BSA RECOMMENDATIONS ON THE EU DIGITAL SERVICES ACT

EXECUTIVE SUMMARY

BSA | The Software Alliance ("BSA")[1] is the leading advocate for the global software industry before governments and in the international marketplace. Our members[2] are enterprise software companies that create the technology products that power other businesses, offering tools such as cloud storage services, customer relationship management software, human resource management programs, identify management services, and collaboration software. BSA supports the development of relevant policy instruments and smart regulation that strengthen the Digital Single Market in Europe. In this context, we welcomed the Commission's proposal for a Digital Services Act (DSA) as a good starting point to update the rules provided by the 2000 E-Commerce Directive, and as it strives to strike the right balance between ensuring online responsibility and accountability, while allowing digital businesses to continue to grow and innovate.

BSA recommends for the EU co-legislators to focus on the below objectives to ensure a balanced and effective Digital Services Act:

1. Ensure that the tailored approach of the Commission proposal is maintained
2. Enact obligations that strengthen accountability while being proportionate and effective
3. Ensure that requests are sent to the entities best placed to respond
4. Clarify the concept of dissemination to the public
5. Provide for clear and compliance-friendly requirements
6. Allow for enough time to adapt to new rules

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry. Its members are among the world's most innovative companies, creating software solutions that help businesses of all sizes in every part of the economy to modernize and grow. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy. Follow BSA at @BSAnews.

[2] BSA's members include: Adobe, Akamai, Atlassian, Autodesk, Bentley Systems, BlackBerry, Box, Cloudflare, CNC/Mastercam, DocuSign, Dropbox, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Workday, and Zoom.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

ADOPTING A PROPORTIONATE AND EFFECTIVE DIGITAL SERVICES ACT

1. Ensure that the tailored approach of the Commission proposal is maintained

BSA welcomed the Commission's decision to maintain, in its Draft DSA proposal, the structure of the E-Commerce Directive, and **taking a tailored approach to the different obligations and requirements for the different categories of digital services**, based on the actual services they provide.

BSA recommends that it is essential that the Commission, the Parliament and the Council ensure that this structure is maintained during the legislative process leading to the final text. A one-size-fits-all approach that would impose the same rules on all digital services would create disproportionate burdens for many businesses that do not have the ability to view, access or moderate content, or do not disseminate content to the public. Many Business-to-Business (B2B) services providers, for example, do not offer content sharing services directly to end-consumers or the general public, and therefore may not have the ability to remove, edit or curate user-generated content that may appear online. A one-size-fits-all approach would therefore limit the uptake of cloud technologies across businesses and damage the broader data economy.

2. Enact obligations that strengthen accountability while being proportionate and effective

BSA strongly supports the European Commission's approach to the so called 'Know Your Business Customer' (KYBC) principle (articles 19 and 22 of the Draft DSA proposal), limiting its application to online marketplaces. **By taking a tailored approach, identifying and distinguishing the specific conducts that it intends to address** ("mere conduit" – Art. 3; "Caching" – Art. 4; "Hosting" – Art. 5), **the Commission ensures the protection of consumers by preventing dishonest businesses selling illegal products or services online, while avoiding applying inappropriate constraints on business-to-business (B2B) services or other intermediaries which are not directly involved in concluding distance contracts with consumers**. Setting stronger consumer protection rules should first take into account whether the digital services actively provide a business-to-consumer (B2C) good or service, while balancing the need to safeguard safe, smooth, swift and online business operations.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

We would **caution policymakers against expanding the proposed scope of these KYBC provisions and requiring that such obligations should be horizontally implemented by all digital services beyond "online platforms"** (as defined in Art. 2 (h)). The provision of core services to regulated sectors such as operators of essential services depends entirely on the ability to provide robust cloud solutions that are neither designed nor intended for consumers but rather to other businesses that will, in turn, sell products or services to consumers. Enterprise cloud-based solutions are often offered on a "Pay as You Go" principle, which has contributed to the success and security of the cloud, particularly among SMEs, start-ups and developers. A large number of those businesses rely on the scalability of cloud solutions to provide their services to their customers. Therefore, requiring extensive *ex ante* identification and verification checks on all businesses subscribing to cloud services, would create significant barriers to the delivery of cloud services in Europe. Moreover, many B2B cloud services already implement strong safeguards to prevent fraudulent businesses from using cloud services (e.g. contractual obligations in service contracts, security-based services against fraud). Additional and disproportionate KYBC requirements may not only raise privacy and business confidentiality concerns, but could discourage companies, particularly SMEs and start-ups, from moving to the cloud, if held up from accessing services pending KYBC checks and clearance.

For these reasons, BSA is concerned about the proposal of the European Parliament Draft Internal Market and Consumer Protection (IMCO) Committee Report to apply KYBC obligations to all intermediaries (new Articles 13a and 13b). Indeed, while we appreciate the need for strengthening consumer protection, **we do not see any justification as to how the European Parliament achieves this by extending the scope of KYBC obligations beyond what has been initially proposed by the Commission in Article 22**. As mentioned above, an extended scope would impose very burdensome and inappropriate constraints on B2B services that play little to no role in the proliferation of illegal content.

In that regard, BSA supports amendment 1372 put forward by a member of the EPP and amendments 1368, 1369, 1373 and 1375 as well as put forward by members of RE to limit the KYBC obligations only to providers of online marketplaces.

3. Ensure that requests are sent to the entities best placed to respond

The DSA proposal rightfully addresses different obligations to different online services. At the same time, BSA recommends ensuring that additional clarity is provided on which entities are supposed to receive and respond to requests for taking down illegal content. In the diverse digital ecosystem, many services under the scope of the DSA proposal are composed by several different layers, often provided by different entities. As the DSA would go to complement an already well-established body of law in the digital sphere, BSA recommends drawing from the example of existing legislation as the addressees of requests under the DSA

are defined. In this context, the GDPR has established **a well-functioning mechanism with the processor/controller distinction, whereby the data controller is the entity that "determines the purposes and means of the processing of personal data"[3] and the data processor is the entity that "processes personal data on behalf of the controller"[4].** This distinction would fit well the functioning of the DSA proposal, while obviously substituting the "personal data" requirement with "content". This would ensure that the entity closest to the management of the content is immediately addressed for requests of removal under the DSA, thus providing for the most efficient and effective method to take down illegal content. BSA also recommends including language that would mandate a responsibility for the data processor to act, if the 'data controller' is unable or unwilling to comply, or if the 'data controller' itself is the subject of an illegal content request.

As a way of example, many B2B service providers could be classified as "hosting" service under the draft proposal (Art. 5), which would entail compliance with the updated notice and action requirements and removal and information orders (Articles 8 and 9 of the draft proposal). Enterprise cloud providers are often not in a position to identify which of their cloud customers' users is associated with content posted online as they are not directly linked to, nor in direct contact with, the end-users, since it is their own cloud customers who are, in turn, in direct contact with their own customer that is the end-user. As a result, an enterprise cloud provider does not always have a direct relationship with the user uploading the alleged illegal content and may therefore not have the ability to identify the end-user itself nor, *a fortiori*, to take action on the data that is made public. Indeed, most of the time, the enterprise cloud provider would have to contact the cloud customer user who is able to identify the end-user, and then request the cloud customer to remove the illegal content. If there is no compliance on the latter's part, then the enterprise cloud provider would only have the option to terminate the overall service but cannot remove specific content.

For these reasons, in line with Recital 26 of the Draft DSA Proposal stressing that "*any requests or orders [of removal] 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*", **BSA recommends that the proposal includes language clarifying that requests for the removal of illegal content should be sent to the cloud customers first** (i.e. the data controller), as they are the ones in direct contact and relationship with the end user **and, only in second instance – should the cloud customer fail to reply or remove the illegal content – to the enterprise software provider** (i.e. the data processor), **to ensure that action can be taken swiftly, efficiently and by the most appropriate entity**.

[3] Art. 4(7) of the EU General Data Protection Regulation
[4] Art. 4(8) of the EU General Data Protection Regulation

4. Clarify the concept of dissemination to the public

BSA urges the co-legislators to provide additional clarity around the concept of "*dissemination to the public*" (article 2 (i) of the Draft DSA Proposal), which is instrumental in the distinction between hosting providers and online platforms. **The objective** of the Draft DSA **proposal is to ensure that digital services have clear and effective rules, while providing proportionate responsibilities which are tailored to a specific digital service and risk profile.** The current language used to describe the concept of dissemination to the public does not provide the necessary clarifications for all those services that host user-generated content whose defining characteristic is not the dissemination of content.

In this context, **BSA would recommend that the Regulation makes it clear that the dissemination to the public of content, as a condition to qualify as an online platform, should be an essential characteristic of the service**. Moreover, the dissemination should happen on the service that is to be qualified as a platform, not elsewhere. This clarification would also be closely linked with the language included at the end of Recital 14 of the proposal, whereby *"[i]nformation should be considered disseminated to the public within the meaning of this Regulation only where that occurs upon the direct request by the recipient of the service that provided the information*." Recital 14 implies a direct involvement of the recipient of the service to disseminate the content, but it does not clarify that such dissemination should happen on the service itself, in order to qualify as an online platform.

In that regard, we believe that IMCO amendments 249 and 697 (EPP), 245 and 250 (S&D), 242, 243, 695 and 705 (RE) as well as 237 and 246 (ECR) go in the right direction as they exclude cloud services from the scope of the definition of online platforms on the grounds that these services do not play an active role in the dissemination of content to the public. However, amendment 244 (RE) is not aligned with the above as it extends the scope of the dissemination to the public to include "f*ile-sharing services and other cloud services (…) to the extent that such services are used to make the stored information available to the public at the direct request of the content provider"* nor amendment 699 (EPP) which includes services that "*optimizes its content" disseminated to the public in the scope.*

5. Provide for clear and compliance-friendly requirements

BSA would caution against including overly prescriptive and burdensome requirements for all intermediary service providers in the final version of the DSA. As mentioned above, a key strength of the original proposal is its flexibility and its tailored approach to obligations and requirements for different services. The DSA would be missing its main objective if it leads to distracting precious content safety resources with compliance requirements that are unnecessary, overburdening or unfit for purpose.

This is particularly important with some suggested amendments to the IMCO Report.[5] Unlike the initial proposal from the Commission, which considered the diversity of the online ecosystem when proposing harmonised rules for all intermediary services, the IMCO report includes a number of additional obligations that would be neither proportionate for nor applicable to services that are not directed at consumers and do not disseminate content to the public, such as B2B cloud services.

Therefore, **BSA Recommends**:

- **Mandating a 24-hours timeline for "illegal content that can seriously harm public policy, public security or public health or seriously harm consumers' health or safety"[6] would create very significant burdens on service providers**, even more so as it does not distinguish on the type of service provided. More importantly, the determination of whether illegal content would qualify the above description, is left entirely to the service provider, with evidently significant compliance risks. In other words, service providers would have a very limited amount of time to determine whether content fits the above description, and then remove it. Moreover, the current formulation of the Draft IMCO Report would leave the possibility for all users to flag such content, therefore once again putting an unduly burden on the service provider to determine if the conditions are fulfilled and increasing the risk of over-removal of content. BSA recommends ensuring that the requirements for shortened timelines – if deemed necessary – are sufficiently clear, do not mandate an adjudicating role for service providers and provide for a safe harbour for good faith compliance.
- Additionally, the proposed additions by the Rapporteur regarding **Terms & Conditions (Article 12)** – which are clearly and rightfully meant at protecting consumers – do not reflect the realities of the B2B environment where terms such as "fair, non-discriminatory and transparent" are much too vague for business customers. Additionally, using graphical elements such as icons or images to illustrate the main elements of Terms & Conditions (T&C) should not be applicable to business contractual relationships, since there is already an obligation in this article for the terms and conditions to be presented clearly and in an easily readable format. Contracts are the bedrock of customer relationships in the B2B environment: business customers are very sensitive about the value of their data and have negotiating power, as opposed to B2C environments where users do not have a say on contract terms. This strengthens trust and increases transparency between the two parties. Additionally, contracts in the B2B space already include clear rights and obligations in terms of what services providers, can or cannot do with their customers' content and data.

[5] Draft Report on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD))
[6] *Ibid.* Art. 5(1a)(new)

Since this article is meant to be applicable to all intermediaries, it is **necessary to distinguish B2C from B2B services when inserting additional T&C requirements**.

6. Allow for enough time to adapt to and apply new rules

Article 74 of the Draft DSA Proposal currently provides for an application of the Regulation "*three months after its entry into force*". This timeline does not seem realistic from a business and governance and enforcement perspective as the DSA proposal will provide for a significant amount of new obligations in terms of reporting (both internally and externally), in relating to new authorities and in coordinating in trans-national cases. Businesses will also have to designate legal representatives and receive the necessary information from Member-States as to the established DSA Coordinators. **BSA recommends allowing for a period of 18 months after the Regulation's entry into force, which would offer enough time for businesses and Member States to adapt, include and apply the new rules.**