, is being committed or is likely to be committed, **must promptly inform the competent law enforcement or judicial authorities of such a suspicion and provide all relevant information available**.

This can include the content in question, for example a specific online post that gives rise to a suspicion of a threat to the public, such as incitement to terrorism. The provided information should also include the time when the content was published, an explanation of the suspicion and the information necessary to locate and identify the relevant recipient of the service.

Member State concerned

Member State concerned is considered to be "*the Member State in which the offence is suspected to have taken place, to be taking place or is likely to take place, or the Member State where the suspected offender resides or is located, or the Member State where the victim of the suspected offence resides or is located*".

What if the provider of hosting services cannot identify such a Member State?

The provider shall in that case inform the law enforcement authorities of the Member State in which it is established or where its legal representative resides or is established or inform Europol, or both.

Nature of the offences

The notification obligation under Article 18 of the DSA is limited only to **offences involving a threat to the life or safety of persons**, including but not limited to, offences concerning trafficking in human beings or terrorist offences as specified in the relevant EU legislation.

COMMUNICATION CHANNELS

SINGLE POINTS OF CONTACT

The DSA, in its Article 11, obliges all providers of intermediary services:

1. **To designate a single point of contact** to facilitate their **direct communication, by electronic means**, with:

- MSs' authorities,
- The Commission, and
- The European Board for Digital Services (an independent advisory group of Digital Services Coordinators on the supervision of providers of intermediary services).

The electronic points of contact **serve a purely operational purpose and do not require a physical location.**

Intermediary services providers which already have a dedicated mailbox for data disclosure requests of law enforcement authorities can "re-use" it for the purposes of the DSA.

2. **To publish and keep updated the relevant information** on the electronic points of contact, including the **languages** the authorities must use in communications with them.

What are the accepted languages?

At least one of the official languages of the MS in which the provider has its main establishment or where its legal representative resides or is established. Other specified official MSs languages.

LEGAL REPRESENTATIVES

The DSA (Article 13) obliges any provider of intermediary services established outside the EU but offering services within the EU:

1. **To designate a legal representative** in one of the MSs where it offers its services.

Many intermediary services providers have already designated legal representatives in order to comply with their obligations under other legal acts (e.g. GDPR).

2. **To provide up-to-date contact information** relating to their legal representatives to the relevant domestic authorities and **make this information publicly available and easily accessible**.

Provided the relevant requirements of the DSA are complied with, the legal representative can also act as a point of contact.

3. **To ensure that the legal representative has the necessary powers and sufficient resources** to guarantee efficient and timely cooperation with MSs' authorities, the Commission and the European Board for Digital Services, and to comply with any decisions adopted by them.

Legal representative's liability

The designated legal representative can be held **directly liable for non-compliance with DSA obligations**, without prejudice to liability and legal actions that can be initiated against the provider of intermediary services itself.

The **Electronic Evidence Regulation** requires access of service providers to a secure and reliable decentralised IT system. All written communications under the Regulation, including the exchange of requested data between competent authorities and service providers will have to be carried out through such a system with only certain exceptions.

The **Electronic Evidence Directive** requires that service providers that are not established in the EU but offer their services in the EU, appoint legal representative(s) in a MS; information must be made publicly available and regularly updated. The representative and the service provider can be held jointly and severally liable for non-compliance with the Electronic Evidence Regulation.

ENFORCEMENT OF THE DSA

ENFORCEMENT STRUCTURE

The oversight and enforcement of the obligations under the DSA are **shared between the European Commission and the MSs:**

1. The **Commission** is exclusively responsible for overseeing and enforcing the additional obligations to manage systemic risks that the DSA imposes on providers of VLOPs and VLOSEs.
2. The **Commission and the MSs** share the powers of supervision and enforcement of all other DSA rules applicable to VLOPs and VLOSEs.
3. For the rest of intermediary services providers, the task of supervising their activities and enforcing compliance with the DSA lies exclusively with **national authorities of the MS** in which the main establishment of the intermediary services provider is located.

MSs must designate at least one competent national authority to supervise and enforce the DSA and identify one competent national authority as their **Digital Services Coordinator**.

Digital Services Coordinators

The Digital Services Coordinators act as a **single point of contact** with regard to the DSA application for other national competent authorities, the Commission and the European Board for Digital Services in their respective MS.

The enforcement of the obligations under the **Electronic Evidence Regulation** lies with the enforcing State and its competent authorities. The enforcement procedure is triggered by the issuing authorities. Enforcement may only be denied on the basis of limited grounds.

SANCTIONS

1. FINES

Maximum amount of fines that may be imposed on providers of intermediary services for a failure to comply with a DSA obligation must **not exceed 6% of the annual worldwide turnover**, in the preceding financial year, of the provider of intermediary services concerned, or 1% in case of minor infringements.

Periodic penalty payments not exceeding 5% of the average daily income or worldwide annual turnover in the preceding financial year per day may also be imposed for failure to comply with certain obligations under the DSA.

Under Article 54 of the DSA, the **recipients of intermediary services also have the right to seek compensation** from providers of intermediary services for any damage or loss suffered as a result of an infringement by those providers of their DSA obligations.

2. TEMPORARY ACCESS RESTRICTIONS

In **particularly serious cases of infringements**, the Digital Services Coordinator of the competent MS can under certain conditions, request its competent judicial authority to order the temporary restriction of access of recipients to the service concerned by the infringement or to relevant online interface.

The **Electronic Evidence Regulation** envisages pecuniary penalties imposed by MSs in case of infringements. The pecuniary penalties provided for must be effective, proportionate and dissuasive. MSs must ensure that pecuniary penalties of up to 2 % of the total worldwide annual turnover of the service provider's preceding financial year can be imposed.

WHEN WILL THE DSA APPLY?

The DSA entered into force on 16 November 2022.

VLOPs and VLOSEs must comply with the obligations the DSA imposes on them **within four months of their designation**.

Following the first round of designations on 25 April 2023, VLOPs and VLOSEs had to start to comply with the obligations imposed upon them as of 25 August 2023. The European Commission designated 17 VLOPs and 2 VLOSEs that reached at least 45 million monthly users in the EU:

- Alibaba AliExpress
- Amazon Store
- Apple AppStore
- Booking.com
- Facebook
- Google Play
- Google Shopping
- Instagram
- LinkedIn
- Pintarest
- Snapchat
- TikTok
- Wikipedia
- YouTube
- Zalando
- Bing
- Google Search

On 20 December 2023 the European Commission adopted a second set of designation decisions, designating 3 VLOPs:

- Pornhub
- Stripchat
- XVideos

Following their respective designations as VLOPs, Zalando and Amazon, as well as Pornhub, Stripchat and XVideos initiated legal proceedings before the Court of Justice of the EU, challenging their designation as VLOPs.

As of **17 February 2024**, all other intermediary services must also comply with their obligations under the DSA.

This document was prepared using information obtained from publicly available resources and legislation in force at the time of writing.

Icons used in the document were designed by Freepik.

If you find the information in the document to be incomplete or incorrect, please contact the Eurojust SIRIUS team at:

sirius.eurojust@eurojust.europa.eu

Website:

https://www.eurojust.europa.eu/sirius

For a general overview of the DSA and its importance for the investigation of intellectual property crimes, see the factsheet developed by the Intellectual Property Crime Project at Eurojust: