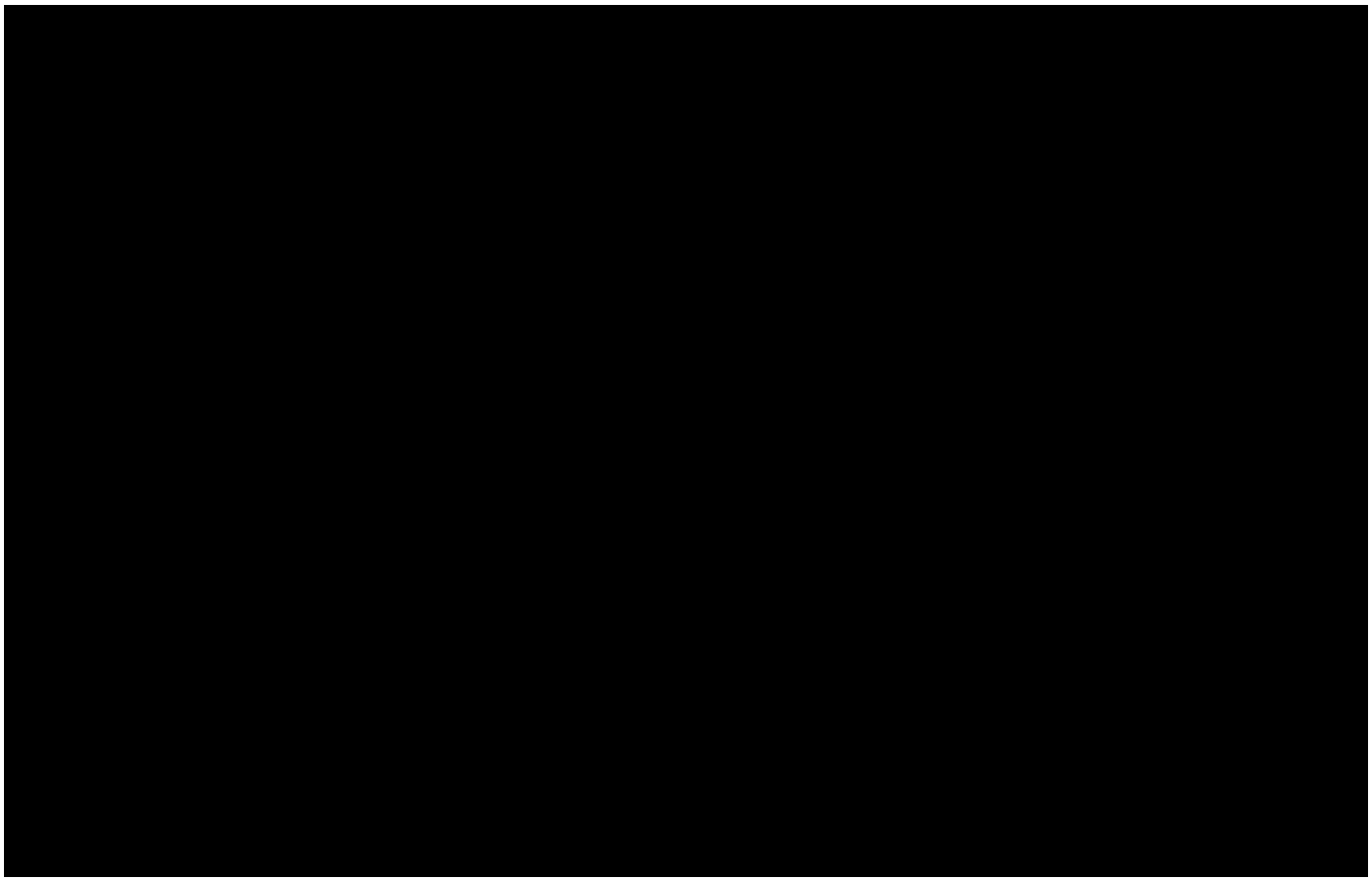
January 7, 2022



Digital Services Act

Article 13 b (new)

Text proposed by the Commission	*Amendment*
	Article 13b
	Traceability of business users
	1. A provider of intermediary services shall ensure that business users can only use its services if the provider of intermediary service has obtained the following information:
	(a) the name, address, telephone number and electronic mail address of the business user;
	(b) a copy of the identification document

of the business user or any other electronic identification as defined by Article 3 of Regulation (EU) No 910/2014 of the European Parliament and of the Council[1a];

(c) the bank account details of the business user, where the business user is a natural person;

(d) where the business user is registered in a trade register or similar public register, the trade register in which the business user is registered, and its registration number or equivalent means of identification in that register;

2. The provider of intermediary services shall, upon receiving that information and until the end of the contractual relationship, make reasonable efforts to assess whether the information referred to in points (a) and (d) of paragraph 1 is reliable and up-to-date through the use of any freely accessible official online database or online interface made available by a Member States or the Union or through requests to the business user to provide supporting documents from reliable sources.

3. Where the provider of intermediary services obtains indications that any item of information referred to in paragraph 1 obtained from the business users concerned is inaccurate or incomplete, that provider of intermediary services shall request the business user to correct the information in so far as necessary to ensure that all information is accurate and complete, without delay or within the time period set by Union and national law.

Where the business user fails to correct or complete that information, the provider of intermediary services shall suspend the provision of its service to the business user until the request is complied with.

4. The providers of intermediary services shall store the information obtained pursuant to paragraph 1 and 2 in a secure manner for the duration of their contractual relationship with the business user concerned. They shall subsequently delete the information.

5. Without prejudice to paragraph 2, the providers of intermediary services shall only disclose the information to third parties where so required in accordance with the applicable law, including the orders referred to in Article 9 and any order issued by Member States' competent authorities or the Commission for the performance of their tasks under this Regulation.

6. The providers of intermediary services shall make the information referred to in points (a) and (d) of paragraph 1 available to the recipients of the service, in a clear, easily accessible and comprehensible manner.

_____

[1a] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

Justification

The narrow approach of limiting Know Your Business Customers (KYBC) provisions to online marketplaces is a missed opportunity to ensure that the DSA provides a meaningful tool to address the broad range of illegal activities online.

KYBC obligations should apply to all intermediary service providers. A business cannot operate online without being hosted, or without advertisement and/or payment services. Requiring providers of intermediary services, having a direct relationship with the businesses concerned, to know the identity of their business customers would automatically reduce illegal content online in a minimally burdensome way.

A broad KYBC is clearly in line with the express objectives of the DSA, namely ensuring a safe, predictable, and trusted online environment for businesses and consumers. KYBC duties will impose minimal burdens on legitimate businesses, all of which are easily identifiable, and consumers will benefit from an online environment where business operators are easily identifiable.

Subsidiarity

Recital 26

Text proposed by the Commission	*Amendment*
(26) Whilst the rules in Chapter II of this Regulation concentrate on the exemption	(26) Whilst the rules in Chapter II of this Regulation concentrate on the exemption

from liability of providers of intermediary services, it is important to recall that, despite the generally important role played by those providers, the problem of illegal content and activities online should not be dealt with by solely focusing on their liability and responsibilities. ***Where possible, third parties affected by illegal content transmitted or stored online should attempt to resolve conflicts relating to such content without involving the*** providers of intermediary services ***in question. Recipients of the service should be held liable, where the applicable rules of Union and national law determining such liability so provide, for the*** illegal content ***that they provide and may disseminate through intermediary services. Where appropriate, other actors, such as group moderators in closed online environments, in particular in the case of large groups, should also help to avoid the spread of*** illegal content ***online, in accordance with the applicable law. Furthermore, where it is necessary to involve information society services providers, including providers of intermediary services, any requests or orders for such involvement should, as a general rule, be directed to the actor that has the technical and operational ability to act against specific items of illegal content, so as to prevent and minimise any possible negative effects for the availability and accessibility of information that is not illegal content***.

from liability of providers of intermediary services, it is important to recall that, despite the generally important role played by those providers, the problem of illegal content and activities online should not be dealt with by solely focusing on their liability and responsibilities. ***In many cases,*** providers of intermediary services ***are best placed to solve the problem of*** illegal content ***and activities by removing or blocking access to such content, particularly at the request of third parties affected by the*** illegal content ***transmitted or stored online***.

Recipients of the service should be held liable, where the applicable rules of Union and national law determining such liability so provide, for the illegal content that they provide and may disseminate through intermediary services. Where appropriate, other actors, such as group moderators in closed online environments, in particular in the case of large groups, should also help to avoid the spread of illegal content online, in accordance with the applicable law. Furthermore, where it is necessary to involve information society services providers, including providers of intermediary services, any requests or orders for such involvement should, as a general rule, be directed to the actor that has the technical and operational

ability to act against specific items of illegal content, so as to prevent and minimise any possible negative effects for the availability and accessibility of information that is not illegal content.

Parties with the technical and operational capacity to take action against illegal content must therefore ensure that third parties can identify them easily and contact them in order to combat illegal content.

Justification

Recital 26 unhelpfully states that where possible, third parties affected by illegal content transmitted or stored online should attempt to resolve conflicts relating to such content without involving the providers of intermediary services in question. However, this disregards the fact that intermediaries are often best placed to address illegal content in an effective manner.

Search

A single webpage or website may include elements that qualify differently between 'mere conduit', 'caching' or hosting services and the rules for exemptions from liability should apply to each accordingly." **[IN FAVOUR]**
For example, a search engine could act solely as a 'caching' service as to information included in the results of an inquiry. Elements displayed alongside those results, such as online advertisements, would however still qualify as a hosting service.

Justification

The DSA should not grant new liability privileges. Enhancing the accountability of search engines can be achieved through the introduction of effective due diligence obligations, not by granting them a broad and unjustified "safe harbour". Recital 27a suggests the possible qualification of search engines as "caching". Categorising search engines as "caching" providers would remove the incentive for search engines to fight against illegal content online.

Commission Guidelines

Request a split vote on amendment 106 on Article 1a (Scope)

1st part: Text as a whole excluding "4. By [12 months after… in Article 1a(3)" **[IN FAVOUR]**
2nd part: These words **[AGAINST]**

Justification

Article 1a calls for the publication of guidelines by the Commission to clarify any potential conflict between this Regulation and other Directives and Regulations. This approach aiming at addressing the lex specialis status in relation to the DSA lex generalis will cause more problems than it could resolve. A large amount of interpretation

will be necessary. This is not the role of the Commission, and which could put at stake existing current Union law legislation and create legal uncertainty.

Notice and Action

Request a separate vote on amendment 207 on Article 14 (3a) **[AGAINST]**

Justification

The DSA aims to increase safety and trust online by mandating online services to remove illegal content as soon as they become aware of illegal content, notably through a notice. Article 14(3a) directly contradicts this obligation and creates legal uncertainty by allowing illegal content to remain online despite having been properly notified to the online service. The DSA would therefore fail effectively to protect victims of illegal content, whether European companies or end-users, from malicious actors online or non-diligent online services.

Signatories