Priorities for the EU Digital Markets Act and Digital Services Act

Ensure open, fair, trusted, and competitive European digital markets and services

May, 2021

Contents

Executive Summary

Executive summary

- Ibec engaged in national and EU consultative processes on the development of the European Commission's 'digital services package'. This paper presents Ibec recommendations to EU co-legislators on the further development of that package, including the Commission's proposed Digital Markets Act (DMA) and Digital Services Act (DSA).

- Ibec support efforts to increase trust in further digital transformation and to protect businesses and people online. We support free and fair competition and efforts to ensure Member States, businesses, and citizens can reap the benefits of a Digitalised Single Market. We support a clear, robust risk-based and evidence-based approach that addresses illegal content and behaviour on digital services and promotes competition in digital markets in line with the EU's economic goals.

- **Recommendations on the Digital Services Act (DSA):**
    - Maintain legal certainty for business, encourage continued investment. Ibec welcomes the Commission's proposal to preserve key principles of the eCommerce Directive (ECD), including country of origin; conditional liability limitations for online intermediaries; and no general monitoring obligations. Good Samaritan provisions to enable voluntary own-initiative investigations is also welcome.
    - Harmful (but legal) content should not form part of the liability regime and the DSA due diligence obligations should not lead to regulation via the backdoor of lawful content . Online platforms should also be enabled to moderate such content according to their policies.
    - Build confidence for business, encourage continued investment. What is illegal offline should remain illegal online. We support requirements for formalities on notices, and measures that allow for careful and effective decision making on content removal.
    - The definition of 'online platform' should be targeted and proportionate to the proposed obligations. The proposed definition is overly broad and risks capturing service providers deep in the digital supply chain that may have no direct link with the online dissemination of goods, services, or content to the public nor legal access or control over client/user generated data/content. For example, cloud service providers. The legislation should clarify that such services are not considered online platforms under the DSA.
    - The criteria for defining very large online platforms (VLOPs) should be refined to introduce a more precise trigger for additional regulation, including financial means of services or societal risk profiles.
    - The trusted flagger system should be proportionate, workable and enhance co-operation between online platforms and trusted bodies, including rightsholders. Objective vetting criteria for the appointment of trusted flaggers will be needed to ensure the efficacy of this system. Flaggers must meet standards of objectivity

and be balanced across issue areas, so as not to give weight to one over others.
    - Transparency reporting should be targeted, proportionate and reflect differences between services.
    - Facilitate meaningful user redress, efficiently, without enabling bad actors and without undermining the freedom to conduct a business, and prevent out-of-court mechanisms from having unintended consequences.
    - Traceability of traders is important to maintaining trust online. Traceability should be proportionate and workable to encourage legitimate online trade.
    - Preserve and uphold the country-of-origin (COO) principle. As an internal market instrument, the objective of the DSA should be to ensure full harmonisation. Any derogations required by Member States, should be limited, targeted and proportionate to achieving clearly identified public interest objectives. Further guidance on the interpretation of the COO principle would be welcome and the supervision and enforcement framework must align.
    - The European Board for Digital Services (EBDS) should ensure consistent application of DSA principles.
    - Clarify the proposed governance processes to ensure that there is due process for companies.
    - Sanctions should be proportionate and based on systemic violations, where there has been a sustained failure to comply with specific DSA obligations, rather than one-off events.
    - Extend the DSA implementation timeline (Article 74) to 12-18 months to enable businesses and authorities to put the necessary resources in place to implement the regulation.

- **Recommendations on the Digital Markets Act (DMA):**
    - Provide an evidence based and predictable process for designating gatekeepers and their obligations, led by an expert EU body. We support open, fair, efficient, and contestable digital markets for the benefit of consumers and business.
    - Build confidence for business and continued investment. Substantial legal change should not be implemented via delegated acts but by ordinary legislative procedure.
    - Clearly define the relationships between the DMA and parallel national and EU competition and markets legislation, and between the European Commission and national authorities. Ensure a risk-based, evidence based and harmonised approach.
    - Carefully design remedies to target the sources of gatekeeper status and avoid overly broad interventions which have unintended consequences for the wider market.
    - Provide for a timely consultation with designated firms and relevant stakeholders including business users and competing firms. Enable proportionality and deepen mutual understanding of issues and the technical implications of certain obligations. The objective of the consultation and dialogue should be a more expedient, targeted,

and evidence-based implementation of obligations that limits unintended consequences.

- Clarify Article 5(b). It is unclear whether designated business users can offer their products and services at different prices and conditions on their own website, not just on other platforms.
- Support a proportionate and efficient investigations and enforcement framework. Clarify how the DMA committee will cooperate with the European Competition Network.
- Rules should have a clear connection to the DMA's metrics for success. The DMA claims that its rules will significantly increase GDP, employment, sales, and consumer surplus. Any rules that ultimately become part of the DMA should have a clear connection to achieving these goals.

1

Introduction

1. Introduction

European Commission legislative proposals on the regulation of digital markets and services, known as the 'digital services package', are acknowledged as significant developments in the evolution of a European digitalised single market (DSM). The stated aims of the Commission package are 'to create a safer digital space in which the fundamental rights of all users of digital services are protected; and to establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally'.

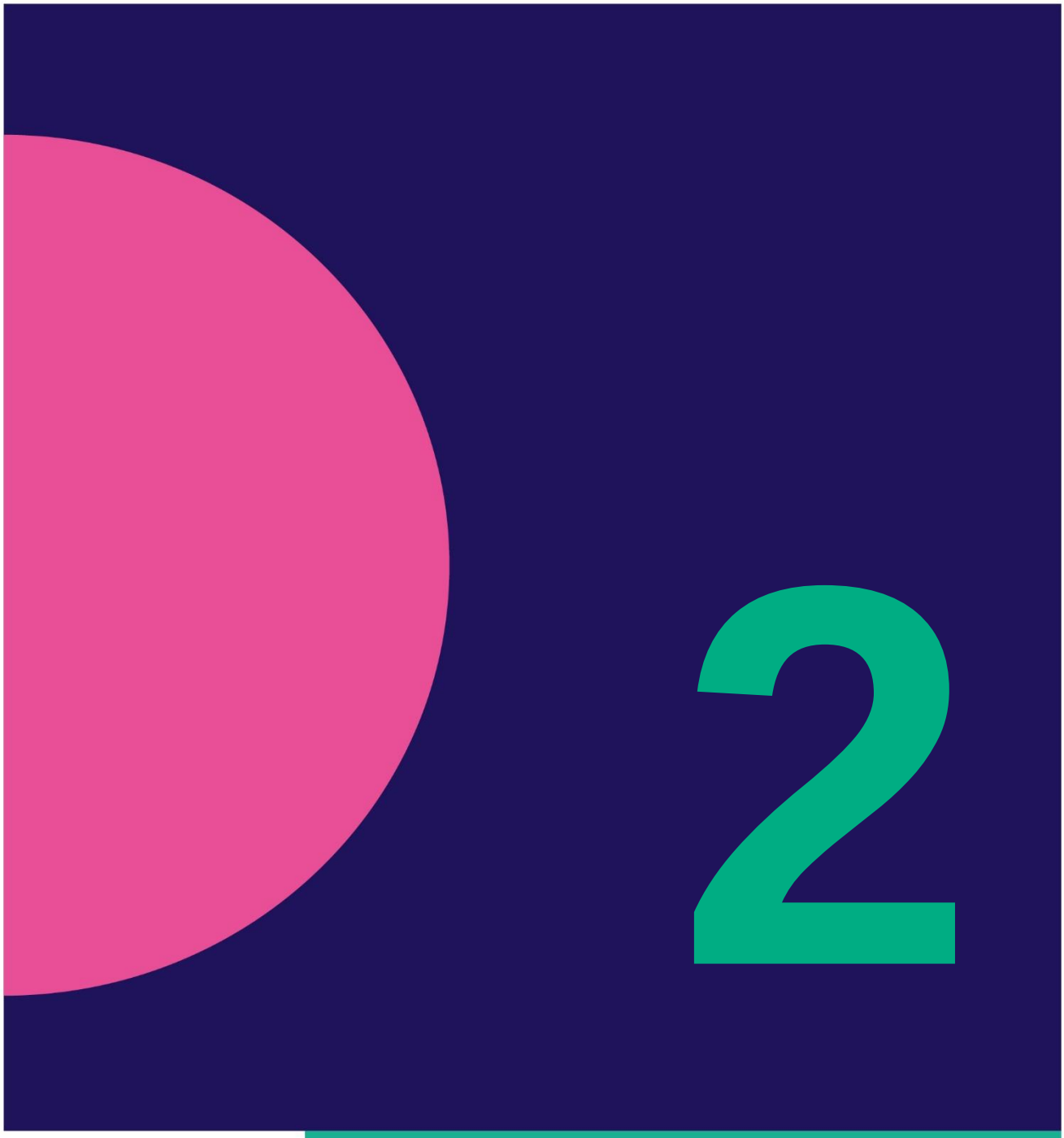
Ibec engaged in EU and national consultative processes in the development of the European Commission digital services package[1]. We support efforts to increase trust in further digital transformation and to protect businesses and people online. We support free and fair competition and efforts to ensure Member States, organisations, businesses, and citizens can reap the benefits of a DSM. To implement an open digital future, preserve, and support further digital innovation and protect businesses and individuals online, we encourage legislators to take a clear, robust risk-based and evidence-based approach to regulation, consistent with existing European and national law.

This paper presents Ibec recommendations to EU co-legislators on the further development of the European Commission's digital services package, including the proposed Digital Markets Act (DMA)[2]and Digital Services Act (DSA)[3].

[1] For example, https://www.ibec.ie/-/media/documents/influencing-for-business/digital-policy/open-digital-future-dsa-paper.pdf

[2] European Commission (2020) Proposal for a Regulation of the European Parliament and the of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15.12.2020 COM (2020) 842 final 2020/0374 (COD). https://ec.europa.eu/info/sites/info/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf

[3] European Commission (2020) Proposal for a Regulation of the European Parliament and the of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15.12.2020 COM(2020) 825 final 2020/0361 (COD). https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-parliament-and-council-single-market-digital-services-digital



EU Digital Services Act

2. Recommendations on EU Digital Services Act

- **Maintain legal certainty for business, encourage continued investment**. **Ibec welcome the Commission's proposal to preserve key principles of the eCommerce Directive (ECD), including country of origin; conditional liability limitations for online intermediaries; and no general monitoring obligations**. These ECD principles are important to firms of all sizes and have facilitated market certainty, innovation, and economic growth. It is right that they should be retained.
    - Liability should be determined by intermediary *activity*, not business model, to reflect the complexity and diversity of digital business, and the fact that a single digital business can involve multiple intermediary activities.
    - Liability should be based on actual knowledge and failure to act. Liability should not result from illegal content of which a platform is not aware.
    - Article 6 should be expanded to ensure intermediaries who carry out own investigations, for legal compliance; or for content that may violate their terms of service, are not barred from the limited liability regime. Encourage further progressive action by intermediaries.

- **Harmful (but legal) content should not be subject to removal or monitoring obligations.** It is difficult to define, culturally sensitive and contextual. The removal of such content must be balanced against the protection of fundamental rights. Online platforms should also be enabled to moderate such content according to their policies.
    - Article 35 should clarify that codes of conduct will focus on illegal content and systemic risks in line with criteria in Article 26(1) only and not permit the use of Chapter IV powers. Article 26 should further clarify that guidelines from regulators shall not include measures related to takedown of harmful but legal content.

- **Build confidence for business, encourage continued investment**. It is important to formalise a workable system of notice and takedown, clarifying definitions of illegal content and proportionate actions expected of digital services, respecting both fundamental rights and differences between digital services. We caution against overly prescriptive provisions or provisions that would incentivise companies to remove content without careful decision-making.
    - **What is illegal offline should remain illegal online.**
    - **We support requirements for formalities on notices, and measures that allow for careful and effective decision making on content removal**.
        - There should be a hierarchy of responsibility enshrined in the DSA which directs the obligation to act towards the intermediary with the most direct control over the content or behaviour in question. This would remove the overlapping obligations inherent in the proposals and avoid destabilising complex digital supply chains.

- The quality of the notice and whether the content it identifies is illegal or not should be considered and clarified in Article 14(3). As currently drafted, Article 14(3) suggests that any notice meeting criteria in 14(2) would constitute 'actual knowledge' and trigger a requirement to act regardless of third-party rights. This scenario raises concerns around potential misuse of the notice and action process and the creating conflicts with third party rights.
- The inclusion of "reference" to an illegal activity in Art 2(g) could lead to excessive takedowns of content that demonstrates or references an illegal activity, for example a film of a car speeding.
- Claimants should have recourse to accessible and affordable legal process where claims require knowledge of third-party rights which intermediaries would not or could not know. Article 6 should be clarified to safeguard intermediaries from claims arising from good faith actions where such knowledge is absent.

- **The definition of 'online platform' should be targeted and proportionate to the proposed obligations**. The proposed definition is overly broad and risks capturing service providers deep in the digital supply chain that may have no direct link with the online dissemination of goods, services, or content to the public nor legal access or control over client/user generated data/content. For example, cloud service providers. The legislation should clarify that such services are not considered online platforms under the DSA. The potential inclusion of such services within the definition of online platforms would introduce legal confusion to complex supply chains and create tension with the DSA's goals. The definition and coverage of "online platforms" (Art 2(h)) within the scope should be modified accordingly and limited to those that only disseminate public information. As noted above, there should be a cascading hierarchy of responsibility for intermediaries to avoid overlapping and conflicting obligations, and responsibility for harms and illegal content being pushed deep into complex digital supply chains and ensure action is always taken closest to the content sources.

- **The criteria for defining very large online platforms (VLOPs) should be refined to introduce a more precise trigger for additional regulation**. The proposed quantitative criteria could extend obligations very broadly without a clear purpose or goal for the additional regulation. The purpose should be clearly defined and informed by an evidence-led process. Qualitative factors, such as financial means or societal risk profile of the service, should be considered to differentiate which obligation, supervision and enforcement rules should apply to which platforms. Qualitative factors could also be considered in determining which platforms should take additional measures to prevent the dissemination of illegal content, for example the underlying technological capabilities and functionalities of a given service.

- **The definition of marketplaces, or "online platforms that allow consumers to conclude distance contracts with traders" (Articles 5(3) and 22):** It should be clarified that these provisions are aimed at capturing online marketplaces and, therefore, apply to online platforms that allow the consumer to conclude a distance contract with the trader on the online platform (and not on the third-party trader's site).

- **The trusted flagger system[4] should be proportionate, workable and enhance co-operation between online platforms and trusted bodies, including rightsholders**. Trusted flaggers can play an important role in highlighting illegal content and goods that can help intermediaries, rightsholders and authorities. Any final decision necessary on whether flagged goods or content are illegal should rest with the authorities. Further clarity would be welcome on:
    - The definition of an 'organisation of industry'.
    - How Digital Services Co-ordinators (DSCs) assess trusted flaggers.

- **Transparency reporting[5] should be targeted and proportionate and reflect differences between services**. Many service providers participate in voluntary codes of conduct promoting online safety. Accountability is important to maintaining trust online. However, this should be proportionate in achieving consumer transparency and not expose business sensitive information. The requirement to make all statements of reasons for every removal available to the public (under Article 15(4)) raises questions of scalability and proportionality and lacks clear value for users and regulators, and could risk user privacy, lead to abuse by bad actors, and interfere with law enforcement investigations. Safeguards should be added to ensure transparency and data access obligations are reasonable, flexible, and proportionate.

- **We support proportionality and fairness in arbitration processes. Facilitate meaningful user redress, avoid misuse, revise Article 18**. It is important that users have the ability to appeal content decisions. Platforms already offer such mechanisms. However, we are concerned that DSA provisions on out-of-court mechanisms (Article 18) may have potential unintended consequences such as:
    - Enabling bad actors: Article 18 opens up avenues for abuse and does not scale to the millions of decisions online platforms make. Bad actors could use alternative dispute resolution (ADR) to arbitrate every content removal at a company's expense. They could slow down the process for legitimate seekers of redress.
    - National authorities' removal orders: Under the current DSA text, content uploaders may arguably also challenge services' removals made pursuant to national authorities' removal orders (under Article 8), including where those orders may be confidential and appear as the online platforms' own decision.
    - Fragmentation and confusion: 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 issues or policies. Given the scale of content moderation online platforms engage in, trying to make sense of a patchwork of often contrasting decisions by different bodies across the EU risks paralysing online platforms' content moderation systems.

  Article 18 needs revision to ensure it is not abused. For example, the DSA should require that users first exhaust the appeals mechanism that online platforms are required to set up via Article 17 (internal complaint-handling mechanisms) and institute penalties for bad actors that abuse out-of-court

[4] Article 19
[5] Articles 13, 23, 33. Recitals 39, 51, 65

redress. It should also make clear that intermediaries are immunized from liability for actions taken to implement decisions made in out-of-court redress.

- **Traceability of traders is important to maintaining trust online (Article 22)**. **Traceability should be proportionate and workable to encourage legitimate online trade.** Legally mandated know your business customer (KYBC) is welcome and could assist traceability of counterfeit or dangerous products. Information provided by traders to online platforms should be proportionate and workable so as not to discourage legitimate online traders. Information, which is not related to a trader's traceability, and may not be known at the time of account creation, should not be required. Registration should be coherent with other legal obligations to prevent duplication. We would also welcome clarification that the information under Article 22(1)(d) only applies to those products subject to the Market Surveillance Regulation. We understand that not all Member States have national identification documents as referred to in Art 22(1)(b) and verifiability of information provided is not always possible. Further to this, third countries may have diverse systems too. A passport should be listed in Art 22 as a possibility. It should be clarified that the trader should provide the information required under Article 22 to the online platform, given it would be impossible for the online platform to chase information about economic operators down the value chain. Online platforms should not be liable for false information provided by traders and it should be clarified that the "reasonable efforts" obligation (Article 22(2) is limited to official public and freely available databases. Online platforms should not be required to engage in follow-up requests with each trader.

- **The DSA should preserve and uphold the country-of-origin (COO) principle**. This is important to the functioning of the internal market.
    - **As an internal market instrument, the objective of the DSA should be to ensure full harmonisation**. Illegal content can be further defined at Member State level.
        - **Any derogations required by Member States, should be limited, targeted and proportionate to achieving clearly identified public interest objectives**. While acknowledging national cultural differences, it is important to ensure that the laws of one Member State do not overly impact what users in other Member States can view online.
        - **Further guidance on the interpretation of the COO principle would be welcome**.
    - **The European Board for Digital Services (EBDS) should ensure consistent application of DSA principles** with the inclusion of COO to activity reporting DSCs in Article 44. The option for Digital Service Co-ordinators to refer cases to the EBDS must not be the exception that becomes the rule.

- **Clarify the proposed governance processes**. The Digital Services Co-ordinators (DSCs) could simplify co-operation with legal enforcement authorities. The EBDS could assist the DSCs and ensure consistent application of regulation and legal certainty. However, further clarity would be welcome on Articles, 45, 46 and 49, including:

- Cross-border co-operation processes among DSCs to support the COO.
- Processes for joint investigations.
- Due process for companies, including sufficient time to respond to various authorities.
- Thresholds that trigger investigations and enforcement.

- **Sanctions should be proportionate and based on systemic violations,** where there has been a sustained failure to comply with specific DSA obligations, rather than one-off events**.**

- **Extend the DSA implementation timeline (Article 74)** to 12-18 months to enable businesses and authorities to put the necessary resources in place to implement the regulation.

3

EU Digital Markets Act

3. Recommendations on EU Digital Markets Act

- **The DMA's scope should be refined to ensure consistency and reflect the focus on gatekeepers.** The DMA risks being over-inclusive in some respects and under-inclusive in others and leaves open the possibility for overlapping and conflicting EU and national rules. In particular:
    - Article 1(6) should be amended to preclude national rules from regulating substantially the same practices as the DMA.
    - Article 2(2)(g) should be removed to avoid covering a broad range of non-gatekeeper services that fall within the definition of 'cloud'.
    - Article 3(2)(a) should be removed or replaced with a service-level turnover threshold to avoid unequal treatment between platforms of the same size and importance simply because of the revenues of their owners.

- **Provide clear and predictable criteria for designating gatekeepers and their obligations**. We support fair, efficient, and contestable markets for the benefit of consumers and business.
    - We acknowledge the proposed use of qualitative criteria and quantitative thresholds to define gatekeepers. However, the designation process should be refined. The definition of thresholds should aim to avoid the inclusion of smaller digital services and those that could not act as gatekeepers.
    - Clarify Article 3(1)(b). Services only providing a technical service but not acting as a digital intermediary should not be designated as a gatekeeper. The focus should be on core services acting as a true gateway for market access where business meet end users. Gatekeepers are understood to be the 'go-to-market' channel which serves as an important gateway for business customers to reach end users. Companies which do not function as such, even if they provide certain "core platform services" as defined in the DMA, should not be obligated because the definition currently included for the concept of gatekeeper is too broad and not specific enough. For example, not all cloud services are go to market channels. A clarification of the definition of "business users" is also needed, as it currently captures business users using core platform services of a gatekeeper to support the internal workings of a business user. This could for example be HR management services, procurement management services, archive services or cybersecurity and disaster recovery services which rely on "*cloud computing services*" (defined as core platform services) and which could be characterized as being used by business users "*in the course of offering goods or services*" to end users. These kinds of internal operations, however, do not function to offer or market products or services to their users. Therefore, it should be clarified that business users are entities using the platform services offered by the gatekeeper to reach their own users.
    - Article 3(2) should be refined as it renders the more relevant designation criteria set out in Article 3(1) irrelevant. This would

avoid sweeping in companies that may be large but without market power and subjecting them to a highly burdensome process of proving the fact to an unwritten and potentially arbitrary standard.
    - A new step should replace the designation process in Article 3(3) and (4) involving a detailed economic analysis led by an expert EU competition body, and subject to consultation with relevant parties.
    - Provide guidance on the application of Article 3(6) that allows the European Commission to designate gatekeeper status even when a business does not fulfil the quantitative thresholds of Article 3(2).

- **Support legal certainty for business and continued investment**.
    - Substantial legal change should not be implemented via delegated acts but by ordinary legislative procedure based on evidence-led proposals aligned with the EU's economic goals.
    - Article 1(6) could be strengthened to prevent Member States passing measures that relate to DMA to avoid a fragmented regulatory framework for gatekeepers.
    - The definition of 'business user' is broad. Notwithstanding the term "user" it could be interpreted to include resellers, prime contractors (using the gatekeeper as their subcontractor), managed service providers and business users using the core platform service to support their internal functions. It should be narrowed to focus on users who use a potential gateway to promote or offer services or goods.

- **Clearly define the relationships between the DMA and parallel national and EU legislation, and between the European Commission and national authorities**. Ensure a risk-based, evidence based and harmonised approach.

- **Provide for a targeted remedies and consultation**. The goals of Articles 5 and 6 are important. However, many of the obligations in Articles 5 and 6 relate to specific anti-trust cases and business models. This means they need further specification if they are to be applied to all gatekeepers designated in the DMA.
    - Given the dynamism and diversity of platforms the proposed remedies are insufficiently flexible and targeted. Remedies should be tailored to address specific competition barriers and precisely targeted to identify and avoid unintended consequences.
    - A designation process based on detailed economic analysis will deepen the competition authority's understanding of the market and better inform the design of remedies.
    - The choice and design of remedies should be informed by detailed concurrent consultation with the designated firm and other interested parties, including business users and competing firms.
    - Regulatory dialogue should be strengthened in the proposal. A timebound regulatory dialogue (e.g., 6 months) can enable proportionality and help deepen mutual understanding of issues and the technical implications of certain obligations. This in turn will help to ensure DMA's legal certainty. Specifying obligations in a

regulatory dialogue reduces the risk of DMA being legally challenged in court e.g., by businesses who will deem compliance measures applied by in-scope companies insufficient. The objective of the dialogue should be a more expedient, targeted, and evidence-based implementation of obligations that limits unintended consequences and ensures legal clarity in the years to come.

- Periodic suspension or full exemptions from a specific obligation could be agreed by the regulator based on specific and clear overriding public interest reasons (Article 9). In addition, pro-competitive focused legal defences could be introduced in the DMA. This would allow for in-scope companies to be able to justify their conduct based on the efficiency, innovation, or other benefits it brings. The Commission could consult with relevant stakeholders and give consideration to the impact on the contestability of digital markets. Such legal defences are available in a recently passed German competitional law reform act and the new competition regime proposed by the UK's Competition Markets Authority.

- **Compliance should not compromise security and integrity of services offered by in-scope companies**
  - A number of provisions contain safeguards that inform the scope of the specific obligation. For instance, Art. 6.1.b allows a gatekeeper to restrict an app uninstallation which is essential to the functioning of the OS or device. Art. 6.1.c provides for the right of the gatekeeper to take proportionate measures to protect the integrity of the service or device.
  - In our view risks to the integrity, security or functionality of a service may arise in the implementation of many -if not all- art. 5 and 6 obligations. Therefore, these considerations (i.e., integrity, security, functioning) should be considered as an overarching principle and not be limited to a few provisions.

- **Clarify Article 5(b).** It is unclear whether designated business users can offer their products and services at different prices and conditions on their own website, not just on other platforms.

- **Support a proportionate and efficient investigations and enforcement framework:**
  - The regulator should have substantiated reasons to investigate before using the powers in Chapter V. The deadline for 14 days on the right to be heard Article 30 should be extendable at the discretion of the regulator based on the complexity of the obligations. Chapter V should clarify third-party responsibilities during investigative procedures.
  - An Article 7(2) decision should be a necessary step before any enforcement under Article 25. This is to ensure gatekeeper companies are not disproportionately punished for good faith

compliance efforts and get a chance to course correct their compliance efforts before any enforcement action.

- Clarify how the DMA committee will cooperate with the European Competition Network.
- Given the impact of the obligations, the right to judicial review should be earlier in the process for example once a market investigation has been conducted. The scope of judicial review (Article 35) is too narrow. It provides for views for decisions involving fines.

About Ibec

Ibec is Ireland's largest lobby group and business representative. We campaign for real changes to the policies that matter most to business. Policy is shaped by our diverse membership, who are home grown, multinational, big and small and employ 70% of the private sector workforce in Ireland. With 38 trade associations covering a range of industry sectors, 6 offices around Ireland as well as an office in Brussels. With over 240 employees, Ibec communicates the Irish business voice to key stakeholders at home and abroad. Ibec also provides a wide range of professional services and management training to members on all aspects of human resource management, occupational health and safety, employee relations and employment law.

www.ibec.ie/digitalpolicy
@ibec_irl
Connect with us on LinkedIn