April 2021

A Single Market for Digital Services:
DOT Europe Questions and Recommendations on the DSA

Table of Contents

1. Introduction and Executive Summary

With the Digital Services Act (DSA), the European Commission has proposed a new package of rules with a view to creating a real Single Market for digital services. DOT Europe – the voice of leading digital, online and tech companies in Europe – welcomes this approach. We see the DSA as a real opportunity to establish a clear and flexible horizontal framework for all digital services, which provides legal certainty for stakeholders at large, without chaining itself to today's technological reality.

In January 2020, DOT Europe called on the European Commission to introduce a new Online Responsibility Framework to enable service providers to better tackle illegal content online, and we are encouraged to see that many of the points we raised then have been taken into account in this new proposal.

Moreover, some of the measures proposed in the DSA (collectively known as due diligence obligations) are not necessarily new concepts, and several online service providers make use of similar measures on a voluntary basis to tackle different issues on their services. Given this experience, and the diversity of services on offer, DOT Europe members have much to contribute to the discussion on the practicality and feasibility of the proposals in the DSA.

To this end, below we put forward some initial questions, examples, and recommendations on Chapters I to III of the DSA. We believe these questions will need to be considered by policy-makers when reading the proposed text, in order to derive all the benefits of this new regulatory approach and deliver a balanced and proportionate framework that addresses stakeholders' concerns, while supporting innovation in the EU Single Market.

2. Structure and Definition of Services in DSA: Concerning Articles 2 and 25

The DSA has the potential to establish a new approach to tackling illegalities online – one which takes account of the diversity of services in the online ecosystem and proposes asymmetric, proportionate, and tech-neutral responsibilities to address the challenges in the online space. This approach will ensure that EU rules take account of the different nature of online services, the kinds of content they deal with, and what they can and cannot do within the confines of the service offered. DOT Europe welcomes this approach but wishes to highlight the importance of the terminology and the precision of definitions in the DSA.

DOT Europe Questions:

- Article 2(d) addresses the question of geographical scope, and the concept of "offering services" in the Union or establishing a service provider's connection to the Union based on a "significant" number of users. ***What does a "significant number of users" mean in practice?***
- Article 2(g) sets out a definition for illegal content, which describes content as "any information, which, in itself or by its reference to an activity, including the sale of products or provision of services is not in compliance with Union law or the law of a Member State". This "reference" to illegal activity may have a broader than intended effect on content removal under the DSA, and indeed other existing instruments (such as the recently adopted Regulation for Preventing the Dissemination of Terrorist Content Online). ***What is the scope of this new definition of content? Does the content itself have to be illegal, or does legal content which happens to feature an illegal activity within the content file also qualify? Can the distinction between content/information and conduct be more explicitly recognised in the text?***
- Article 2(h) defines an "online platform" as a hosting service which "stores and disseminates to the public information" at the request of the recipient of the service. This definition determines the range of responsibilities a "platform" must take on board under the broader DSA framework. ***What does dissemination to the public mean in practice? Do policy-makers intend for it to be broader and refer, for example, to services which allow users to post content on the service itself, or do they also intend for it to refer to services which provide links for the sharing of information, but which can only be posted elsewhere outside of the service? Would the definition of "online platform" therefore exclude B2B intermediaries deep in digital supply chains, which provide technical services to providers disseminating public information?***
- ***How would the definition of an "online platform" in the DSA - which is focused on the storage and dissemination of content to the public - interact with the definition of an "online content sharing service provider" under the Directive on Copyright in the Digital Single Market?*** Under Article 2(6), the OCCSSP definition focuses on the "storage and sharing" of content to the public, but which explicitly excludes services such as electronic communications services, online marketplaces, cloud storage services, and open-source software sharing- and developing-services – to name a few.
- The definition of "online platform" in Article 2(h) also includes hosting services that store and disseminate to the public information unless such activity "is a minor and purely ancillary feature of another service". ***Under what circumstances would such activity be considered "minor" or***

"ancillary", and why the reference to "another" service? How does this affect, for example, IT infrastructure services (such as cloud infrastructure) which provide the underlying tools for online platforms to develop their own systems?

- ***How do policy-makers consider that infrastructure and enterprise services will fit within the scope of the DSA more generally?*** These services traditionally fall under Articles 12-15 of the e-Commerce Directive, but they cannot act on specific pieces of content for the purposes of the DSA and should not be considered "online platforms".
- Digital services are becoming increasingly sophisticated, with many different features and functionalities included within a single service, thus causing some uncertainties on the application of the DSA. For example, it is currently unclear whether the DSA is applicable to relevant ancillary features (e.g. hosting functionalities) of a main service that falls outside the scope of the DSA. ***How would policy-makers address the question of ancillary features which can appear in different services?*** Recital 15 of the DSA provides some guidance, but further clarification would be welcomed.
- Article 25 creates a category of "very large online platform" (VLOP) services, based on a threshold of a certain number of "average monthly active recipients" within the EU population. ***Given the importance of this threshold and the consequences it will have for service providers operating in the EU, is it appropriate that the criteria to determine the "average monthly active recipients" are left to be defined via delegated acts at a later stage? How does this sit with the very limited time period with which online service providers are provided to comply with the DSA?***
- ***Furthermore, how do policy-makers plan to clarify the definition of "average monthly active recipients"?***
    - ***Is it any individual who browses on a particular service?***
    - ***Must a user have a specific account with that service which enables them to post content on that service, or complete a transaction on that service? What about situations where one account gives access to various services?***
    - ***Must the user be an "active" user? What about dormant user accounts, are they counted as well?***
    - ***What about enterprise services? Does one license count as one user, regardless of the individuals using the license?***
    - ***Given the variety of users and the variety of ways they can interact with services, will the concept of "active recipient" or "user" differ by type of service provided?***

Examples:

- Re Article 2(d): There is a concern that the "significant number of users" criterion could produce unintended consequences. For example, it could inadvertently incentivise non-EU service providers to lock out EU customers who actively seek their services, in order to fall outside of the geographical scope of the DSA - thereby interfering with free trade and the free flow of ideas. Absent a clear definition of what "significant" means, the law would put active obligations on providers who cannot know whether they fall into the scope of the DSA, creating legal uncertainty.

But defining a fixed threshold that applies to all types of services would also be inappropriate, as different types of services (B2B vs. B2C, distance selling versus social media etc.) will by nature have different numbers of users and a different "significance" threshold. For example, for a web hosting service, five thousand users may be significant, while for a social network, five thousand might not be as significant.

- Re Article 2(g): Where a video is uploaded on a service, which itself is legal and the property of the user who created it, but which happens to capture a car breaking a national speed limit or a person stealing someone's bag in a crowded street, is this content deemed to be illegal content for the purposes of Article 2(g), as it refers to an illegal action? Similarly in the case of advertised products, where the product itself is legal, but the functionality described in the particular advertisement might be over-embellished, would this advertisement qualify as illegal content for the purposes of the DSA?
- Re Article 2(g): For short term rental platforms, determining illegal activity necessitates having a knowledge of highly specific and localised housing, tourism, and zoning rules, among other areas. Often, reports relate to alleged breaches of contractual obligations (e.g., of tenancy agreements) which a short-term rental platform cannot validate, and which generally do not constitute any breach of laws. In many instances, the determination of illegality depends on circumstances that exist outside of the platform, and of which the platform has no knowledge. Similarly, for products offered online, issues of illegality may again be connected to information that is not available to marketplaces. A mis-sized CE mark could make goods non-compliant, and therefore illegal. These elements have to be taken into account when considering what qualifies as illegal content under the DSA, particularly if that content is determined by the simple reference to an illegal activity – which can e.g. be based on a local law on fire safety or a fixed number of annual rental days.
- Re Article 2(h): In a situation in which an online service provider is trying to determine whether it meets the criteria to qualify as an "online platform" for the DSA: where a cloud service hosts content for a private user, but makes it possible for the user to create links to their files and share it with third parties on another service (making information available to the public directly within the cloud service's ecosystem would not be possible), would this qualify as dissemination for the purposes of Article 2(h)?
- Re Article 25: Where a user has created an account with a marketplace for a specific purchase, and some years later ends up creating a separate account on that same marketplace using a different email address, but the same delivery address, are they counted as a single user of a service or two users? Would their first account still qualify them as an "active recipient" of the service? Would the account holder have to use the account in the month/months of the assessment in order to "count" and if so, would this be accessing the service, spending time on it, or taking some active step with the content such as liking, commenting, posting, or purchasing? What about guest users who make a one-off purchase without creating an account, how would they be counted?

DOT Europe Recommendations:

- Despite the complexity of the task, it is essential that the DSA as a horizontal instrument also provides sufficient clarity to ensure regulatory certainty for all players involved.

- Concepts in Article 2 such as "dissemination to the public", "illegal content" and "minor and purely ancillary feature" will require clarification. Otherwise, the DSA will produce unintended consequences for online service providers which cannot possibly comply with elements of the proposal – e.g., due to the structural nature of the service offered, or for users whose content is uploaded which is technically legal but may inadvertently capture something that a service provider is forced to remove. Such a clarification should also specify that IT infrastructure services deeper in the internet stack (i.e. cloud infrastructure services, content distribution services, DNS services) are not considered "hosts" under the DSA, while B2C cloud services are not considered "online platforms" under the DSA.
- Another key component of the DSA will be the method used for defining VLOPs under Article 25 - this should not be left to delegated acts. The concept of "active recipient" under Article 25 will also require clarification. Additionally, Recital 54 refers to the numbers of "recipients of a platform" while Article 25 refers to the number of "recipients of a service" – there can be several services provided on a single platform, and this kind of discrepancy can be the deciding factor for a company trying to figure out what obligations they must comply with at EU law. Policy-makers must pay very close attention to the terminology employed in this Article, and indeed the overall DSA.

3. Liability Regime: Concerning Articles 3 - 7

We welcome that the DSA maintains the core principles of the e-Commerce Directive's limited liability regime and elevates them in the proposed Regulation. For the past 20 years Articles 12-15 of the e-Commerce Directive have provided legal certainty for the development of innovative services in the Internal Market and ensured the protection of fundamental rights in the online space. The DSA, as a horizontal Regulation, is a suitable vehicle to preserve these principles and build upon them. While there are some technical questions that will require clarification during the legislative debate, it is important for policy-makers to keep in mind the purpose of the liability regime and the role it continues to play for online services and users alike.

DOT Europe Questions:

- Article 5 of the DSA sets out the exemption for liability for hosting service providers, but deviates in paragraph (3) by stating that the exemption shall not apply "with respect to liability under consumer protection law of online platforms allowing consumers to conclude distance contracts with traders", where the information is displayed on the service in a manner that "would lead an average and reasonable well-informed consumer" to believe that the information/product/service is provided by the platform. ***What is the scope of paragraph 5(3) – what are "online platforms allowing consumers to conclude distance contracts with traders" and what is a "reasonable well-informed consumer"?*** Service providers are already required to disclose the status of a trader of a product or service under consumer protection law (in particular, the recently adopted Consumer Omnibus Directive), which would therefore indicate that that product or service is not provided by the service provider itself. ***As such, how will Article 5(3) of the DSA interact with those existing provisions?***
- Next, Article 5(3) refers to liability arising under consumer protection law, which appears to create a very specific liability regime for certain types of illegalities within a parallel liability regime

applicable to a subset of online services. ***What does this mean in practice? How will this provision interact with the Product Liability Directive, the Consumer Rights Directive, and the Directive on Contracts for the Sale of Goods?***

DOT Europe recommendations:

- Remove Article 5(3) of the DSA. Article 5(3) adds an element of subjectivity to liability law which does not benefit consumers, as they cannot determine in advance whether a court will find that they even have a claim against a marketplace in such a situation. Article 5(3) also lacks clear criteria on what is expected from marketplaces to avoid such a misperception in practice. Finally, Article 5(3) seems to only address liability from a particular vertical angle, which does not fit within the overall horizontal nature of the DSA. Where there are more specific issues relating to consumer protection and online marketplaces, they ought to be given due consideration and dealt with in a separate legal instrument, e.g. in the revision of the General Product Safety Directive. Policy-makers can thereby focus on the coherence of the DSA, and factor in what vertical initiatives need to be integrated into this new horizontal regime.
- Overall, the importance of the limited liability regime set out in Articles 3-7 of the DSA cannot be understated. It provides all service providers with the legal certainty to operate in the EU Single Market and puts in place checks and balances to prevent the general monitoring of users and protect their fundamental rights.
- Article 6 of the DSA proposal will be particularly important for the functioning of the DSA as a whole – by explicitly stating that service providers do not lose their limited liability protection through voluntary actions or any actions taken in order to comply with EU law, the DSA can provide service providers with the necessary legal certainty required to fully engage with the obligations in Chapter III of the DSA proposal itself - without facing legal liability for both action and inaction. For this reason, it should be clarified that the protection afforded by Article 6 of the DSA also applies to voluntary actions taken to enforce the online service providers' Terms and Conditions, whether by manual or automated means.

4. Orders to Act: Concerning Articles 8 and 9

Both Articles 8 and 9 of the DSA set out a system under which different Member State judicial or administrative authorities can issue orders for action or the provision of information to online service providers, regardless of whether that online service provider is established in the Member State issuing the order. While these Articles create more certainty for service providers about the necessary information to include in these orders, there are still a number of questions that need to be addressed.

DOT Europe Questions:

- ***How are Articles 8 and 9 going to work in practice, where an order is received for action or information on something that is illegal in the Member State issuing the order but is not illegal in the service provider's country of establishment?*** Article 8 also states that the Member State authority issuing the order can specify the scope of the territorial order for action. ***Does this mean that a single Member State administrative authority can request the removal of a piece of***

content in another Member State or at EU level? How do policy-makers hope to avoid unintended consequences such as the over-removal of content under this Article?

- ***How do policy-makers wish to address the absence of procedural rules to clarify how providers can challenge orders that are unsubstantiated, disproportionate, or unlawful?*** Service providers need clear and effective means to do so without having recourse to lengthy and costly court proceedings.
- ***How will a prioritisation of orders take place?*** Such a prioritisation is essential to ensure proportionality of the due diligence requirements, so as to prevent or minimise any possible negative effects for the availability and accessibility of information that is not illegal content. Policy-makers will also have to reconcile the fact that this may place additional burdens on the lead Digital Services Coordinator (DSC) of establishment, if they are required to take action in relation to a large number of (potentially unsubstantiated) orders. ***How would the redress mechanisms for content providers based in a different country to the Member State issuing the order, or the Member State in which the service provider is established, work in practice?***

Examples:

- For collaborative economy platforms (and short-term rental platforms in particular), platforms may receive orders not only from 27 national authorities, but from hundreds of local authorities across the EU. This raises practical questions for the applications of orders under Articles 8 and 9 - for short-term rental activity at European level, the takedown obligations of a platform can frequently lie in those instances where there is a cross-border element to the listing, for example, a French property listed on a Spanish platform.
- Continuing with this above example, what about the geographical scope of an order relating to a French property listed on a Spanish platform? Where a short-term rental accommodation listing of the French property does not meet the local requirements for fire safety and the Spanish authorities ask the platform to remove it, would the platform have to block access to it in Spain or France, throughout the EU, or take it down globally?

DOT Europe Recommendations:

- The country-of-origin principle (COO) is one of the central pillars of the EU's Internal Market and is what has made it possible for different online services to scale and provide their services to EU citizens at large, while only having to contend with the laws of one Member State rather than 27 Member States. The DSA is underpinned by a framework of cooperation and engagement between online service providers, national authorities, and DSCs, not to mention other stakeholders in the online ecosystem (e.g. trusted flaggers). Constructive engagement will be better supported where online service providers can, within a content oversight framework, develop working relationships with the authorities in their Member State of establishment. It is therefore of vital importance to the effective functioning of the DSA that policy-makers keep the COO principle and the overall objectives of the DSA in mind when making changes to Articles related to oversight and cooperation, including Articles 8 and 9 of the proposal.
- For the purposes of legal certainty, Article 9 should be aligned with the principles and requirements in the e-Evidence Regulation (which is at the final stages of negotiation), including

the need for harmonized legal frameworks for cross-border law enforcement requests within the EU, and strong procedural and substantive safeguards.

- Provisions related to requests for information should remain limited to information that the service provider collects to provide the service, and which lies within its control. Further clarification should be provided on the timeline for service providers to comply with requests for information, as well as ensuring that provisions on information sharing with the DSA remain without prejudice to existing data sharing legislation including the GDPR and the DAC 7 Directive. Orders to provide information should remain limited to specific items of information related to specific individual recipients of the service and should not be broadened.

5. Information on Content Moderation Practices: Concerning Articles 12 and 29

DOT Europe Questions:

- Article 12 sets out that service providers must make clear in their terms and conditions what restrictions they have put in place in relation to the use of the service, including "information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review". ***What clarity can policy-makers provide to ensure that service providers can know what information to include in their terms and conditions, without going so far as to disclose to bad actors how to bypass certain content moderation procedures? Could this obligation be fulfilled through links from the terms and conditions to other materials (e.g. Help Centres) to ensure that users are not bombarded with constant update notifications?***
- Article 29 requires VLOPs to provide more detailed information on the functioning of their recommender systems, specifically the parameters used in their recommendation systems. Similar to Article 12 above, ***how can policy-makers ensure that the information provided on the functioning of recommender systems will not be harnessed by bad actors who seek to game or defraud the system in order to harm consumers or give themselves an unfair advantage over competitors?***
- Articles 4 and 5 of the Platform to Business (P2B) Regulation refer to information which services within the scope of the Regulation must provide in their terms and conditions to business users, and the main parameters determining ranking on a service. ***How will policy-makers ensure that coherence is maintained between the DSA and the requirements under P2B, where several service providers will fall within the scope of both Regulations?***

Examples:

- Some marketplaces surface listings to potential buyers on the basis of a number of criteria, including location, "age" of the listing (i.e. when it was listed), and user history (i.e. what that user has previously been interested in). Sellers can sometimes try to game the systems – for example by editing or duplicating listings. If a marketplace provided full transparency into the precise details of the recommender systems, there is a concern that sellers would find it easier to game the system and buyers would see lower quality content.

DOT Europe recommendations:

- The granularity of the information required by both Articles 12 and 29 to provide clarity to users will need to be carefully considered by policy-makers and a balance will need to be found to avoid generating broader consequences.
- The target audience of the information under both Articles will also need to be considered. Given the paradoxical risks of providing bad actors with a guide on how to game service providers' systems, it is recommended that the disclosure of this kind of information in terms and conditions should be limited and focus on education and the building of trust among users.
- Language is required in the text to clarify that the service provider is not required to disclose information that, with reasonable certainty, would result in public harm through the manipulation of content moderation procedures or the disclosure of trade secrets, in line with the Trade Secrets Directive.
- Policy-makers should take into account that "recommender systems" can take many different forms they can also just refer to content that is organised in a particular way based on very objective considerations – a chronological recommender system is still a recommender system. Similarly, policy-makers ought to keep in mind that it will never be possible for a user to completely opt out of how a service provider presents content in some manner or another, in the same way it is not possible for a person going to a supermarket to completely rearrange the shelves there. User choice on how information is presented also helps to build both a greater understanding of the functioning of online services and provides more control over a user's online environment. For example, many online service providers already offer users options to switch the view of content to chronological order, by the most popular interactions, or by other preferences, in the same way a shopper can choose to walk around a supermarket using whichever route they prefer.

6. Notice and Action Rules: Concerning Articles 14 and 15

Online service providers rely on a notice and action regime through which users and stakeholders can submit notices relating to the illegal content or activity they encounter on the service (many service providers also employ a separate system for content that is not illegal but violates terms of service, e.g. nudity). Notice and Action is an important tool for effective content moderation for many service providers, and the DSA provides an opportunity to provide further clarity and harmonization to these processes. That said, the DSA proposal significantly lowers the evidence threshold required to trigger the legal obligation on an online service provider to act on a notice. While the intention is to provide clarity, this formulation increases the risks to online service providers and highlights the importance of setting clear limits on what qualifies as a notice, and on when must it be processed according to the new DSA rules (as failure comes with such significant penalties). The DSA will need processes with sufficient flexibility to match different models of operations as well as to ensure resilience against abuse.

DOT Europe questions:

- ***Did policy-makers intend to equate all substantiated notices with actual knowledge under Article 14(3)?*** As drafted, there is a concern that Article 14(3) will give rise to a situation in which

a service provider is incentivised to potentially remove notified content out of caution - even where the content notified is not actually illegal, or the report itself is evidently wrong or dubious in nature, in order to retain their limited liability protection. This significantly lowers the evidence threshold for take-down and creates a wide scope for the abuse of third-party rights by bad actors.

- ***Do policy-makers consider that an unsubstantiated notice still qualifies as a "notice" within the meaning of Article 14? Also, what about duplicate notices? Should these also be processed?*** While Article 14 refers to the criteria for a substantiated notice, it does not specify how a service provider would identify such a notice nor a process to follow. Indeed, in paragraph 6, it is mentioned that "any notice" should be processed following the mechanisms set out in Article 14 without indicating if an unsubstantiated notice is still considered a notice and needs to be processed pursuant to this Article.
- ***Recognising that notice and action mechanisms under Article 14 are applicable to both hosting services and "online platforms", which respectively could include IT infrastructure services and the online platforms operating on them, how will the DSA ensure subsidiarity of obligations?***
- Some policy-makers wish to go beyond simple notice and action rules for certain types of service providers or illegalities and introduce a notice and stay-down rule instead. ***How would policy-makers reconcile this approach with the prohibition on general monitoring maintained in Article 7 of the DSA?***
- ***How much detail must a service provider include in a statement of reasons under Article 15? What clarity can policy-makers provide to ensure that service providers can know what information to include in their statement of reasons, without going so far as to disclose to bad actors how to bypass certain content moderation procedures?*** While this is considered to some degree in Article 9, this is not specified here.
- The P2B Regulation already covers the statement of reasons for online services providers in relation to their business users. ***Will there be some coherence made between the statement of reasons to be provided for business customers and end consumers under Article 15 of the DSA?***
- ***How would policy-makers avoid scenarios in which the provision of an overly detailed statement of reasons may give rise to data protection concerns, or may obstruct investigations (there is no exception for criminal activities that may be(come) subject to investigations)?***
- ***Regarding Article 15(4), what is "a publicly accessible database"? What is the intention of having such a database, bearing in mind the burden this puts on service provides to compile and provide this information (e.g. removing personal data from every single statement of reasons prior to publication)?***
- In the case of an online service provider which allows a user to post comments or content without creating an account, or other means of communication (e.g. email or phone number), ***how would the service provider approach the user with all the information related to the statement of reasons?***

Examples:

- A service receives a 100-page fax with URLs and other elements of an otherwise valid notice contained within the overall document. Does a fax of a notice qualify as one of the "electronic

means" of submission for the purposes of Article 14? Would systematically ignoring such communications leave a service open to penalties under the DSA? If they received 100 or 1000 of these per day, would this change the answer?

- In a marketplace context, there is a significant concern of anti-competitive practices connected to that absolute power given to any notice issuer. What prevents a seller from notifying all the product listings of its main competitors one day before Black Friday? Article 20 on notice abuse unfortunately does not seem sufficient to address these concerns, especially if in parallel Article 14(3) gives rise to actual knowledge regardless of the notice, its source, or its contents. The most likely outcome will then be over-blocking by the service provider of the notified content.
- In relation to the Article 14(3) and the concept of "actual knowledge": imagine a scenario in which a substantiated notice is submitted to a service provider for a piece of video content. A notifier alleging that the video contains illegal hate speech would give the service provider actual knowledge of this potential illegality under Article 14(3), but what if that same video contains another possible infringement - e.g., an IP infringement - which was not the subject of the notice, would this still count as actual knowledge for the purposes of Article 14(3)? Continuing with this example, in the event that the service provider reviews the notice for illegal hate speech, determines that there is insufficient information to substantiate the allegation, and consequently leaves the video online, would the service provider then be liable for the IP infringement, which was also in the video file notified, but which was not the subject of the notice and which the service provider could not assess?
- Policy-makers will also need to consider the different kinds of services that will be applying these notice and action rules. For many services, the mobile experience is very important as it is the main user interface. These services often use in-app notices in order to create a frictionless reporting experience for users, which may at the same time also limit the information display capabilities. By extending the information provision requirements under Article 15, some service providers may have to collect personal information such as email addresses and move away from an in-app notice system.

DOT Europe recommendations:

- While Article 14 defines sound criteria for a notice to be considered as substantiated, another element of information is needed in the notice in the case of infringement of intellectual property rights: the identification of ownership. This is essential for effective and efficient processing of notices dealing with this type of illegal content since only the rights owner will know if there is a license in many situations.
- Policy-makers should clarify in Article 14(3) that a notice that ticks off all the elements of a substantiated notice does not, in itself, give rise to actual knowledge. A substantiated notice does not necessarily mean that a service provider has actual knowledge of an illegality – policy-makers are encouraged to keep in mind that a substantiated notice can be submitted to an online service provider including all of the necessary elements listed in Article 14, but service providers need time to assess a notice and identify valid information (e.g. in defamation cases). Following assessment, it may still be the case that the content notified is perfectly legal. If this wording is not adapted, this could mean that immediately after receiving the substantiated notice the service provider should immediately remove or disable access to the disputed content, in order to avoid

liability. Firstly, this would lead to a risk of over-removal of content. Secondly, it does not fully safeguard third-party rights in the way the e-Commerce Directive does today. Thirdly, an online service provider should have the choice not to act on a piece of content it considers valid, and this decision should be considered an action - in addition to removing or disabling access to content.

- In fact, it is recommended that "action" should constitute any service provider response on the notice, be it via action taken on the content, the decision not to act against the content, or via updates provided to the notice issuer following the service provider's assessment of the notice.
- For the purposes of both Articles 14 and 15, it should be clarified that a service provider should not face liability where it takes a good-faith decision to leave up notified content where it believes that content is not (obviously) illegal, nor when it makes a good-faith decision to take down content based on a notice which it believes to be justified.
- To ensure subsidiarity of obligations and avoid incidental take down or disabling of legal content, notice and take down mechanisms under Article 14 should first be directed towards the service provider with direct access and control over the specific piece of illegal content in question, e.g. because IT infrastructure providers do not have technical capabilities to remove or disable individual items of content - and if compelled by the DSA may have to disable entire websites or domains.
- In terms of any extension of Article 14 into a notice and stay-down regime, policy-makers should also take into account that a notice and stay-down approach is akin to a general monitoring obligation. This is because it would require the service provider to search all uploads for specific notified infringements – general monitoring is about who is monitored, not what a service is looking for. The ban on general monitoring – as maintained in the DSA - forms an important part of the foundation of rules for online service providers in the Internal Market, protecting not only the freedom of expression but also the right to privacy and the freedom to conduct a business. Some argue that a notice and stay-down obligation would equate to a specific rather than a general monitoring obligation, due to a narrow scope which would only oblige a service provider to check for a specific illegality rather than every possible illegality. However, even if a notice and stay-down obligation were to only apply to previously notified content, this would still oblige a service provider to check every user upload for the presence of that specifically notified content. Moreover, where it is the use of the content and not the content itself which leads to the alleged illegality, a service provider would be required to make frequent assessments of every use of that piece of content across its service. Policy-makers should keep the importance of Article 7 of the DSA in mind and consider the relationship between the principles of the initial e-Commerce Directive and the aims they set out to achieve – a specific monitoring obligation cannot be employed in either a legal or practical sense as a means of bypassing this rule. Policy-makers should instead consider how to ensure that there are safeguards in place in the DSA for service providers to proactively come up with a variety of solutions to address the issues with previously identified infringing content. A legal safeguard like that of Article 6, which ensures that service providers can take these proactive actions without losing their limited liability protection, will avoid this conflict with Article 7 of the DSA.
- Regarding the information to be published in the statement of reasons, Article 15 would benefit from the addition of some of the same conditions as in Article 9(2)(a) in terms of necessary and

proportionate information, since this publicly accessible information could enable bad-faith actors to circumvent the measures service providers have put in place.

7. Transparency Reporting: Concerning Articles 13, 23, 24, 30 and 33

There is an ongoing debate on the opacity of service providers' decision-making, their automated tools for content moderation, the reach of the ads they feature, and any additional measure they take to tackle illegalities that might arise on the service. Transparency reporting is a useful tool to help stakeholders understand the efficacy of the systems service providers put in place, and to share information with experts to consider how to improve on existing practices.

The DSA aims to take a graduated approach to transparency reporting, to place proportionate burdens on online service providers. Proportionality is a crucial factor when considering these transparency obligations, not just in respect to the size or reach of a service but also considering the nature of the illegalities that might arise on a service, the types of content a service interacts with and what they can or cannot disclose based on the inherent architecture of the platform. The underlying purpose and intended audience of the transparency reports will also need to be considered for each different proposal in the DSA, if this is to be a flexible framework for all service providers, which does not result in unintended consequences and create cost, burden and risk without achieving the objectives of the DSA.

DOT Europe questions:

- ***What kind of transparency outputs do policy-makers want, and to what end?*** Articles 13, 23, 24, 30 and 33 all propose different transparency obligations for different service providers, depending on the size and reach of the service, but the audience for the transparency reports is not considered. Moreover, Article 13 would require transparency reporting by all intermediaries without exception. This is a vast range of intermediaries - some performing narrow functions deep in the digital supply chain and which would never receive a DSA notice - yet the same reporting obligation is placed on those services as on a consumer-facing service which allows users to upload unlimited self-generated content.
- ***Are the transparency reports on take-down volumes and appeals rates intended for general users or are they for the DSCs who will be overseeing the DSA framework? Would DSCs have capacity and resources to supervise so many reporting entities and scrutinise their transparency reports?***
- Articles 13, 24 and 33 will require a massive variety of online service providers to develop transparency reports on an annual or six-monthly basis. ***What level of granularity will be required for these reports, bearing in mind the frequency of these reports where these are twice a year? Will aggregate data be acceptable, and can this be specified in the text of the proposal? At what point is a saturation of information reached where meaningful transparency is no longer possible?***
- ***Will the DSCs be legally responsible for reading these reports in order to discharge the duties of their role under the DSA?***

- Bearing in mind that significant information on specific risks could cause vulnerabilities in service provider systems, ***are policy-makers willing to accept aggregate risk trend reporting as sufficient information for the broader public under Article 33?***

Examples:

- For some marketplaces, many of the non-compliant listings are not in relation to illegal content, but in violation of other terms of service, e.g., a Handmade Policy. This can be reflected in how these marketplaces report on policy enforcement currently and should remain the focus if top violations are those to their terms of service, especially if policy-makers want the transparency report to really showcase the breadth of problem of illegal content on services.
- Context is also required when looking at outputs in transparency reports. For example, on a live streaming platform the quantity of content taken down may be rather low, which is not necessarily an indication of low enforcement but simply the ephemeral nature of the content. This is similar for a marketplace and a social network – both services are very different, and a reporting framework would have to take this into account.

DOT Europe recommendations:

- As a starting point, policy-makers are encouraged to consider the unintended consequences of these transparency obligations: regardless of whether one looks at the rules for "online platforms" or "VLOPs", transparency reporting should not assist ill-intentioned users or bad actors to circumvent service providers' content moderation measures and procedures. This possibility is considered in Article 33(3) for the transparency obligations on VLOPs, but it is no less of a concern for "online platforms" or hosts in general.
- Consequently, policy-makers should take a problem-specific approach when determining where they would like to see increased transparency and the level of detail required, reflecting on the audience of the transparency reports for each of the different proposals in the DSA. There should be a clear distinction made between data that is provided to authorities for enforcement purposes versus data that is aggregated and published for the general public. It should also be considered that the public disclosure of certain types of data in transparency reports could be commercially sensitive, for example when it comes to the sharing of the number of users of a service per Member State as suggested in Article 23(2) of the proposal. The granularity of the transparency reporting will need to be considered by policy-makers, taking these potential consequences into account. The Recitals of the DSA could perhaps include language specifying the intended audience of the transparency reports under the different Articles of the DSA, to provide legal clarity and guidance to service providers in terms of what they would have to share and how.
- Policy-makers will also need to determine where there is added value in having such transparency reports outside of what is already being done, particularly given the sheer volume of reports that are likely to be generated under the DSA. There are already many examples within the industry, where there is a great deal of transparency with customer-facing information on the working of recommendation systems, privacy notices on the use of their data and a number of regular reporting on content moderation etc.

- Policy-makers should also take into account that these general transparency rules will apply to many different types of services, and flexibility will be required. Specifically regarding Article 13, these general reporting requirements are likely to apply better to some services than others, so the outputs in a transparency report will need to be viewed in the context of the service provided and the content involved. Percentage reporting is advisable to give a clearer picture on the volume of notices received, take-downs, etc.
- Policy-makers must keep in mind that there is no "magic button" which will enable a service provider of any size to automatically pull and deliver the data in the right structure and format of a transparency report. Transparency requirements should take this into account (e.g. in Article 24 of the proposal) and be proportionate and flexible when it comes to the format of the actual reports for any of the proposals in the DSA, to avoid a situation in which, for example, a service provider has to pull resources from pressing issues on content moderation to formatting for transparency reporting. Some service providers will encounter more violations of terms of service than illegalities, some will have more resources and access to information about the nature of their services than others, and many service providers will have to build data retention systems for repositories for online advertisements, complaint handling and reinstatement of content etc., so these technical considerations need to be kept in mind when looking at these rules.
- Policy-makers should give due regard to the characteristics of an online service provider when defining requirements, so that specific data points will make sense and provide meaningful information. Where there is a case for using equivalent metrics, this should be allowed.
- Another point to consider is the idea of transparency reporting obligations applying more broadly, for example, by extending the obligation to certain parties submitting notices to online service providers such as rightsholders, trusted flaggers, governments, competent authorities, out-of-court settlement bodies etc. It would be useful to have more information on where notices are filed, the numbers, the rejection rates and the sort of issues notified (e.g. types of rights, goods and content, infringement in question) - to enhance cooperation among stakeholders and optimise notice and action procedures.
- More generally, it is recommended that the tasks and objectives of the DSCs are clearly set out in the DSA (as in, for example, the Electronic Communications Code) - this could include objectives around market observation and the assimilation of information and learnings based on the transparency reports submitted by online service providers.
- With respect to Article 30, a number of service providers today offer public-facing ad archives as a means of ensuring more transparency to their users and public interest researchers. Efforts to bring more transparency to the online advertising ecosystem are to be encouraged but must be mindful of the fact that not every service is the same and that some targeting parameters may be too sensitive to disclose. In reflecting on the ad transparency provisions of the DSA, policy-makers are encouraged to maintain consistency with the various other legislative and non-legislative discussions where ad transparency is a topic of active debate, notably the impending legislative proposal on political advertising and the Code of Practice on Disinformation. To ensure legal certainty and standardisation, the various initiatives should maintain a connected approach as to how ad archives are understood and implemented at a technical level.

- Finally, with respect to Article 33, reports on aggregate risk trends ought to be the aim of this transparency obligation, to avoid the disclosure of specific information on risks and mitigation measures inadvertently causing new vulnerabilities. Such information can disclose methodologies and be used to circumvent technical measures.

8. Complaint Handling and Dispute Resolution: Concerning Articles 17 and 18

DOT Europe Questions:

- ***How do the proposals in Articles 17 and 18 relate to or interact with the Alternative Dispute Resolution (ADR) Directive, the Online Dispute Resolution Regulation, and the mediation aspects of the P2B Regulation, or the alternative dispute resolution provisions in the Copyright Directive and the Audiovisual Media Services Directive? Are dispute settlement bodies needed in addition to the court system and existing alternative dispute resolution systems established under these instruments?***
- Experience from the P2B Regulation shows ***that these dispute mechanism bodies do not necessarily exist, how will this experience be built up and these bodies developed? Will there be different types of bodies for different services or types of content?***
- There does not seem to be a COO approach to engagement with out-of-court dispute settlement bodies in Article 18; ***does this mean that a service provider will have to engage with different dispute-settlement bodies in the 27 Member States? Is there a risk that these provisions will lead to fragmentation, or that national authority removal orders under Article 8 could end up being reviewed under alternative dispute resolution procedures?***

Examples

- Some marketplaces' first interactions under the P2B Regulation resulted in mediation cases which were about different policies and law – which posed significant difficulties as each mediator per case is supposed to have expertise in the relevant policies and laws.
- Bad actors could use ADR to arbitrate every content removal at a company's expense and could thereby slow down the process for legitimate seekers of redress. Article 18 opens up avenues for this abuse and does not scale to the millions of decisions online service providers make.
- The use of ADR by content uploaders to review any content moderation decision is highly likely to result in contradicting decisions by different ADR bodies in different Member States as regards the same laws, issues or policies, or national authorities' removal orders. As such, Article 18 could lead to fragmentation and confusion. Given the scale of content moderation online service providers engage in, trying to make sense of a patchwork of often contrasting decisions by different bodies across the EU risks paralysing online service providers' content moderation systems

DOT Europe Recommendations:

- In general, users should go through internal complaint handling systems - as required by the DSA – first. These systems can then be overseen by the regulatory framework proposed in the DSA to avoid unintended consequences.
- Per Recital 16, where the service provider acts on the basis of a notice, or on the order of an authority, any ensuing dispute should be exclusively between the notice submitter/authority and the affected recipient, as the service provider does not necessarily have all the facts that led to the notice/order and is acting at the submitter's request. Service providers must have a choice about whether to interact with a dispute settlement body (for example where that body is unable to deal with disputes in a language used by the service provider) and they must be able to challenge a dispute settlement body designation if that does not meet the criteria set out in the DSA.
- Clarity would be welcome as to the possibility for parties to challenge the conclusion of a dispute settlement body in the event that a party disagrees with the outcome, in order to maintain full access to justice.

9. Trusted Flaggers: Concerning Article 19

Like transparency reporting, collaboration with trusted flaggers is one of a variety of methods service providers can use to improve their content moderation. That said, it should not be presumed that the use of trusted flaggers is a consistent standard across all types of online service providers – the efficacy and value of these types of collaboration depend greatly on the nature of the services offered and the kinds of content on a given service. The DSA proposes to make the use of trusted flaggers more typical for all types of "online platforms", but there are some important questions to consider for Article 19, to make sure that the mandatory integration of trusted flaggers into existing systems does not do more harm than good.

DOT Europe Questions:

- ***Will there be a set list of criteria which will be used to assess the expertise of applicant trusted flaggers across all EU Member States in order to guarantee a certain level of knowledge and experience in the relevant fields? Will there be a vetting and evaluation mechanism in place, and who will be involved in this process?*** Given online service providers' experience in working with trusted flaggers, ***is there room for online service providers to be involved in the selection process?***
- If a specific Member State determines that it wants to appoint trusted flaggers who focus on a specific set of issues, ***will there be limits or restrictions placed on Member States, to prevent service providers from becoming overwhelmed by an unmanageable number of partnerships with trusted flaggers?***
- ***Will all notices submitted by a trusted flagger receive the prioritization mentioned in Article 19(1) irrespective of which service or type of content they are directed at and if so, will the criteria which determine the eligibility of an applicant to become a trusted flagger reflect the need for expertise across all types of digital services and content? Alternatively, will a trusted flagger's priority be limited to certain issue areas and if so, how will this be organised***

- Given that there appears to be no limit to the number of trusted flaggers that the Digital Service Coordinator of a Member State can appoint, ***is there not a risk that this could create an imbalance between how many trusted flaggers are appointed in each Member State?*** Also, taking into account that the 'mandate' of a trusted flagger is not limited to his or her country of origin, ***could this not lead to situations in which numerous trusted flaggers from the same Member State could flood a service's inbox with notices regarding content that might be illegal in their state but is perfectly legal in the country of origin of the service, essentially blocking out other, more relevant notices?***
- Given that there may be more experts in some issue areas than in others, ***is it not likely that this imbalance of expertise will be reflected in the number of trusted flaggers dealing with the different types of illegal content? If so, how will it be ensured that the trusted flagger model will not become a system in which some types of illegal content are quickly detected and dealt with due to a large number of trusted flaggers whereas other issue areas are drowned out due to being represented by fewer trusted flaggers?***
- On a similar note, ***given that services must give priority to notices submitted by trusted flaggers, will they no longer be available to prioritise notices which are related to the most urgent, or more serious issues?***
- ***Where online service providers currently work with trusted flaggers, they often engage with them and develop dialogues to follow-up or get clarifications - will this be possible under the DSA?***
- ***Will the Digital Services Coordinators be responsible for training trusted flaggers on company-specific services and reporting mechanisms?***
- In order to foster the systemic use of trusted flaggers and ensure the continued efficacy of the work carried out by trusted flaggers - ***do policy makers envisage adding a reporting obligation for the trusted flaggers to provide clarity on their work on an annual basis?***

Examples:

- In the case of IP-related "flags", would a trusted flagger have to demonstrate that they own the rights for the relevant claim, or would it be sufficient for a trusted flagger just to hold the status of trusted flagger, to have experience in counterfeit notices? For example, could a trusted flagger acting on behalf of Nike then notify a counterfeit issue to a marketplace regarding a possible infringement of Adidas' IP.
- Overall, it is to be expected that there are more people with an expertise in IPR than people with an expertise in e.g., terrorist content. Therefore, it could become the case that a large part of notices that are submitted by trusted flaggers deal with IPR which in turn could 'drown out' any notices concerning other types of content or result in a local imbalance in the type of illegal content notified on the service and, potentially, on the content taken down.

DOT Europe Recommendations:

- Service providers will need to be able to process notices flexibly, depending on the nature of the notifier and the nature of the alleged illegality notified. For example, certain types of illegalities

can require a more urgent response (e.g. CSAM, or activity which would give rise to material and bodily harm), and these will have to be prioritised above notices from trusted flaggers. More clarity and flexibility are needed in the proposal, since Article 19 currently states that the notices coming from trusted flaggers should be dealt with more urgently than other notices. Specifically, service providers should be able to deal with certain types of illegalities which require an urgent response (such as child sexual abuse material or terrorist content) as quickly as possible, bypassing the queue of notices submitted by trusted flaggers on less crucial issues.

- Given the status of trusted flaggers' notices and their foreseen role under the DSA, objective vetting criteria for the appointment of trusted flaggers will be needed to ensure the accuracy of this system. Moreover, as online service providers have some experience in working with trusted flaggers, some clarification would be welcome as to how service providers can be involved in the process of awarding trusted flagger status.
- Limitations on the number of trusted flaggers appointed per type of expertise and competence of each Member State will be necessary, to ensure that the system of trusted flaggers remains efficient and does not overflow the normal notice and action systems of the online service providers.

10. Repeat Offenders: Concerning Article 20

DOT Europe Questions:

- ***What do the terms "frequently", "manifestly illegal content" and "gravity" mean for the purposes of Article 20?***
- ***How does this proposal interact with the fairness to business users principle established in P2B?***

DOT Europe Recommendations:

- Article 20 should provide the flexibility for the online service provider to assess whether or not to adopt measures against misuse of their services. If an online service provider wishes to process and consider all notices for illegal content submitted to it (regardless of whether the notifier previously submitted manifestly unfounded notices or not), it should be able to continue doing so – assuming the risk that this may entail in terms of liability.
- Conversely, while it may be appropriate in some circumstances to take into account proportionality and to issue prior warnings, in some very severe cases (e.g., provision of child pornography, attempted sale of illegal drugs) one violation can be enough to justify the suspension of an account.
- In addition, Article 20(3)(d) should be deleted, as it would require online service providers to evaluate the "intention" of the alleged abuser, which would entail a subjective assessment which service providers are not appropriately placed to investigate or judge.

11. Suspicious Criminal Activity: Concerning Article 21

DOT Europe Questions:

- ***How broad is the scope of Article 21?*** It is presumably relating to illegal content and activity given the intended scope of the DSA, but it is not clear at what point a service provider can be reasonably certain that a threat to life and safety is "likely to take place" for this obligation to kick in. ***What is actually expected of an online service provider in order to identify "suspicious criminal behaviour"?***
- What does 'any information giving rise to a suspicion' represent – ***what type, and format, of information should be acknowledged as being in scope?***
- ***What will be done with the information provided to law enforcement? Will law enforcement authorities be required to provide details on actions taken?***

Examples:

- Under this Article, any violation of the restrictions on public gathering and events that have been adopted by Member States in the context of COVID-19 could be considered as a criminal offence and would have to be reported by an online service provider.

DOT Europe Recommendations:

- The breadth of the obligation in Article 21 is unclear and potentially far-reaching. Policy-makers should clarify what constitutes a "threat to life", and how a service provider is to determine when a threat is "likely to take place", and what "reasonable certainty" will mean in practice.
- For coherence, it is advisable that explicit reference be made to existing definitions, e.g. under the Directive on combatting CSAM, and that this provision better aligns with the similar obligation under the recently adopted Regulation on Addressing the Dissemination of Terrorist Content Online.
- There is a concern that the requirement under Article 21 risks breaking trust with the users of a service, where the service provider mistakenly reports incorrect suspicions or because services become required to report all suspicions about users to the authorities. This Article should therefore be tightly drafted and take account of the above questions and concerns.
- It should also be made clear that there is no resulting constructive liability for situations that are not notified to law enforcement by a service provider – reasonableness and proportionality should always be considered.

12. Traceability of Traders: Concerning Article 22

While Article 22 of the DSA does not propose a new concept, it is proposing to elevate a "know-your-trader" (KYT) proposal to a mandatory EU-wide obligation, which can have more far-reaching consequences. The final rules in the DSA will need to be clear, privacy-friendly, and proportionate. They will also need to be supported by the right infrastructure, to be scalable while enabling the businesses of all sizes to thrive.

DOT Europe questions:

- The process of screening traders against publicly available databases for this obligation can be costly and operationally burdensome - ***how would policy-makers maintain proportionality in the application of this obligation, and ensure it does not amount to a general monitoring obligation, especially as the information may change over time? Also, what kind of databases do policy-makers have in mind?***
- ***Do policy-makers foresee that a harmonised agreement on the kind of "identification document" required will be possible?*** For example, EU VAT and EOIRI numbers can be checked for validity but not for whether the person providing them is the owner.
- ***How do policy-makers want to reconcile the verification of information about traders with the current requirements under the Consumer Omnibus Directive?***
- ***Why would a marketplace need to check bank account details if the trader has already been subject to financial KYT under Anti-Money Laundering obligations? If a trader agrees to the payment provider confirming their details to the marketplace, would this not be sufficient for the purposes of the DSA, given that the checks already conducted by the payment service provider?***
- ***To what degree is the identity of the economic operator of value to the end-user, considering this is product-specific information and this identity has nothing to do with the "traceability" of the trader?*** There is a concern that the obligation in Article 22(1)(d) could introduce a monitoring obligation for one specific legal requirement and product type (as there is no general obligation for a product to have an economic operator).
- ***Does the self-certification mechanism in Article 22(1)(f) shift the liability for product safety to the trader?***
- ***What are "reasonable efforts" in the context of Article 22(2)?*** Random checks would be appropriate, as a systematic verification of any changes to the trader information would quickly amount to impermissible general monitoring.

DOT Europe recommendations:

- The definition of "trader" in Article 2(e) of the DSA corresponds to that of Article 2(2) of the Consumer Rights Directive and should not be altered during the legislative process – it is important that the DSA takes account of existing EU legislation, to create a coherent framework for online service providers.
- It should also be made clear that the KYT obligation is not intended to refer to business-to-business configurations, including those where the business customer is in fact the end user of the service. This is a real concern for services using a "pay-as-you-go" model, e.g. cloud-based software services, which allow anyone to open a "business account" using a credit card and email address, and begin operations for their "business, craft or profession". In such a case, it is not feasible for the service provider to have to check the credentials of every individual who wishes to purchase a licence for use by their team of collaborators, or a department within their company or their own business.
- Continuing the coherence point, alignment should be made between the KYT requirement in the DSA and existing legislation in other fields of law which already prescribe rules for data collection,

verification and reporting of users by online service providers. These include the Anti-Money Laundering Directive and Transfer of Funds Regulation, and the Directive on Administrative Cooperation in the Field of Taxation (the newest revision DAC 7 is to be adopted by March or April 2021, which includes obligations for platform operators). Some additional elements should be examined more carefully and where possible aligned with existing legislation:

  - Method of verification: Flexibility is needed in order to allow services to automatise the process. To make this proposal workable and proportionate for service providers of all sizes, the verification of traders' identities could be done against publicly available databases as an initial verification. These databases will also need to be both scalable and accessible to avoid blockages. Where EU VAT and EOIRI numbers are not available, there should not be an obligation to fall back on documents which services are not in a position to assess. This process could be followed by document-based verification being a manual process, and therefore more recommended as a second rank. Alternatively, a system based on users' self-declaration could be established whereby business users are required to declare their details to a service provider in order for the service provider to then perform their checks based on any traceability rules. Service providers should also be empowered to adopt a risk-based approach to determine any cadence for rescreening of business users.
  - "Kick-out mechanism": Flexibility should be given around the point at which the service provider is forced to block the trader in case of non-compliance with KYT rules. As an example, under the DAC 7 Directive, the seller can get two reminders prior to the block. Moreover, service providers should not incur liability or be forced to stop providing services to a user based on mere suspicions. The mere fact for a user to provide incomplete or inaccurate data under due diligence requirements does not constitute proof of illegal behaviour on the service, at least until an authority issues a formal notice on the matter.

- When it comes to reporting, authorities should provide simple and secure ways for service providers to report data, and for their data to be treated following the submission of a report. Transparency or other reporting requirements to authorities can sometimes hinder the quality, relevance, and security of the shared information. Situations can arise in which data structure is not clearly established or even processed by authorities (e.g. systems may fail to absorb high volumes, or to recognize non-Latin characters even when the data is of global nature). The aim should be to adopt standardised technical requirements, whereby service providers are able to automate and ensure the security of the transmission, while retaining flexibility to allow the service provider to develop systems best suited for their services as well.
- The "economic operator" in goods legislation is not logically connected to the "trader" in the DSA - a trader will have many products with different economic operators, and the economic operator is the same for a product no matter who sells it. This concept should remain in the vertical corpus of law related to goods and should not be confused with the obligations in the DSA. As it stands, the proposal in relation to economic operators in Article 22 of the DSA goes beyond the final text of the Compliance and Enforcement Regulation, as the economic operator's information is required to be displayed despite the fact that the economic operator is not intended to have compliance obligations vis-à-vis end users, and service providers will need to "vet" the economic operator's information, which is difficult to do when there are no guardrails on who can serve in

this capacity in the EU. Moreover, marketplaces do not have a relationship with economic operators and there is no public register. In addition, the product scope of these DSA obligations is not clear as these requirements appear to apply to all offers, rather than being limited to CE-market products (as in Article 4 of the Compliance and Enforcement Regulation). This would potentially require low risk products (like books and apparel) to have a designated economic operator in the EU for the purposes of the DSA.

- As such, Article 22(1)(d) relates to the goods, not the trader. Only the first trader to sell a particular product on a particular marketplace would logically need to provide such documentation, creating an unfair burden on that first seller. There is no database of the contacts sought in 22(1)(d). The contact under the Market Surveillance Regulation is accountable to a regulator for producing documentation, not for responding to members of the public. In addition, it will be virtually impossible for online service providers to chase verification of this information down the value chain.

13. Risk Management: Concerning Articles 26 to 28

DOT Europe Questions:

- Article 26 obliges VLOPs to carry out risk assessments for systemic risks, which can be tailored to the service, but which could be very far reaching given the diversity of the issues – actual or foreseeable – which a service provider needs to monitor. ***What parameters would policy-makers put on these risk assessments? How can a VLOP recognise what is a foreseeable risk, versus an anomaly on the service?***
- ***Would policy-makers consider specifying what is meant in Article 26 by risks to the "protection of public health, minors, civic discourse, or actual or foreseeable effects related to electoral processes and public security" more concretely? Moreover, given the subjectivity of some of these categories, will the determination of risk be based on the law of the land in a VLOP's country of establishment, or on their terms of service?***
- Given the subjectivity of some of the risks specified in Article 26(1), there is a strong possibility that the scope of risk-mitigation measures will extend beyond illegalities and attempt to tackle content that is potentially harmful but is not necessarily illegal under EU or Member State law. ***How do policy-makers envisage that this can be achieved in such a way, without the service provider's risk-mitigation actions themselves posing a risk to the exercise of fundamental rights on a platform, thereby undermining the purpose of Articles 26 and 27?***
- ***What kind of auditors do policy-makers consider have the sufficient expertise and resources to carry out audits within the meaning of Article 28? Will these auditors be obliged to consider standards of reasonableness and proportionality when making operational recommendations within the meaning of Article 28?***
- A one-year timeframe for audits will be challenging, given the scope of the audit tasks. If external audits remain mandatory in the DSA, pushing out the timeframes to every two or three years could also help meet the auditor supply challenges. ***What is the timeframe for the audits, and is there some flexibility foreseen?***

- ***How would the risk factors relating to human rights overlap or differ from the non-financial reporting obligations around business and human rights that are horizontal across all businesses, and which are also currently under review?***

DOT Europe Recommendations:

- Articles 26 and 27 are drafted in such a way as to recognise the diversity of services in the ecosystem and the variety of tools needed to combat specific risks. This flexibility is very important to the overall success of this approach and must be complemented by the safeguard proposed in Article 6 of the DSA to ensure that the VLOPs taking steps to mitigate any identified risks can do so with the necessary assurances and legal certainty. It is also advisable to consider how service providers might use other initiatives to demonstrate accountability and effective risk management and mitigation in the context of these Articles. For example, some service providers make use of safety advisory bodies or transparency centres or provide regular public updates on any changes to terms or service or community guidelines – these additional mechanisms could help to reduce possible pressures stemming from the frequency of reporting for all parties.
- The scope of risk mitigation should be focused on illegalities and should not extend into content that is harmful but not necessarily illegal – to avoid possible adverse consequences for the exercise of fundamental rights on these services (at least until such a time as a clear and workable DSA framework is in place, and this issue could then be re-examined).
- Even at this stage of the legislative process, policy-makers should consider who could fulfil the role of "auditor" for the purposes of Article 28. Under the P2B Regulation, service providers were required to find "independent mediators" to comply with those new rules – it has proven very difficult to find mediators who have the necessary expertise to carry out the role prescribed under P2B, and who are also independent. Given that these auditors will play a central role in the framework of the DSA, it will be necessary to reflect on whether a sufficient number of expert independent auditors actually exist – or where they can come from – to make this work in practice.
- Adopting a risk-based approach to audit findings is also recommended, to support the development of action plans and remediation. For example, rather than 'positive, positive with comments, or negative' assessments (as is currently proposed in Article 28(3)), the risk-based tiers could be: (i) no/limited control gaps/findings, with observations; (ii) medium control gaps/findings - 12-month remediation timeline; (iii) high control gaps/findings - six-month remediation timeline; (iv) critical control gaps/findings - three-month remediation timeline.
- To support the usefulness of the findings of the independent auditors, especially given the large scope proposed in Article 28(1), the DSA should provide mechanisms to facilitate areas of more specific focus in a given auditing period. For example, this could include DSCs providing an annual plan that identifies to VLOPs and their auditors' key areas of interest for the upcoming reporting period.
- Given the voluntary nature of Codes of Conduct, it is also recommended that these frameworks should be excluded from the scope of audits under Article 28(1), and that reporting and verification processes be tailored to each of the Codes of Conduct instead.

14. Compliance: Concerning Articles 31, 32, 34, 35, 36, 37 and 57

DOT Europe Questions:

- Article 35 indicates that regulators will have wide powers to issue rules on illegal and indeed lawful content through future Codes of Conduct, which in some cases appear to be strongly recommended if not mandatory for certain VLOPs. ***How can policy-makers ensure that these recommendations are reasonable and proportionate? How frequently can they be updated to better reflect innovations in the ecosystem, thereby ensuring that this element of the DSA framework is future-proof as well?***
- Given that the provisions under Articles 31 and 57 relate to highly sensitive commercial data, ***what safeguards do policy-makers foresee for both provisions***?

DOT Europe Recommendations:

- Given the extent and sensitivity of the data that must be provided to the DSC and the Commission under Article 31, it is strongly recommended that the technical conditions under which VLOPS are to provide this data are not left to be defined by delegated act. The data which would be shared under this provision would be commercially sensitive, and consequently any technical requirements under which this would take place should be part of the DSA Regulation itself.
- For data access in Article 31 more specifically, it is suggested to:
    - Define "reasoned request" to set parameters around what information can be requested and shared with vetted researchers, in line with the GDPR data-minimisation principle. It is also recommended to include transparency around the funding vetted researchers receive as part of the vetting process, as “commercial interests" might not cover researchers who, for example, have major academic projects funded by competitors or critics of the “very large platform” at issue.
    - Allow online service providers to take additional measures to protect the privacy of data subjects (e.g., through pseudonymisation), where appropriate.
    - Set limits on what can be done with the data and clarify that the data should not be further shared/disclosed, in line with the GDPR purpose-limitation principle.
    - Consider how to ensure that the conditions under which data sharing may take place respect necessary security standards.
- All service providers should have the opportunity to engage in Commission’s process for the development of Codes of Conduct pursuant to Article 35. Given that the definition of VLOP is currently based on the proportionate calculation of a service provider’s users in the EU, and that this can change rapidly for an online service provider, to only involve VLOPs in the development of the Codes (from the service provider side) would run the risk of developing codes that new VLOPs could not comply with, based on their resources or the nature of the services they provide.
- Article 35 should also set out the broad boundaries within which the Codes would be developed. For example, no Code should mandate general monitoring or require additional trader traceability measures.

- It is also recommended that an element of flexibility is preserved for the development of Crisis Protocol obligations as described in Article 37. Efforts to facilitate and encourage better protocols in crisis situations is welcome, but there is a concern that specific measures taken during a crisis might be taken out of context or used as a means to regulate service providers through the backdoor at a later stage. For example, a situation in which monitoring is introduced on the back of a specific crisis protocol is not desirable and runs the risk of bypassing proportionality checks and safeguards for user privacy and fundamental rights – this would be incompatible with Article 7 of the DSA and would undermine the horizontal purpose of the framework.
- Article 57 relates to highly commercially sensitive information. Providing explanations over databases and algorithms in response to information requests by the Commission would be more proportionate than granting direct access and would help to provide useful insights for those who might be less familiar with the workings of those specific algorithms. In addition, such information requests should only be directed to online service providers on the basis of a non-compliance investigation and under strict confidentiality safeguards.

15. Other Considerations

DOT Europe Recommendations:

- In keeping with the horizontal nature of the DSA, should a situation arise in which there is a need for fines or penalties, these should be used by the DSCs to tackle systemic breaches of the due diligence obligations, not individual infringements, and should only be pursued in the event of a breakdown of dialogue between the parties.
- The Commission and the DSCs will all play a significant role in the framework this proposal establishes. This new oversight and enforcement system is essential to the overall functioning of the DSA as a new regulatory approach. Consequently, more clarity on the tasks and objectives of these parties would be welcome, particularly on the operation of COO under the envisaged cooperation framework between DSCs in different Member States under Articles 45-46. This clarity will help to ensure that the DSA can be a success as a flexible and tech-neutral horizontal instrument to establish a Single Market for digital services in the EU.
- On Article 74, it is recommended that policy-makers consider extending the implementation period for this Regulation. The DSA proposes a new framework for all stakeholders, and its success will depend on the ability of all the parties in the chain to effectively play their role. Service providers will need time to prepare the operational changes mandated by the final DSA, and much will also depend on the capabilities of the DSCs and their resources.

With this paper, DOT Europe aims to raise constructive questions for the ongoing debate on the DSA. These questions and conversations will likely evolve, but we believe these practical questions need to be a part of these early considerations, in order to achieve a balanced and workable framework for all stakeholders.