



Online Marketplaces under the DSA Non-paper

The European Commission proposal for a [Digital Services Act](#) (“DSA”)¹ upholds the cornerstone conditional intermediary liability framework, and introduces due diligence obligations for online intermediaries, including Know-Your-Business-Customer (“KYBC”) obligations for online marketplaces.

We appreciate the opportunity to contribute constructively to discussions surrounding the DSA. It is in that spirit that we are sharing this non-paper. Whereas we support the European Commission’s approach and the need to ensure a high level of consumer protection, we are concerned by attempts by some stakeholders to re-purpose the DSA, spoil its horizontal nature, and preempt parallel legislative deliberations on these issues via the [General Product Safety Regulation](#)² (“GPSR”). As we explain below, these stakeholders propose introducing a number of far-reaching requirements for online marketplaces, which completely disregard their intermediary nature and undermine SMEs’ viability and innovation at large.

In particular, we recommend:

- **Defining online marketplaces** explicitly in the text. We urge policymakers to follow the lead of the European Parliament Committee on Industry, Research and Energy (“ITRE”) and clarify that an online marketplace is “an online platform that allows consumers to conclude distance contracts with traders on the platform”.
- **Retaining the intermediary liability rules** for online marketplaces, as in the European Commission’s proposal. We urge policymakers to reject introducing amendments that, directly or indirectly, result in a loss of the hosting safe harbor for online marketplaces. Such proposals penalise innovation with liability, and risk harming consumers and European businesses.
- **Ensuring due diligence obligations** have regard for online marketplaces’ intermediary nature, are proportionate, and are not contrary to the prohibition on general

¹ European Commission Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services and amending Directive 2000/31/EC.

² European Commission Proposal for a Regulation on general product safety, amending Regulation (EU) No 1025/2012, and repealing Directive 87/357/EEC and Directive 2001/95/EC.

monitoring. We urge policymakers to reject proposals around **staydown obligations** and expansion of the KYBC obligations from traders to **traders' products**.

We also suggest redirecting product safety discussions to the recently proposed GPSR. The GPSR aims at regulating product safety on online marketplaces and is the better legislative initiative to tackle due diligence requirements. This will help ensure that the DSA maintains its horizontal nature.

Definition

The DSA proposal does not provide a definition for online marketplaces. It is implicit that online marketplaces are “online platforms that allow consumers to conclude distance contracts with traders”.³

For the sake of legal certainty, **it is important that a definition of online marketplace is included in Article 2 of the DSA. It is equally important that that definition is aligned with how online marketplaces are defined in other EU legislative instruments.** In particular:

- The recently adopted [Omnibus Directive](#)⁴ amends the [Consumer Rights Directive](#)⁵ to require that contracts concluded on online marketplaces fulfill specific information requirements.⁶
- The [NIS Directive](#)⁷ provides that “[a]n online marketplace allows consumers and traders to conclude online sales or service contracts with traders, and is the final destination for the conclusion of those contracts. It should not cover online services that serve only as an intermediary to third-party services through which a contract can ultimately be concluded.”⁸

³ See Articles 5 and 22 of the DSA.

⁴ Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules (“Omnibus Directive”).

⁵ Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (“Consumer Rights Directive”).

⁶ Article 4(5) of the Omnibus Directive.

⁷ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (“NIS Directive”).

⁸ Recital 15 of the NIS Directive.

- The [Regulation on Consumer ODR](#)⁹ defines online marketplace as “a service provider [...] which allows consumers and traders to conclude online sales and service contracts on the online marketplace’s website”.¹⁰

We are concerned by the fact that the European Parliament ITRE committee is the only one so far to have introduced in their report an amendment to align the text of the DSA with these legislative instruments. Lack of alignment does not just undermine legal certainty. It also risks causing regulatory fragmentation across the EU. National authorities could consider that online platforms that redirect consumers to third-party trader websites to conclude contracts there, must also be considered to be online marketplaces under the DSA. Inconsistent interpretations of what is an online marketplace would result in administrative burden and higher costs for online platforms, which is not in line with the harmonisation objective of the DSA.

We therefore recommend that the co-legislators follow ITRE’s lead and clarify that an online marketplace is “an online platform that allows consumers to conclude distance contracts with traders on the platform”.

Liability

We welcome the recognition in the DSA proposal that the conditional liability safe harbors are a foundation of the digital economy and should remain in place. Under the European Commission proposal:

- As hosting services, online marketplaces should not be liable for specific content they carry where: (i) they do not have knowledge of that content being illegal; and (ii) upon obtaining such knowledge, act expeditiously to remove or disable access to it.¹¹
- No safe harbor for consumer law infringements should exist, where online marketplaces present content or enable transactions in a way that leads consumers to believe that the content is provided by the online marketplace itself or a trader acting under its control.¹² We consider that this approach is in line with the requirements in the recently adopted [Omnibus Directive](#) for online marketplaces to inform consumers: (i) whether third parties offering content through the online marketplaces are traders or non-traders; and (ii) how obligations related to the contract are shared between those third parties and the online marketplaces.¹³

⁹ Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (“Regulation on consumer ODR”).

¹⁰ Article 4(1)(f) of the Regulation on Consumer ODR.

¹¹ Article 5(1) of the DSA.

¹² Article 5(3) of the DSA.

¹³ Articles 3(4)(a) and 4(5)(1) of the Omnibus Directive.

We are however concerned by proposals made in the European Parliament that effectively make it impossible for modern online marketplaces to rely on the hosting safe harbor. For instance:

- Some stakeholders propose that no safe harbor should apply to an online marketplace that plays an “active” role by providing assistance in optimising, classifying, organising, referencing or promoting the content at issue, or that has “control” over the content, including by the use of automated means such as algorithms.

We would note that **such proposals are at odds with the way modern intermediary services, including online marketplaces, operate. They penalise innovation with liability, and risk harming consumers by incentivising online marketplaces to remove helpful functionalities (e.g. that allow a user to search within product categories, or that recommend results on the basis of a user’s location).** These kinds of proposals also ignore the most recent [case-law](#) by the Court of Justice of the EU, which provides that the fact that an online platform automatically indexes content uploaded, has a search function, or recommends content on the basis of users’ profiles or preferences, should not cause it to lose the hosting safe harbor.¹⁴

- Other stakeholders propose that an online marketplace should not be able to benefit from the hosting safe harbor where the contract between the trader and the consumer is concluded through facilities provided by the online marketplace, or the online marketplace withholds the identity of the trader after the transaction, or the online marketplace uses payment systems that enable it to withhold payments by the consumer to the trader. They argue that such functionalities evidence that the trader is under the online marketplace’s “control”.

We would note that such proposals are counter-productive. **The possibilities for integrated payments, or the conclusion of contracts through facilities provided by online marketplaces, are highly advantageous for both third party traders and consumers. Third party traders get access to global markets with lower barriers to entry. Consumers benefit from more product choice, better security and additional helpful features.** There is no reason why these possibilities would result in traders being under the “control” of online marketplaces. The EU should opt for policy choices that allow online marketplaces to innovate and compete on such helpful features, instead of promoting policies that punish online marketplaces by removing the hosting safe harbor because they offer such features.

- There are also stakeholder proposals that an online marketplace should lose the safe harbor where it allows consumers to conclude contracts with non-EU traders, and there

¹⁴ Joined Cases C-682/18 and C-683/18, YouTube and Cyando, judgment of 22 June 2021, paragraph 114.

is no economic operator in the EU liable for product safety, or the appointed economic operator does not respond to consumer claims.

We would note that such an outcome would not only be blatantly disproportionate, but also cause legal uncertainty. First, under the [Market Surveillance Regulation](#),¹⁵ the obligation to appoint an economic operator in the EU does not apply to all products. Second, **it is simply impossible for an online marketplace to predict, when it onboards a trader, whether its appointed economic operator may or may not respond to future consumer claims. Such a requirement would in fact incentivise online marketplaces to block non-EU traders from using their platforms to reach EU consumers, and very likely amount to a breach of the EU's obligations under international trade rules.**

- Similarly, some stakeholders propose that an online marketplace should lose the safe harbor where it allows consumers to conclude contracts with non-EU traders, and the products do not comply with EU or national product safety rules.

We would note that this requirement is, again, disproportionate. It equates online marketplaces to compliance surveillance authorities, whereas in reality **products can change at any time without the online marketplace's knowledge.** In that sense, this requirement would also constitute a general monitoring obligation for online marketplaces, which is explicitly prohibited by the DSA.¹⁶

- Finally, there are stakeholders who propose that an online marketplace should not be able to benefit from the hosting safe harbor where it does not comply with DSA due diligence obligations.

We would note that this requirement evidences a serious misconception as to why the hosting safe harbor exists in the first place. **The safe harbor is not a “benefit” granted to hosting services, including online marketplaces. Rather, it is an expression of the basic legal principle that one may not be found liable for an illegal act it is not aware of.** More importantly, it is a fundamental rights safeguard, including the freedom to conduct a business and the freedom of expression.

In light of the above, **we urge policymakers to reject introducing requirements to the DSA that, directly or indirectly, result in a loss of the hosting safe harbor for online marketplaces.**

¹⁵ Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (“Market Surveillance Regulation”).

¹⁶ Article 7 and Recital 28 of the DSA.

Due Diligence Obligations

We stand behind the DSA objective to address the sale of illegal goods and services on online marketplaces. We do however **caution against the introduction of due diligence obligations that completely disregard online marketplaces' intermediary nature.**

a) “Staydown” Obligations

A number of stakeholders are calling for “staydown” obligations to apply to online marketplaces. These include, for example, requirements that online marketplaces:

- prevent the reappearance of illegal goods or services they previously removed from their platforms; or
- check traders' offers against lists of goods or services previously identified as illegal, prior to making them available on their platforms.

We would note that, other than the **general monitoring concerns** that these proposals raise, complying with such “staydown” obligations would also raise practical problems:

- In many cases, **the illegal nature of a product cannot be assessed by the online marketplace on the basis of previously removed products. The legal or illegal nature of a good or service may depend on elements that the online marketplace can simply not be aware of.** Think of products imported from another country without the permission of the IP owner (“parallel imports”);¹⁷ or the inclusion by a manufacturer of alleged patent-infringing technology in a product; or the inclusion by a developer of IP-protected content in an app without a license. These examples show that even identical listings on an online marketplace could require an independent assessment that could not be carried out via automated tools and technology, hence amounting to a disproportionate burden under the [case-law](#) of the Court of Justice of the EU.¹⁸
- Moreover, even if an online marketplace is in a position to conduct an independent assessment of a product without the use of automated tools, it may still not be capable of assessing whether the product is illegal. **Many online marketplaces do not have**

¹⁷ Under EU law, distributors may freely import IP-protected goods from one Member State to another, where the goods have been put on the EU internal market by the rightsholder or with its consent. The determination of whether a good has been “put on the market” is not always straightforward. For example, where a trademark owner provides products to distributors free of charge, the products are not deemed to have been put on the market. Consequently, the trademark owner can successfully prevent further distribution of these products in the EU.

¹⁸ Case C-18/18, *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, judgment of 3 October 2019, para. 45.

actual control of the goods made available through their platforms and cannot therefore carry physical inspections. Requiring them to do so would effectively require them to change their business model. This would create barriers to entry for new marketplaces, resulting in less competition and, eventually, less user choice. Such a requirement would also infringe online marketplaces' freedom to conduct a business.

b) Obligations to Know Your Business Customer's Products

Under the European Commission DSA proposal, online marketplaces are required to:

- collect certain information from *traders* prior to allowing them to make use of their services; and
- upon receiving this information from traders, make reasonable efforts to assess whether the information is reliable, by conducting own investigations or requesting supporting documents.

Where the online marketplace obtains indications that the information is inaccurate or incomplete, it must request the trader to correct it. Where the trader fails to do so, the online marketplace must suspend the provision of its service to the trader until the request is complied with.

Some stakeholders are arguing that this KYBC principle should not be limited to traders, but *also extend to their products*. In particular, they require that online marketplaces:

- collect information to allow the “unequivocal identification” of the good or service offered;
- confirm that the good or service offered complies with EU law (including as regards CE marking, warning and label requirements);
- run independent checks of the product information provided, both prior to publishing traders' offers and throughout their contractual relationship.

We are concerned that such requirements completely disregard the intermediary nature of online marketplaces. **Online marketplaces connect sellers and buyers to enable the purchase of products. As noted above, they usually do not have actual control of the goods made available through their platforms and cannot therefore carry out physical inspections. How are they to independently confirm the accuracy of any information a trader provides?**

Due to this intermediary nature, **it would be disproportionate to subject online marketplaces to the same due diligence obligations that apply to manufacturers, importers or distributors.** Requirements along the lines of verifying that a product bears the CE marking and is accompanied by the necessary documentation in a language the user

understands apply to distributors under the current regulatory framework,¹⁹ where the distributor is the seller *vis-a-vis* the consumer. Requiring online marketplaces to also do so would be akin to requiring the owner of a shopping mall to check compliance with EU law of every product different shops on its premises sell.

Online marketplaces should be subject to due diligence obligations that reflect that they are intermediaries, rather than sellers. A different outcome would unnecessarily duplicate regulatory requirements and blur the distinction between different actors across the supply chain. This would cause legal uncertainty and increase compliance costs, which would most likely be passed-on to consumers.

We would also note that subjecting online marketplaces to a disproportionate regulatory framework may have knock-on effects on the ability of SMEs to reach a broad consumer base, but also on the ability of consumers to benefit from wider product choice and lower prices. **Smaller third-party traders may be overwhelmed by the amount of information they need to provide to have their products marketed through online marketplaces. Online marketplaces may be incentivised to allow on their platforms large, established third-party traders since the risk of non-compliance is likely to be lower with those.**

A better way forward

The European Commission published its draft [General Product Safety Regulation](#) (“GPSR”) on 30 June 2021. This legislative proposal aims to update the applicable [General Product Safety Directive](#),²⁰ including with regard to sales made through online marketplaces. **We consider that the GPSR is the most appropriate instrument to address due diligence obligations for online marketplaces, and that the DSA should maintain its horizontal nature.**

If policymakers however wish to move forward with introducing specific due diligence obligations for online marketplaces in the DSA, we recommend a framework that both achieves the aim of securing a high level of consumer protection and accounts for the intermediary nature of online marketplaces:

- There are different kinds of online marketplaces, some of which may not have direct relationships with traders. For example, an online marketplace may have a direct contractual relationship with another online marketplace, rather than with the traders making offers available on that marketplace. **A KYBC obligation should therefore allow online marketplaces flexibility to collect the required information directly from the trader, or from partners that the trader works with and already collect this information** (e.g. other online marketplaces, payment processors).

¹⁹ See, for example, Article 13 of Directive 2014/53/EU on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment (“[Radio Equipment Directive](#)”).

²⁰ Directive 2001/95/EC on general product safety.

- Under the current legislative framework, not all traders are required to appoint an economic operator. **The requirement to collect information from traders about their economic operators under the KYBC obligation, should either be deleted, or only applied to products subject to the [Market Surveillance Regulation](#).**
- Online marketplaces should not be required to proactively collect information on products third party traders sell on their platforms. **They should rather design their user interfaces in a way that allows third party traders to directly include product-specific information in them. Traders should also be required to self-certify that their products comply with EU law.**
- Online marketplaces should be required to collect the KYBC information and to ensure that traders have inserted all required information about their products prior to making them available on their platforms. Online marketplaces should not however be required to run independent checks of this information. **Checks by online marketplaces should only be required *ad hoc* by market surveillance authorities, where the latter have reasonable safety concerns about particular traders or products.**
- **Online marketplaces should be required to remove from their platforms products identified as illegal by market surveillance authorities.**
- **The collection of information from traders through application of the KYBC provisions should not result in potential liability for online marketplaces.**

We appreciate the opportunity to discuss those alternative proposals in more detail in order to ensure that any regulatory framework for online marketplaces is proportionate, effective and ensures a high level of consumer protection.

* * *