Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

JEAN MONNET CHAIR IN DIGITAL TRANSFORMATION AND AI POLICY

# DIGITAL ECONOMY AND DATA STRATEGY

**Course Market Law and Regulation a.y. 2022-2023**

**Course convenor: Professor Valeria Falce (Valeria.Falce@unier.it)**

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

# Module 2.

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

# COMPETITION VS. REGULATION IN DIGITAL MARKETS

# THE DIGITAL SERVICES ACT PACKAGE: THE CASE OF THE DIGITAL MARKETS ACT («DMA»)

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

- Does competition law prove to be effective when it comes to digital markets?

- The answer relies on the analysis of the Digital Service Act Package…

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

- **The Digital Services Act package** was presented by the European Commission in December 2020. It includes:

- the **Digital Services Act**
- the **Digital Markets Act**

Both legislative acts were quickly adopted by the Council and the European Parliament in 2022.

The new rules better govern the digital space and digital services, including social media platforms. They:

- ensure digital users have access to safe products and protect users' fundamental rights
- allow free and fair competition in the digital sectors to boost innovation and growth

Co-funded by the Erasmus+ Programme of the European Union

- In addition, a **European Data Governance Act**, which is fully in line with EU values and principles, has been proposed in the context of the European strategy for data.

- The Data Governance Act seeks to increase trust in data sharing, strengthen mechanisms to increase data availability and overcome technical obstacles to the reuse of data.

- The Data Governance Act will also support the set-up and development of common European data spaces in strategic domains, involving both private and public players, in sectors such as health, environment, energy, agriculture, mobility, finance, manufacturing, public administration and skills.

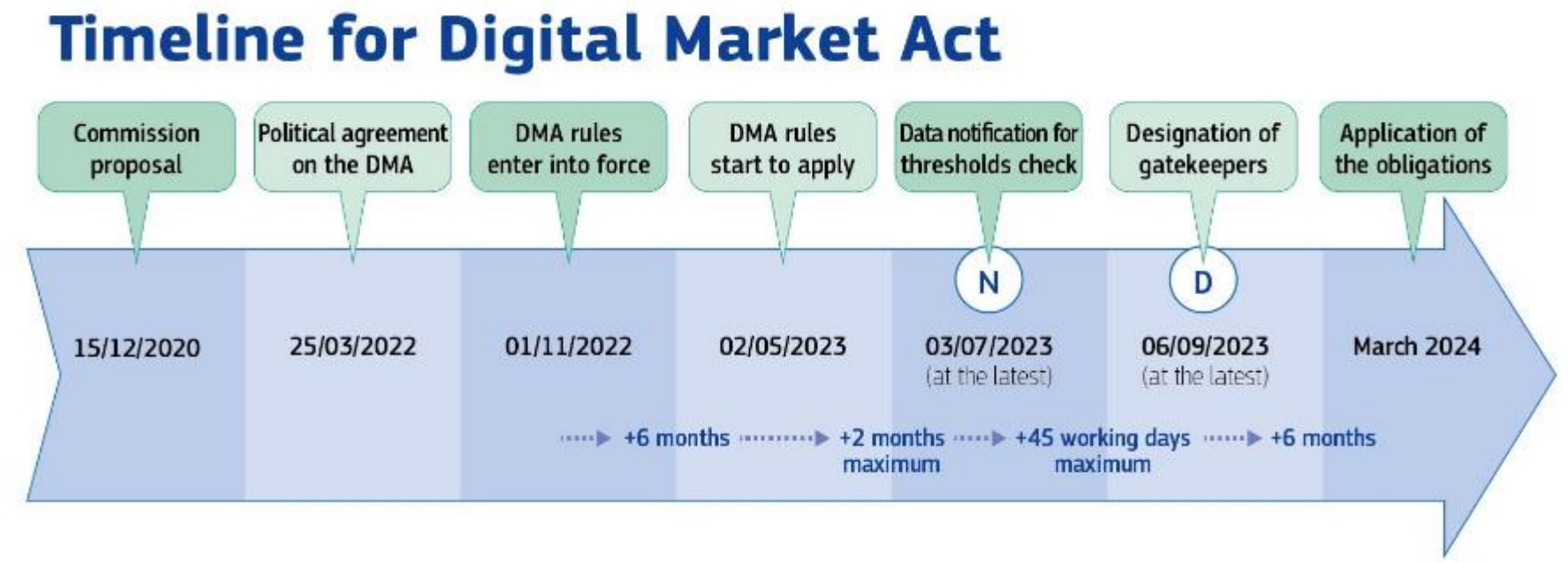
- The Data Governance entered into force on 23 June 2022 and, following a 15-month grace period, will be applicable from September 2023.

# Competition vs. Regulation
# The Digital Services Act Package: the case of the DMA

- In September 2022, the European Parliament and the Council adopted the Regulation on contestable and fair markets in the digital sector, better known as the Digital Markets Act ("DMA").
    - Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector [2022] OJ L265/1 (hereafter: DMA).
- The legislative process was speedy and, unusually, the final text is stricter than the one proposed by the European Commission (EC) in December 2020.
    - EC, Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector COM(2020)842 final
- With the legislative process in the rearview mirror, it is time to start looking forward to its implementation.
    - See Commission Implementing Regulation (EU) . . ./. . . of XXX on detailed arrangements for the conduct of certain proceedings by the Commission pursuant to Regulation (EU) 2022/1925 of the European Parliament and of the Council
    - On 14 April, the European Commission adopted implementing regulations detailing how the Digital Markets Act will function in practice.

# Competition vs. Regulation
# The Digital Services Act Package: the case of the DMA

As of 12 October 2022, the DMA was published in the Official Journal and entered into force on 1 November 2022. Before 3 July 2023, companies have to provide the Commission with information about their number of users so that the Commission can designate "gatekeepers" before 6 September. Gatekeepers will then have until March 2024 to ensure that they follow the obligations of the DMA.



# Competition vs. Regulation
# The Digital Services Act Package: the case of the DMA

| | | |
|---|---|---|
| Official Journal | **12 October 2022 (OJ L 265/1)** | |
| Entry into force | **1 November 2022** (20th day following publication in Official Journal) | |
| Application of DMA provisions | **1 November 2022** (date of entry into force) | ➢ European Commission (EC) must establish a High-level group to provide with advice and expertise on implementing the DMA (Article 40).<br>➢ EC may adopt implementing acts, inter alia, to lay out details of notification forms and practical arrangements for cooperation and coordination between itself and the national authorities (Article 46).<br>➢ EC may adopt guidelines to facilitate DMA's effective implementation and enforcement (Article 47).<br>➢ EC may mandate European standardisation bodies to develop appropriate standards (Article 48).<br>➢ EC may adopt delegated acts to supplement the DMA, inter alia, by specifying the methodology for setting details of the quantitative thresholds to identify gatekeepers (Article 3(6)).<br>➢ Digital Markets Advisory Committee assisting EC in implementing the DMA starts work (Article 50) |
| | **2 May 2023** (6 months after entry into force) | ➢ Most provisions apply.<br>➢ Article 5 obligations and prohibitions (to apply directly to gatekeepers following designation):<br>o processing and use of end users' personal data<br>o parity clauses<br>o anti-steering<br>o business or end users may raise issues of non-compliance<br>o tying<br>o bundling<br>o transparency concerning online advertising practices.<br>➢ Articles 6 and 7 obligations and prohibitions (to apply to gatekeepers subject to further specifications under Article 8(2)):<br>o data silo<br>o uninstalling apps and changing default settings<br>o sideloading<br>o self-preferencing<br>o switching apps<br>o interoperability<br>o transparency concerning online advertisement performance<br>o data portability<br>o data access |

# Competition vs. Regulation
# The Digital Services Act Package: the case of the DMA

| | | |
|---|---|---|
| | | ○ search data access<br>○ access to app stores, search engines and social networking services<br>○ rules on terminating provision of service<br>○ interpersonal communications services' interoperability<br>○ basic functionalities' interoperability.<br>➢ Articles 13, 14 and 15 obligations:<br>○ anti-circumvention<br>○ information on concentrations<br>○ audit describing customer profiling techniques. |
| | **25 June 2023** | ➢ Provisions concerning representative actions apply (Article 42).<br>➢ Provisions concerning whistleblowers apply (Article 43). |
| Gatekeeper designation procedure | **2 May 2023** | ➢ Gatekeeper designation procedure starts. |
| | **By 2 July 2023** (within 2 months of entry into application) | ➢ Providers of core platform services (CPS) must self-assess whether they qualify as gatekeepers.<br>➢ Providers of CPS that meet the quantitative thresholds must submit a notification to the EC (Article 3(3)). |
| | **From summer 2023** | ➢ EC shall designate a gatekeeper within 45 days of receiving complete information (Article 3(4)).<br>➢ EC may conduct market investigations to assess the evidence submitted by a CPS provider to rebut presumption of gatekeeper designation (Articles 3(5) and 17(3)).<br>➢ EC may conduct market investigations to designate as gatekeeper a CPS provider that does not meet the quantitative thresholds but satisfies the qualitative criteria (Articles 3(8) and 17(1)). |
| Compliance with obligations and prohibitions | **From 2024** (within 6 months of gatekeeper designation) | ➢ Gatekeeper shall comply with obligations and prohibitions laid down in Articles 5, 6 and 7 (Article 3(10)).<br>➢ Gatekeeper shall provide EC with a report describing the measures implemented to ensure compliance (Article 11).<br>➢ Gatekeeper shall submit audit to EC describing customer profiling techniques (Article 15). |
| Updating obligations for gatekeepers | **From 2025** | ➢ After conducting a market investigation (18 months) on its own initiative or at the request of at least three Member States, EC must submit a report and may:<br>○ present a legislative proposal to add new CPS or new obligations in the DMA,<br>○ propose a delegated act to add to existing obligations (Articles 12 and 19).<br>➢ Council and Parliament experts must be consulted on any delegated act, in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making. |
| Review clause | **3 May 2026** | ➢ EC must evaluate the regulation and report to the Parliament, the Council and the European Economic and Social Committee on any amendments needed (Article 53). Evaluation must assess specifically the need to extend the Article 7 interoperability obligation to online social networking services, or to amend the provisions concerning the list of CPS, the obligations and their enforcement. |

# Competition vs. Regulation
# The Digital Services Act Package: the case of the DMA

1. **The idea underlying these initiatives is that competition law is too narrow, either by design or through judicial interpretation (in particular in the United States), which has led to under-enforcement, especially in the digital economy. Accordingly, the new laws are supposed to recalibrate enforcement.**

- The DMA is explicitly grounded on the assumption that competition law alone is unfit to effectively address challenges and systemic problems posed by the platform economy.
- Indeed, the scope of antitrust rules is limited to certain instances of market power (e.g., dominance on specific markets) and of anti-competitive behaviour.
- Furthermore, its enforcement occurs ex post and requires an extensive investigation of often very complex facts on a case-by-case basis. Moreover, it does not address, or does not address effectively, the challenges to the well-functioning of the market posed by the conduct of gatekeepers, which are not necessarily dominant in competition law terms.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DMA

1. **The idea underlying these initiatives is that competition law is too narrow, either by design or through judicial interpretation (in particular in the United States), which has led to under-enforcement, especially in the digital economy. Accordingly, the new laws are supposed to recalibrate enforcement.**

- As a result, a regulatory intervention is invoked to complement traditional antitrust rules by introducing a set of ex ante obligations for online platforms designated as gatekeepers, and dispensing enforcers from defining relevant markets, proving dominance, and measuring market effects.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DMA

**2. The declared aim of the DMA is to protect a different legal interest from those of antitrust rules, notably it pursues an objective that is different from that of protecting undistorted competition on any given market, as defined in competition law terms, which is to ensure that markets where gatekeepers are present are, and remain, contestable and fair, independently from the actual, likely or presumed effects of the conduct of a given gatekeeper (DMA, Recital 11).**

- Accordingly, the relevant legal basis is represented by Article 114 TFEU, rather than Article 103 TFEU, which is intended for the implementation of antitrust provisions pursuant to Articles 101 and 102 TFEU.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DMA

**3. The DMA's stated objective is "to ensure that markets where gatekeepers are present are and remain contestable and fair." (DMA, Recital 11)**

- Those goals of contestability and fairness are not explicitly defined.
- The clearest articulation of contestability is that it relates to "the ability of undertakings to effectively overcome barriers to entry and expansion and challenge the gatekeeper on the merits of their products and services." (DMA, Recital 32)
- The idea is that the features of platform markets (network effects, strong economies of scale, benefits from data) currently limit the contestability of gatekeeper positions and that the DMA should lower the barriers to entry, in particular to the benefit of new challengers.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DMA

**3. The DMA's stated objective is "to ensure that markets where gatekeepers are present are and remain contestable and fair." (DMA, Recital 11)**

- Those goals of contestability and fairness are not explicitly defined.
- Fairness, by contrast, relates to "an imbalance between the rights and obligations of business users where the gatekeeper obtains a disproportionate advantage." (DMA, Recital 33)
- The idea is that gatekeepers use their superior bargaining position to appropriate the efforts of business users, either directly (by exploiting them) or indirectly (by excluding them from the market, especially when they compete with services provided by the gatekeeper).

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DMA

**4. In other words, the DMA is aimed at making room for innovation by smaller players and letting such players reap the benefits from their innovative (and other) efforts.**

- In short, the DMA tries to distinguish itself from EU competition law but only succeeds in doing so to a limited extent. Fairness goes back to intra-platform exclusion and exploitation, while contestability refers to inter-platform competition (although promoting and not simply protecting such competition goes beyond competition law).
- At the same time, the DMA's reason for adoption (as a response to competition law's perceived ineffectiveness) and more prescriptive nature are reminiscent of sectoral regulation. It is thus not necessary to fit the DMA into a competition law straitjacket, but it is justified to use competition law as a reference point. Substantive or procedural departures from competition law may very well be justified when the law is not attaining its goal of undistorted competition (and its corollary, consumer welfare).

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DMA

In addition to sketching this global push for platform regulation, it is important to situate the DMA within the wider EU effort to regulate various aspects of digital markets, focusing on the instruments that it interacts with.

First, the DMA is part of a package that also includes the **Digital Services Act (DSA)**, which focuses on the accountability of online platforms regarding illegal and harmful content.

Second, the DMA goes a step further than the **Platform-to-Business (P2B) Regulation** of 2019, which focused on introducing transparency in the relation between platforms and their business users.

Third, the DMA shares a concern for data protection with **the General Data Protection Regulation (GDPR)**, and even strengthens it on certain fronts.

Fourth, the DMA's contestability goal is reminiscent of the pluralism pursued by the **Audiovisual Media Services Directive**.

Finally, though not adopted with the digital economy in mind, the **Unfair Commercial Practices Directive** has a similar focus on fairness and also includes a "blacklist" of banned practices.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DMA

- **The Gatekeeper concept**
- The DMA's scope is determined by the concept of "gatekeeper".
- "Gatekeeper" is defined as an undertaking providing core platform services (CPS) that is designated as gatekeeper according to certain criteria (DMA, art. 2(1)).
- It makes sense to look at the two components – CPS and gatekeeper status – separately.
- CPS are defined by reference to a close list of types of online platforms (DMA, art. 2(2)).

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DMA

- **The Gatekeeper concept**
- They include the usual suspects, including intermediation services (e.g., marketplaces and app stores), search engines, social networks, OS, and advertising (intermediation) services, as well as some less obvious choices (i.e., video-sharing services, number-independent interpersonal communication services (NIICS), web browsers, virtual assistants and cloud computing services).
- The DMA defines each of these CPS separately, often in reference to other EU regulation. The idea is that CPS constitute gateways in the digital economy, with the capacity to affect a large number of end-users and businesses, which is not a problem in itself. Sufficiently serious concerns around fairness and contestability only arise when a CPS becomes an unavoidable gateway – in other words, a gatekeeper.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DMA

- **The Gatekeeper concept**
- Gatekeeper status is dependent on three qualitative criteria. For each criterion, there are quantitative thresholds; when those are met, the qualitative criterion is presumed to be fulfilled.
- According to those qualitative criteria and corresponding quantitative thresholds, an undertaking qualifies as gatekeeper if

(a) it has a significant impact on the internal market: this is the case where it achieved an annual EU turnover above €7.5B in each of the last three financial years, or where its average market cap amounted to at least €75B in the last financial year, and it provides the same CPS in at least three Member States;

(b) the CPS it provides is an important gateway for business users to reach end-users: this is the case where in the last financial year, the CPS had at least 45M monthly active end-users established or located in the EU and at least 10,000 yearly active business users established in the EU;

(c) it enjoys an entrenched and durable position: this is the case where the thresholds of (b) were met in each of the last three financial years.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DMA

- **The Gatekeeper concept**

| Potential Gatekeeper | Core Platform Services | | | |
|---|---|---|---|---|
| | Intermediation | Search | Social | Video-sharing |
| Google (Alphabet) | Play Store | Google Search | — | YouTube |
| Apple | App Store | — | — | — |
| Microsoft | Microsoft Store | — | LinkedIn | — |
| Amazon | Amazon Marketplace | — | — | — |
| Facebook (Meta) | Facebook Marketplace | — | Facebook Blue, Instagram | Facebook Watch, IGTV/ Reels |
| | NIICS[120] | OS | Browser | Advertising[121] |
| Google (Alphabet) | Gmail, Messages, Google Meet | Android (Auto) | Chrome | Related to CPS (search), intermediation |
| Apple | Mail/iCloud, iMessage | iOS (CarPlay), macOS | Safari | Related to CPS (intermediation) |
| Microsoft | Outlook, Teams | Windows | Edge | Related to CPS (social) |
| Amazon | — | — | — | Related to CPS (intermediation) |
| Facebook (Meta) | Messenger, WhatsApp, Instagram | — | — | Related to CPS (social), intermediation |

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DMA

- **The DMA Obligations**

- The DMA contains a list of 22 prohibitions and obligations included in three separate groups:
  - Article 5 enumerates 9 items, mostly prohibitions, which are supposed to be self-explanatory and self-executing;
  - Article 6 lists 12 items, mostly obligations, which may require additional specificity by the Commission; and
  - Finally, Article 7 adds a horizontal interoperability obligation among communications applications, which requires a phased implementation given its complexity.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DMA

- **The DMA Obligations**
- Even if the DMA itself does not cluster these prohibitions and obligations, it can be useful to group them around four categories. This clustering of obligations allows the link between the objectives of the DMA and its substantive part, as well as the relationship between the individual obligations, to be made more explicit.

    1. **Preventing anti-competitive leverage from one service to another**. This category includes the prohibition of tying one regulated core platform service (CPS) to another regulated CPS, or tying one CPS to identity or payment services, as well as the prohibition of specific discriminatory or self-preferencing practices.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DMA

- **The DMA Obligations**

2. **Facilitating business and end users switching and multi-homing**, thereby reducing entry barriers arising from user demand. This category includes the prohibition of Most Favoured Nation clauses, anti-steering and anti- disintermediating clauses, as well as disproportionate conditions to terminate services. It also includes the obligation to ensure that it is easy to install applications or change defaults, as well as to port data outside of core platform services.

3. **Opening platforms and data**, thereby reducing supply-side entry barriers and facilitating the entry of complementors, competitors and disruptors. This category includes horizontal and vertical interoperability obligations, FRAND access to app stores, search engines and social networks, and data access for business users as well as data sharing among search engines on FRAND terms.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DMA

- **The DMA Obligations**

4. **Increasing transparency** in the opaque and concentrated online advertisement value chain. This more specific category includes transparency obligations on price and performance indicators, which are to the benefit of advertisers and publishers.

The first category includes mostly prohibitions that are inspired by competition cases and are hence drafted in a relatively detailed manner. The second and – especially – the third categories include mostly obligations couched in more general terms and sometimes going beyond what could be imposed by way of competition law remedies. Each of these categories points to different aspects of contestability and fairness, as defined above. When the obligations are read together with the corresponding recitals, it becomes apparent that almost all of them relate to contestability, and many of them to fairness as well. The justifications set out in the recitals often blend contestability and fairness, underlining that they are indeed linked and that contestability seems to be the leading objective.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DMA

- **The DMA Obligations**

It is also possible to divide most of the DMA's obligations in just two groups: negative and positive. Although there are too many exceptions to speak of a "rule," negative obligations tend to correspond to the DMA's fairness goal, that is, to protect intra-platform competition, while positive obligations are more likely to relate to contestability, that is, to promote inter-platform competition. Let us examine the two groups.

**Negative obligations or "don'ts"** - proscriptive rules - are the prohibitions typical to competition law. Enforcement of such obligations results in injunctions or cease-and-desist orders ("reactive" remedies). In the DMA's text, negative obligations can be recognized from their wording, with "shall not" or "shall refrain" being giveaways (although language is bendable and thus not always helpful to unearth the nature of the obligation). An example of a negative obligation is the prohibition of antisteering measures, which prevent business users from communicating and promoting offers to end-users acquired via the CPS. These negative obligations tend to relate to the DMA's fairness goal, that is, seek to prevent gatekeepers from excluding or exploiting (business) users of its CPS.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DMA

- **The DMA Obligations**

**Positive obligations or "dos"** - prescriptive rules - are less usual for competition law. When it comes to remedies, a simple injunction does not suffice; rather, positive obligations require the enforcer to specify a desired course of action in greater detail ("proactive" remedies). Such remedies are not unheard of in competition law but are usually avoided given that they come with a greater need for design expertise and consistent monitoring. It is therefore only logical that most of the DMA's positive obligations are those that are "susceptible of being further specified" (Article 6). The text hints at the nature of such obligations with phrases like "shall allow (and technically enable)" and "shall provide." A good example is the obligation of gatekeeper search engines to provide third parties with access to ranking, query, click, and view data on FRAND terms. Positive obligations tend to relate to the DMA's contestability goal, that is, the promotion of inter-platform competition.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DMA

- **The DMA Obligations**

| Article | Obligation[170] | Goal | Precedents |
|---|---|---|---|
| Negative obligations | | | |
| 5(2)(a) | Not process personal data from third parties | Inter-platform | Bundeskartellamt (BKA), *Facebook*[171]<br>Competition and Markets Authority (CMA), Digital advertising market study[172] |
| 5(2)(b), (d) | Not combine personal data from CPS with data from third parties and other services gatekeeper | Inter-platform | BKA, *Facebook* and *Facebook/Oculus*[173]<br>Autorità Garante della Concorrenza e del Mercato (AGCM), *Facebook*[174]<br>CMA, Digital advertising market study |
| 5(2)(c) | Not cross-use personal data from CPS in other services gatekeeper | — | Belgian Competition Authority, *Nationale Loterij*[175]<br>Autorité de la concurrence (AdlC), *Engie*[176]<br>AGCM, *Enel*[177] |
| 5(3) | Not impose narrow and wide most favored nation clauses (MFNs) | Respectively intra- and inter-platform | EC, *E-books [Apple]*[178] and *E-book MFNs (Amazon)*[179]<br>CMA, *Amazon*[180]<br>BKA, *Amazon*,[181] *HRS*,[182] *Booking*,[183] *Verivox*[184] and *Amazon*[185]<br>AdlC, AGCM and Konkurrensverket, *Booking*[186]<br>Paris Commercial Court, *Amazon*[187] |
| 5(4), 5(5) | Not impose anti-steering and supporting measures (cross-platform access to content) | Intra-platform | EC, *Apple App Store Practices*[188]<br>Dutch Competition Authority (ACM), *Apple*[189] |
| 5(7), 5(8) | Not require use of certain secondary services or registration with other CPS | Intra-platform | ID service: BKA, *Facebook/Oculus*<br>Web browser: CMA, Mobile ecosystems market study[190] and subsequent Mobile browsers market investigation[191]<br>Payment: EC, *Apple App Store Practices*; ACM, *Apple* and CMA, Mobile ecosystems market study<br>Other CPS: EC, *Google Android*[192] and *Facebook Marketplace*[193] |
| 6(2) | Not use business users' data to compete with them | Intra-platform | EC, *Amazon Marketplace*[194] and *Facebook Marketplace* |
| 6(5) | Not self-preference in ranking | Intra-platform | EC, *Google Search (Shopping)*[195] and *Amazon Buy Box*[196]<br>AGCM, *Amazon*[197] |
| 6(6) | Not restrict switching between secondary services | Intra-platform | — |

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DMA

- **The DMA Obligations**

| Positive obligations | | | |
|---|---|---|---|
| 6(3) | Allow un-installation and prompt default selection (search, browser, assistant) | Intra-platform | EC, *Microsoft I* (tying abuse),[198] *Microsoft II*[199] and *Google Android*<br>CMA, Mobile ecosystems market study |
| 6(4) | Allow installation and default selection of third-party apps, app stores | Inter-platform | — |
| 6(7) | Allow equal interoperability with hardware and software features | Intra-platform | EC, *Microsoft I* (refusal to supply abuse) and *Apple Mobile Payments*[200]<br>ACM, Big Techs in the payment system (report),[201] see also the subsequent investigation[202]<br>AdIC, *Google (online advertising)*[203]<br>AGCM, *Android Auto*[204]<br>See also the German "Lex Apple Pay"[205] |
| 6(9) | Provide end-users data portability | Inter-platform | —, but see GDPR, art 20 |
| 6(10) | Provide business users access to self-generated data | Intra-platform | — |
| 6(11) | Provide FRAND access to search data | Inter-platform | —, but see CMA, Retail banking market investigation[206] and PSD2[207] |

| Article | Obligation[170] | Goal | Precedents |
|---|---|---|---|
| 6(12) | Provide FRAND access to app stores, search and social | Intra-platform | App stores: Paris Commercial Court, *Google*[208]; ACM, Mobile app stores market study[209] and CMA, Mobile ecosystems market study<br>Search: EC, *Google Search (Shopping)* |
| 6(13) | Maintain proportionate CPS termination terms | Inter-platform | — |
| 7 | interoperability of NIICS | Inter-platform | —, but see Communications Code[210] |

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DMA

- **The DMA Obligations**

**Positive obligations or "dos"** - prescriptive rules - are less usual for competition law. When it comes to remedies, a simple injunction does not suffice; rather, positive obligations require the enforcer to specify a desired course of action in greater detail ("proactive" remedies). Such remedies are not unheard of in competition law but are usually avoided given that they come with a greater need for design expertise and consistent monitoring. It is therefore only logical that most of the DMA's positive obligations are those that are "susceptible of being further specified" (Article 6). The text hints at the nature of such obligations with phrases like "shall allow (and technically enable)" and "shall provide." A good example is the obligation of gatekeeper search engines to provide third parties with access to ranking, query, click, and view data on FRAND terms. Positive obligations tend to relate to the DMA's contestability goal, that is, the promotion of inter-platform competition.

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

# COMPETITION VS. REGULATION IN DIGITAL MARKETS

# THE DIGITAL SERVICES ACT PACKAGE: THE CASE OF THE DIGITAL SERVICES ACT («DSA»)

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

- The DSA has been published in the Official Journal as of 27 October 2022 and came into force on 16 November 2022. The DSA will be directly applicable across the EU and will apply fifteen months or from 1 January 2024, whichever comes later, after entry into force.

- For online platforms, they must publish their number of active users by 17 February 2023. If the platform or a search engine has more than 45 million users (10% of the population in Europe), the Commission will designate the service as a very large online platform or a very large online search engine. These services will have 4 months to comply with the obligations of the DSA, which includes carrying out and providing the Commission with their first annual risk assessment. EU Member States will have to appoint Digital Services Coordinators by 17 February 2024, when also platforms with less than 45 million active users have to comply with all the DSA rules.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

- The **DSA introduces a new regulatory framework for online platforms**. Its goal is to encourage them to fight objectionable content while respecting users' fundamental rights.
- The DSA **updates and complements the provisions of Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market** (ecommerce Directive), since this Directive no longer appears adequate for governing today's platforms which operate globally, are predominantly managed by algorithms, and host that may be harmful.
- The **adoption of the DSA is a significant achievement resulting from a long-term effort by European authorities to promote responsible moderation practices among major social media platforms**. Over the past two decades, as social networks have expanded, platform operators have increasingly relied on algorithms to curate and moderate content.
- However, the trend towards the privatization and automation of online speech control has raised concerns.

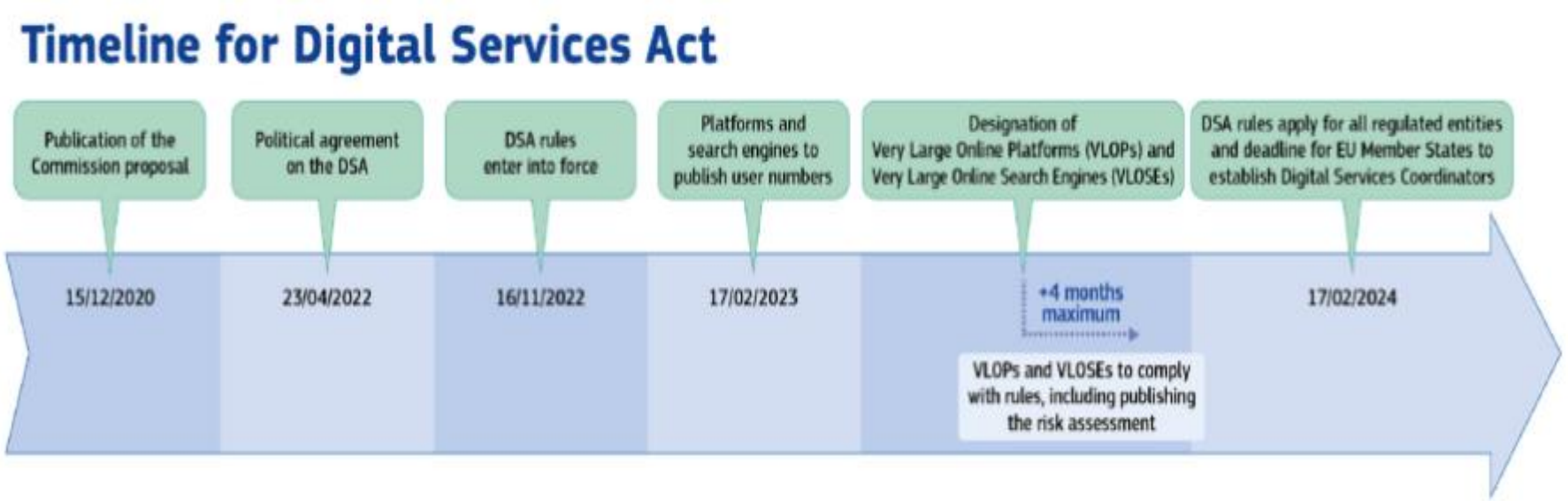
# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

- Flawed moderation practices have prompted European authorities to take action and encourage platforms to implement effective policies against online hate and disinformation.
- In May 2016, Facebook, Microsoft, Twitter, and YouTube entered into an agreement with the EU Commission known as the **"Code of Conduct on countering illegal hate speech online"** to prevent and combat the spread of hate speech on their respective platforms. Over time, other tech companies have also joined this code of conduct.
- In 2018, the EU Commission introduced the aforementioned **"Code of Practice on Disinformation"**, which around 38 tech companies have committed to following. This code was amended and strengthened in 2022 and includes a series of commitments and specific measures designed to address concerns related to disinformation.
- Finally, on March 1, 2018, **the EU Commission published its "Recommendation C/2018/1177 on Measures to Effectively Tackle Illegal Content Online",** which encouraged tech companies to enhance their notice and action procedures, among other things, to more effectively address illegal content on their platforms.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

- However, the DSA is not the only recent legislative instrument affecting platforms' liability and content moderation policies.
- Two legislations, in particular, have consistently strengthened the liability of online platforms and increased their obligations.
- **The Directive 2019/790 on copyright and related rights in the Digital Single Market** establishes that providers of online content-sharing services are directly responsible when users illegally upload protected content.
- Providers may be exempt from liability if they have made best efforts to obtain an authorization from the right holder and to block unauthorized content, if they acted expeditiously to remove a content following a notification from a right holder and if they proactively prevented future upload of that content.
- **Regulation 2021/784 of 29 April 2021 on combating terrorist content online** requires hosting service providers to take measures to prevent its dissemination, including removing terrorist content within one hour after receiving a notice from law enforcement. The adoption of the DSA is another evolution in the EU's ongoing efforts to regulate online platforms and fight against illegal activities on the Internet.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA



# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

**European Commission – Press release**

## Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines

Brussels, 25 April 2023

Today, the Commission adopted the first designation decisions under the Digital Services Act (DSA), designating **17 Very Large Online Platforms** (VLOPs) and **2 Very Large Online Search Engines** (VLOSEs) that reach at least 45 million monthly active users. These are:

**Very Large Online Platforms:**

- Alibaba AliExpress
- Amazon Store
- Apple AppStore
- Booking.com
- Facebook
- Google Play
- Google Maps
- Google Shopping
- Instagram
- LinkedIn
- Pinterest
- Snapchat
- TikTok
- Twitter
- Wikipedia
- YouTube
- Zalando

**Very Large Online Search Engines:**

- Bing
- Google Search

The platforms have been designated based on the user data that they had to publish by 17 February 2023.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

- The Digital Services Act has a vast and comprehensive scope that aims to **regulate the activities of "intermediary services" offering digital services** to legal entities in the European Union, as stated in Article 2.

- **It is immaterial whether the provider is based in the EU or not under the DSA**. If the service provider does not have an establishment in the EU, the DSA's applicability is subject to the "substantial connection" condition with the EU, as outlined by Article 3(d). This means that the provider must have a significant number of EU-based users or targets its activities towards a specific EU member state, such as by using a relevant top-level domain name (Article 3(e) DSA).

- All providers of intermediary services must appoint a **single point of contact allowing for direct communication with the competent supervisory authorities and users**, as provided by Article 11 and 13.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

- The key features of the Digital Services Act can be summarized in **five points**.
- **First**, it is an asymmetrical regulation.
- **Second**, it upholds the principle of exemption from liability while introducing the Good Samaritan principle.
- **Third**, it introduces new obligations for content moderation to combat undesirable content effectively and better protect users' rights.
- **Fourth**, it includes specific provisions aimed at enhancing user and consumer protection.
- **Finally**, it contains very specific implementation and enforcement procedures.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

## 1. Asymmetric regulation

- While the scope of the Digital Services Act is broad, it solely governs **"intermediary services“** rather than the “**information society services”** regulated by the E-Commerce Directive.
- “Intermediary services” refer **to those that transmit and store user-generated content**, as per Article (3)(g) DSA. The DSA further classifies **different types of "intermediary services"** that are available to users in the European Union.
- The **first three categories** were already present in the E-commerce Directive and **include "mere conduit" services, "caching" services, and "hosting" services**.
- The DSA adds **two new categories**: **"online platforms"**, which are a category of hosting services that disseminate information to the public, and **"online search engines"**.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

## 1. Asymmetric regulation

- The distinctions among different service types are significant because the **DSA is not meant to be uniformly applied to all regulated service providers**. Instead, the **DSA takes the form of a "layer cake", designed to be applied asymmetrically** with rules that vary depending on provider characteristics.
- In other words, the **DSA's obligations are structured as a pyramid**, with layered requirements from the bottom to the top. At the base of the pyramid, **the first layer encompasses all intermediary services that have very basic obligations, followed by hosting services, and then online platforms**.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

## 1. Asymmetric regulation

- Moving up the pyramid reveals increasingly **stringent obligations that apply to fewer and fewer categories of providers**.
- At the top of the pyramid, **the most extensive and restrictive obligations are imposed on very large online platforms (VLOPs) or search engines (VLOSEs)** that have at least 45 million average monthly active users in the EU. These additional obligations are justified by the **systemic risks** they pose due to their size.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

## 1. Asymmetric regulation

- While large companies face heavier obligations, **micro and small companies are exempt from certain obligations**. For instance, transparency obligations (article 15), provisions applicable to online platforms (section 3) and provisions applicable to platforms allowing consumers to conclude distance contracts with traders (section 4) are not applicable to micro or small enterprises.
- These small enterprises are defined as companies with **fewer than 250 employees and an annual turnover under €50 million or an annual balance sheet total under €43 million**, as per Recommendation 2003/361/EC.
- Despite this exemption, it could be argued that the threshold are too low and that the DSA's stringent obligations may negatively impact the financial stability and growth of small and medium-sized enterprises, since the companies that are just above these thresholds would be penalized.
- As a result, the DSA would benefit larger platforms and search engines that have the resources to comply with its provisions. In any case, an assessment of the DSA's impact on micro and small companies will be conducted by the Commission after five years, as provided by Article 91(2)(d).

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

## 2. Liability exemption

- **The DSA preserves the exemption from liability established by the E-Commerce Directive in 2000**, with additional clarifications. One significant addition is the inclusion of the **Good Samaritan clause**, which draws inspiration from section 230 of the US Communications Act of 1934.
- The E-Commerce Directive introduced a **new category of service providers called "hosting service providers"** and provided, in its article 14, that these hosting providers are exempt from liability for content stored at a user's request if **they have no actual knowledge of its illegality**. Providers of mere conduit and caching services are similarly not held liable for the information they transmit or store for their users.
- The DSA upholds the liability exemption provided by the E-Commerce Directive for over 20 years. **Article 6 of the DSA provides hosting providers with protection from liability for illegal content stored on their platforms**.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

## 2. Liability exemption

- This protection applies **if they act "expeditiously" to remove access to the content once they become aware of its illegality**. Similarly, Article 4 specifies that mere conduit service providers are not liable for the information transmitted or accessed if they do not initiate the transmission, select the receiver of the transmission or modify the information contained in the transmission.
- Under Article 5, caching service providers are not liable if they do not modify the information and act expeditiously to remove or to disable access to the information upon obtaining actual knowledge of the fact that the information has been removed from its initial source or when required by law or a court order. They must also not interfere with the lawful use of technology.
- Unlike the provisions of the E-Commerce Directive, which had to be transposed into national law, **this liability exemption now applies directly and uniformly across all EU countries**.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

## 2. Liability exemption

- **Article 7 of the DSA allows providers to carry out voluntary investigations or take other measures to detect, identify and remove illegal content**. However, some may worry that this could lead to platforms being considered playing an active role that gives them knowledge or control over the content and losing their exemption from liability as a result. In reality, **engaging in these investigations does not automatically make platforms responsible for the content**. **The Good Samaritan clause was added to the DSA in response to requests from online platforms** for greater clarity and reassurance that they could take voluntary steps to remove illegal content without losing their liability exemption.
- The newly introduced Good Samaritan clause draws inspiration from Section 230 of the US Communications Act of 1934, specifically 230(c)(2)(A), which offers Good Samaritan immunity to platforms. **This immunity allows platforms to intervene in good faith on content without incurring any liability**.
- In the virtual space, **the Good Samaritan immunity guarantees that providers and users of online services will not be held liable for any action taken in good faith to remove or restrict access to content that the provider or user considers objectionable**. Under the DSA, the Good Samaritan clause ensures that providers **can detect and remove illegal content without losing their liability exemption**.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

## 3. New due diligence obligations for content moderation

- **The DSA introduces additional obligations for intermediary service providers beyond the existing knowledge-based liability principle that has been in place for over two decades**. The new obligations provided by the DSA stem from concerns about the effectiveness of the existing knowledge-based liability principle in compelling platforms to address illegal content.
- **The DSA's new obligations are primarily centered around the content moderation activities carried out by the platforms**. This is why the DSA introduces, in Article 3(t), a **broad definition of "content moderation"** as "the activities, whether automated or not, undertaken by providers of intermediary services, that are aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible" with the providers' terms and conditions, including "measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetisation, disabling of access to, or removal", or that affect the ability of users to publish or transmit information, such as the termination or suspension of a user's account.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

## 3. New due diligence obligations for content moderation

- With this definition, **the DSA recognizes the crucial role played by platforms in moderating content**, often using automated tools. It also acknowledges that this moderation activity is not only based on the applicable laws, but **also governed by the platforms' terms and conditions**, which is reflected by the fact that most major platforms now publish increasingly detailed content policies.
- Consequently, the DSA's new obligations related to content moderation can be grouped into **four categories**: **combating illegal content, upholding procedural safeguards in moderation, ensuring transparency, and managing systemic risks**.

## 3. Combating illegal content

- The DSA not only maintains the liability exemption, but it also imposes **new obligations on online platforms to effectively combat illegal content**. This fight against illegal content involves the users and relies mainly on user notifications. The DSA includes extensive guidelines on how to handle user notifications, which have not been as detailed in the past. **Article 16 requires providers of hosting services to establish accessible "notice and action" mechanisms that allow anyone to notify them of the presence of illegal content**.
- The main goal is to make sure that these notice and action procedures are effective in combating illegal content while also safeguarding the rights of users, including protection against unjustified removal.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

## 3. Combating illegal content

- Therefore, **hosting platforms must implement efficient reporting mechanisms and have clear and user-friendly reporting systems in place to enable users to report illegal content**.
- To that end, providers are required by **Article 12 to designate a single point of contact to facilitate direct and rapid communication through electronic means**.
- In addition, Article 22 requires providers to **prioritize reports from trusted flaggers**, which are entities designated by competent national authorities that have demonstrated expertise and competence in identifying illegal content.
- Hosting service providers must **process received notifications in a timely, diligent, non arbitrary, and objective manner, as provided by Article 16(6)**.
- However, it must also be highlighted that providers do not have to take action on the reported content following the reception of a user's notice. **They are only expected to remove the content if the notice is sufficiently clear and adequately substantiated, and if the illegality can be established without a detailed legal examination, as outlined by Article 16(3).**

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

**3. Combating illegal content**

- The fight against illegal content also depends on **effective collaboration with national authorities**.
- **Article 18 imposes an obligation on online platforms to cooperate with national law enforcement or judicial authorities and promptly notify them of any content that may give rise to suspicions of criminal offenses posing a threat to the life or security of individuals**.
- The purpose of this obligation is to **prevent or swiftly address serious crimes**. However, this obligation is limited to criminal offenses that pose a threat to the life or safety of one or more persons, and it does not cover other criminal acts. Additionally, providers must comply with any instructions from authorities to act against illegal content and must justify the measures taken.
- **Articles 9 and 10 provide that national judicial or administrative authorities may issue orders requiring providers to act against specific illegal content or provide information about certain users, but such orders must not constitute a general monitoring obligation**.
- Indeed, the **DSA maintains, in Article 8, the prohibition of mandated general monitoring that already existed in the E-Commerce Directive**. The prohibition concerns obligations "of a general nature" as opposed to obligations "in a specific case", as stated by Recital 30. An example of an obligation “of a general nature” is **the obligation to introduce a system for filtering all electronic communications for an unlimited period and at the provider’s expense in order to block unlawful use or transfer of copyrighted works**. However, an obligation for a service provider to identify and remove specific information deemed illegal by a court and equivalent information is not covered by the prohibition. Despite existing precedents, it is not always easy to distinguish between general and specific obligations.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

### 3. Upholding procedural safeguard in content moderation

Online platform providers not only moderate content in accordance with the relevant laws and regulations, but also **set their terms and conditions, which allow them to determine their own content policies and decide what content to host or remove**.

These moderation standards serve as a private norm that governs online speech in practice. The **DSA is actually one of the first pieces of legislation to recognize the crucial role played by terms and conditions in content moderation**, while also trying to guarantee that the determination of these standards and their enforcement is in accordance with the fundamental rights of users.

To that end, **the DSA adopts a procedural perspective and imposes due process obligations** intended to serve as safeguards against possible arbitrariness by platforms. Furthermore, the DSA does not interfere with the freedom of hosting providers to establish their own content policies.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

**3. Upholding procedural safeguard in content moderation**

The DSA stipulates in **article 14 that providers are required to clarify "any restrictions that they impose in relation to the use of their service" in their terms and conditions**.

The information provided must include «any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making, and human review as well as rules of procedure of their internal complaint handling system».

This requirement has been **analyzed as a form of "codification" of moderation rules**, enabling the enforcement of "the rule of law's principles of legality, predictability, and accessibility for the imposition of sanctions".

Furthermore, **Article 14(4) mandates that service providers must act diligently, objectively, and proportionately while applying and enforcing their terms and conditions**, taking into account the rights and legitimate interests of all parties involved, including users' fundamental rights.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

### 3. Upholding procedural safeguard in content moderation

In addition to clarifying their terms of use, **platforms are obliged to provide a clear and specific explanation of the reasons for the decisions they make about content provided by users constituting either illegal content or being incompatible with their terms and conditions**.

This “statement of reasons” will allow users to challenge the moderation decisions made about them.

The scope of this obligation to provide explanation is particularly broad. Indeed, as illustrated by the wording of the abovementioned Article 3(t), the DSA's definition of moderation actions is comprehensive and all-encompassing.

Article 17 stipulates an **explanation must be provided in the case of “any restrictions of the visibility”**, including “removal of content, disabling access to content, or demoting content”, and in case of suspension, termination or other restriction of monetary payments, of the service, or of the service’s account. In other words, the statement of reasons is required in cases where content is removed, demonetize or demoted, including instances of "shadow banning," where a user's content is concealed from others without their knowledge.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

### 3. Upholding procedural safeguard in content moderation

**According to Article 20, providers must establish an efficient internal complaint handling system that allows users to challenge moderation decisions they believe to be unjust or incorrect**.

This system should enable users to contest decisions related to the removal of allegedly illegal content or the suspension of their account or service provision, as well as decisions not to act on a notice of illegal content. Moderation decisions must be reversed when the complaint contains sufficient grounds.

The DSA provides that **such complaints must be reviewed "in a timely, non-discriminatory, diligent and non-arbitrary manner"**, as stated by Article 20(4).

According to Article 20(6), the appeal decisions must be "taken under the supervision of appropriately qualified staff, and not solely on the basis of automated means".

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

## 3. Upholding procedural safeguard in content moderation

- Users also have **the option to submit disputes to an out-of-court dispute settlement body certified in one of the Member States** based on their independence and expertise, as per Article 21.
- However, this provision may not be effective since Article 21(3) subparagraph 3 provides that "the certified out-of-court dispute settlement body shall not have the power to impose a binding settlement of the dispute on the parties".
- This means that in case of persistent disagreement on moderation decisions, **users will have no other option than to go to court at their own expense, as provided by Article 21(1), subparagraph 3**. Indeed, Article 54 provides that users can always request compensation for any damages or losses incurred due to a breach of the DSA. They can even bring representative actions for the protection of collective consumer interests, as per Article 90.
- **Article 23 provides that online platform providers are required to suspend services to such users, subject to several safeguards**. The user must have been previously warned and the suspension must also be limited to a reasonable period of time. Providers must assess each case individually, in a timely, diligent, and objective manner, and clarify their policies in advance in the terms and conditions.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

### 3. Ensuring transparency

- The DSA not only implements procedural due process but also seeks to **incentivize platforms to act in a responsible manner by imposing precise transparency obligations on them**, especially regarding their moderation practices.
- According to Article 15 of the DSA, **all intermediaries except micro and small enterprises must report annually on their content moderation**. The report must provide information about content moderation at the providers' own initiative, including the use of automated tools. It must include, among other things, the number and type of measures taken that affect information availability, visibility and accessibility and the number of orders received from Member States' authorities categorized by the type of illegal content concerned. Hosting providers must also disclose "the number of notices submitted categorized by the type of alleged illegal content concerned, the number of notices submitted by trusted flaggers, any action taken pursuant to the notices by differentiating whether the action was taken on the basis of the law or the terms and conditions of the provider, the number of notices processed by using automated means and the median time needed for taking the action" (Article 15(1)(b)).

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

## 3. Ensuring transparency

- Online platforms must add information about the basis for the complaints received, the decisions taken following those complaints, the median time needed for taking those decisions and the number of instances where those decisions were reversed. They must also provide information about the number of disputes submitted to out-of-court settlement bodies and the number of service suspensions following the publication of manifestly illegal content or manifestly unfounded notices or complaints, as provided by Article 24. The information reported must be categorized by the type of illegal content or violation of the terms and conditions of the service provider, by the detection method and by the type of restriction applied.
- The DSA imposes increased transparency and accountability measures for very large online platforms (VLOPs) and search engines (VLOSEs). These operators must publish transparency reports twice a year that include information about their content moderation resources and the qualifications of their moderators, as provided by Article 42. In addition, VLOPs and VLOSEs must provide regulators with access the data needed to verify that they are in compliance with the DSA, as stated by Article 40(1)). In this respect, they must be able to explain to regulators the design, logic, operation and testing of their algorithmic systems, including their recommendation systems.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

## 3. Managing systemic risks

- **Article 34 of the DSA stipulates that very large online platforms (VLOPs) and search engines (VLOSEs) with at least 45 million users must evaluate and address "systemic risks" through appropriate policies**.
- They must analyze the extent to which their moderation, recommendation, and advertising systems may affect those systemic risks. This should be done annually and also prior to the deployment of functionalities that are likely to have a critical impact on the risks identified.
- Systemic risks pertain to issues such as illegal content, hate speech, privacy violations, election manipulation, and other similar problems. Moreover, content that generates adverse effects on fundamental rights, civic discourse, electoral processes, public security, gender-based violence, public health, minors, and personal well-being may also lead to systemic risks.
- Although Article 35(1) mentions "illegal hate speech or cyber violence", the definition of systemic risks encompasses content that is not necessarily illegal but may cause problems, such as misinformation on public health, climate change, or politics.
- After assessing systemic risks, VLOPs and VLOSEs should implement "reasonable, proportionate, and effective mitigation measures" to counter such risks, as provided by Article 35.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

## 3. Managing systemic risks

- Moreover, the DSA introduces a unique monitoring system to enforce compliance with these obligations, which includes vetted researchers in addition to national and European regulatory bodies.
- First, VLOPs and VLOSEs are required to provide their assessments of systemic risks to the European Commission and relevant Digital Services Coordinators upon request, as per Article 35(2). The European Board of Digital Services will work with the Commission to publish annual reports on the identification and assessment of systemic risks, including best practices for mitigating these risks (Article 35(2)). Additionally, the Commission may issue guidelines and recommend actions in cooperation with Digital Services Coordinators (Article 35(3)). Within this framework, regulators play a role in determining and approving the strategies implemented to mitigate systemic risks.
- Second, regulators will also benefit from the expertise of researchers who will be provided with access to platform data to evaluate systemic risks. Indeed, Article 40 states that VLOPs and VLOSEs must provide internal data on request to researchers vetted by national regulators. This provision allows researchers to request whatever data they need to asses those risks and to go much further than the analyses provided in the reports prepared by the platforms themselves.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

### 3. Managing systemic risks

- By providing for measures to address the "systemic risks" generated by the operation of large platforms and search engines, the DSA goes far beyond the simple fight against content deemed illegal by the national laws of the various Member States. This includes considering not only illegal content but also "lawful but awful" content that may be harmful. In particular, while European national laws often criminalize hate speech, the same cannot be said of disinformation, which is often difficult to define or demonstrate, and is rarely sanctioned as such.
- In this context, the category of systemic risks can ideally serve as a basis for implementing effective policies to fight disinformation, in line with the Code of Practice on Disinformation implemented at the European Union level. Furthermore, Article 35 enables regulators to issue guidelines and recommendations to mitigate systemic risks, which could include suggestions on the content of platforms' terms and conditions and content policies.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

## 4. Other obligations

- In addition to regulating moderation practices, the DSA contains provisions designed to protect users of online services more generally and in particular consumers who use the services of marketplaces and collaborative economy platforms.
- The DSA includes specific provisions for recommendation systems. According to Article 27, online platforms must provide precise and intelligible information in their terms and conditions about the main parameters used by their recommendation systems.
- Furthermore, the DSA strictly regulates online advertising. Advertising platforms must fully disclose their practices and targeting methods to advertisement recipients as per Article 26.
- Online platform providers must indicate on whose behalf and why the advertisement is being displayed to the user (Art. 26(1) DSA). VLOPs and VLOSEs must maintain a publicly accessible repository containing information about advertisements presented, including their content and the companies on whose behalf they were made, as provided by Article 39 DSA.
- Additionally, article 26(3) prohibits displaying advertising based on profiling using sensitive data such as political opinions, religious beliefs, and sexual orientation. Targeted advertising of minors based on their personal data is prohibited, and specific protection measures must be put in place to ensure their safety online, as per Article 28.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

**4. Other obligations**

- Finally, the DSA strictly prohibits the use of "dark patterns" that manipulate internet users into performing a specific action, such as subscribing to a service, by subconsciously influencing them. According to Article 25(1), providers of online platforms cannot “design, organize or operate their online interfaces in a way that deceives or manipulates” users or in a way that “otherwise materially distorts or impairs the ability of” users “to make free and informed decisions”.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

**4. Specific protection of consumers on marketplaces and collaborative economy platforms**

- Online platforms that allow the conclusion of distance contracts between consumers and traders, such as marketplaces and collaborative economy platforms, have specific obligations that they must fulfill. These obligations include obtaining certain information about their professional users, such as their name, contact details, and identification and registration information, through "know your customer" protocols.
- Article 30 provides that online platforms must make best efforts to verify the accuracy and completeness of the information provided by professional users.
- In addition, these platforms are required by Article 31 to ensure that their interface is designed in a way that complies with consumer law regarding pre-contractual information obligations and product safety.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

**4. Specific protection of consumers on marketplaces and collaborative economy platforms**

- Additionally, these platforms are required to make “reasonable efforts to randomly check in any official, freely accessible and machine-readable online database or online interface whether the products or services offered have been identified as illegal”, as per Article 31 (3).
- If they become aware of any such illegality, they must inform the consumers who purchased the illegal product or service about the trader's identity and all relevant means of redress, as provided by Article 32 DSA.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

**5. Implementation of the DSA**

- In certain respects, the implementation of the DSA is less complicated than that of the Ecommerce Directive, as the Regulation is directly applicable and does not require a transposition law to be adopted by each Member State. However, implementing the DSA requires to determine which authorities are competent to enforce it and which measures these authorities can take.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

**5. Implementation of the DSA**

- The competent authorities to control the implementation of the DSA are the national authorities.
- Member States will designate "National Coordinators of Digital Services", as per Article 49. These coordinators will receive complaints from users, have investigative powers, and may impose sanctions. They will also convene in a European Board for Digital Services, an advisory body designed to promote coordination and cooperation between them.
- The DSA establishes that the Member State in which an intermediary service provider is established has exclusive jurisdiction over that provider, as stated by article 56(1). This principle aligns with the country of-origin rule established in Article 3 of the E-Commerce Directive. Recital 123 of the DSA defines "main establishment" as the location of a provider's head or registered office, where the primary financial functions and operational control take place.
- However, it may be difficult to determine exactly which authorities are responsible for enforcing the DSA. For VLOPs and VLOSEs, the European Commission has the power to enforce the DSA in collaboration with national authorities and coordinators. The Commission holds exclusive authority over obligations that apply solely to VLOPs and VLOSEs, as outlined in Article 56(2) of the DSA. Both National Coordinators and the Commission have jurisdiction over all other DSA obligations for VLOPs and VLOSEs, as per Article 56(3). The Commission will work with national coordinators to investigate potential violations and determine whether to impose fines.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

**5. Implementation of the DSA: enforcement**

The potential severity of penalties for non-compliance with the DSA should incentivize

companies to comply with its provisions. Penalties will be defined in national law and must be “effective, proportionate, and dissuasive”, as provided by Article 52. The maximum penalty cannot exceed 6% of the company’s annual turnover. For some infringements, such as providing incorrect or incomplete information or refusing to comply with inspections, the maximum penalty may be raised to 1% of annual turnover. Companies may also face periodic fines, with each monthly payment not exceeding 5% of their daily turnover.

The European Commission can also impose fines up to these amounts. Repeated non-compliance may result in access restrictions but not a definitive ban within the EU. Under article 82 of the DSA, the European Commission can request a regulator to ask a judicial authority to temporarily restrict user access if there is a serious and persistent breach causing significant harm and involving a criminal offense threatening people’s safety or lives. Therefore, non-compliance may result in temporary access restrictions and fines at worst.

# Competition vs. Regulation
# The Digital Service Act Package: the case of the DSA

**5. Implementation of the DSA: enforcement**

In addition to potentially high penalties for non-compliance, the DSA includes mechanisms designed to encourage compliance by the largest entities.

VLOPs and VLOSEs must appoint a compliance officer, as per Article 41. VLOPs and VLOSEs must also conduct annual independent audits to assess their compliance with the DSA and submit reports to competent authorities (article 37). These reports must include information on measures taken to prevent the dissemination of illegal content on the platform, as well as details of the platform's internal complaint handling system and content moderation procedures.

Compliance with the provisions for controlling systemic risks by VLOPs and VLOSEs is based on an "enhanced supervision system" provided by Article 75. Under this system, the Commission may request that very large platforms provide regulators with an action plan to address potential violations of the DSA.

This action plan may include conducting an independent audit. The Commission has the discretion to determine whether the action plan is sufficient and may reject it if deemed inadequate.

Finally, the DSA stipulates in Article 45 that regulators must encourage and facilitate the development of voluntary codes of conduct at the Union level to support the proper application and ensure consistent implementation of the Regulation, particularly in regards to combating illegal content and mitigating systemic risks.

The Commission and the European Board of Digital Services are tasked with promoting and supporting the creation of these codes of conduct.

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

# COMPETITION VS. REGULATION IN DIGITAL MARKETS

# THE DIGITAL SERVICES ACT PACKAGE: THE CASE OF THE DIGITAL GOVERNANCE ACT («DGA»)

# Competition vs. Regulation: the case of the DGA

- The Data Governance Act ("DGA") is a cross-sectoral instrument that aims to make more data available by regulating the re-use of publicly/held, protected data, by boosting data sharing through the regulation of novel data intermediaries and by encouraging the sharing of data for altruistic purposes. Both personal and non-personal data are in scope of the DGA, and wherever personal data is concerned, the General Data Protection Regulation (GDPR) applies. In addition to the GDPR, inbuilt safeguards will increase trust in data sharing and re-use, a prerequisite to making more data available on the market.

# Competition vs. Regulation: the case of the DGA

- Chapter II of the Act aims to **unlock more value in data held by the public sector**, by opening up this data for **re-use.** Recital 5 explains the objective well:
- "The idea that data that has been generated or collected by public sector bodies or other entities at the expense of public budgets should benefit society has been part of Union policy for a long time [via the Open Data Directive] … However, **certain categories of data (commercially confidential data, data subject to statistical confidentiality, data protected by intellectual property rights of third parties, including trade secrets and personal data) in public databases is often not made available**… not even for research or innovative activities in the public interest…".
- Chapter II aims to promote use of these "difficult" types of data. The provisions **apply to public sector bodies and aim to facilitate "re-use" of the data** – that is, use for commercial, or non-commercial purposes, other than the initial public task for which the data were produced. There are exclusions – for example, the **Act does not cover data held by public undertakings** (owned by public bodies), broadcasters, cultural establishments, data which are protected for reasons of national security, defence or public security.

# Competition vs. Regulation: the case of the DGA

- Like the Open Data Directive, **the Act does not oblige public sector bodies to allow re-use of data, but where data are made available for re-use then it requires that access arrangements must be non-discriminatory, transparent, proportionate, objective and may not restrict competition**. Exclusive access arrangements are restricted. There are also restrictions on fees payable for access.
- Public sector bodies who do provide access must ensure that they **preserve the protected nature of the data**. By way of example, this could mean only releasing data in anonymous form. Or it could mean using secure processing environments – physical or virtual environments which allow access to data, whilst ensuring compliance with other laws and preserving the protected nature of the data. Recital 6 specifically calls put the potential for use of differential privacy and synthetic data as ways of allowing exploitation of data. Those who wish to re-use the data, must agree to continue to respect the protected nature of the data; where data has been released that was originally personal, then this would include agreeing not to attempt to re-identify data subjects.

# Competition vs. Regulation: the case of the DGA

- If a public sector body receives a request to release data, but cannot do so in a compliant way, even by using the techniques above, then **it has an obligation to use best efforts to seek consent to re-use from the data subject/ affected person**, unless this would involve disproportionate effort.
- Allowing re-use of data which is personal, confidential, or otherwise protected by IPRs, whilst simultaneously not prejudicing those same interests, will be difficult. To assist in this, the Commission requires **each Member State to have a competent body to support public authorities in these tasks**. To facilitate re-users of the data, the Member State must also ensure that there is a single point, to which requests for re-use can be directed. This must also list all datasets available for re-use. The Commission will also create an EU wide single access point.

# Competition vs. Regulation: the case of the DGA

- Chapter III of the Act **aims to encourage a new market in neutral data intermediation services**. This is on the basis that, "specialised data intermediation services that are independent from data subjects and data holders [person with a right to license data], and from data users [person with a right to use data], could have a facilitating role in the emergence of new data-driven ecosystems…". The Chapter seeks to achieve this by imposing a **licensing regime on data intermediation services**, where the licence conditions are designed to ensure independence.
- Data intermediation services are services which **aim to establish commercial relationships, for the purpose of data sharing, between an indeterminate number of data holders (or data subjects) and data users**. These commercial relationships could be established through technical, legal or other means. The concept is limited to pure facilitation of data sharing – accordingly, providers who enrich data or otherwise add value to it are not included. Providers who intermediate copyright protected content; closed group arrangements; and arrangements by a single data holder to allow exploitation of its own data are all excluded, as are intermediation services provided by public sector bodies without "aiming to establish commercial relationships for purpose of data sharing". Browsers and email service providers and account information service providers under the PSD2 Directive are also excluded. However, data marketplaces are specifically mentioned as a type of intermediation service.

# Competition vs. Regulation: the case of the DGA

- Intermediation services could also include services set up to intermediate between data subjects who want to make their personal data available, and data users who want to use such personal data. Here, the Act notes the risk of "misaligned incentives". Any intermediation service provider offering services to data subjects must "act in their best interests" when facilitating the exercise of their rights, in particular in providing information about the intended uses of data (and any uses of consented data outside the EU). The Act also anticipates the creation of specialised forms of data intermediaries, "data co-operatives", which are – in effect – owned by the data subjects they represent and whose principal objective is to support data subjects in exercising their rights.

- The Act sets up a two-tier licensing structure. All intermediation service providers must notify (i.e. complete a filing with) the relevant competent authority and must meet specified conditions. Intermediation service providers may also (but are not required to) ask the competent authority to confirm if the provider meets these conditions. If the competent authority issues this confirmation, the provider is then able to use a to-be-developed Commission logo and to use the legend "provider of data intermediation services recognised in the Union" in communications. The competent authority for a service provider is the authority in the member state where the service provider has its main establishment and service providers with no EU presence must appoint a legal representative in the EU – all concepts familiar from the GDPR.

# Competition vs. Regulation: the case of the DGA

- Those offering intermediation services must meet conditions set out in Art.11, all designed to ensure independence. These conditions include the following: intermediation services have to be offered by a separate legal person (i.e. not offering other services); separate use of the data is prohibited; pricing cannot be linked to take up of other services; metadata about service use cannot be used for other purposes (but prevention of fraud/ cyber risk and service development is acceptable); data must be provided in the format received; it can only be converted if this is to enhance interoperability and the provider must allow an opt-out from this; the provider can offer tools to facilitate exchange of data – but must have approval of the data holder/ data subject to do this; licences must be on FRAND type terms; the provider must ensure availability and interoperability with other intermediation services; must put in place technical, organisational and legal measures to prevent transfer or access to non-personal data that would be unlawful & must notify the data holder of any unauthorised access/ use of non-personal data that has been shared and appropriate security measures must be maintained (in other words, GDPR style protections are introduced for non-personal data which is shared via an intermediation service) and, lastly, logs of all intermediation activity must be maintained.
- The recitals to the Act give the impression that data intermediation services will be new types of services, tied to yet-to-exist developments in the data economy. However, it seems possible that many existing organisations may be offering data intermediation services. The provisions seem to be particularly applicable in the ad-tech space. For example:

- Those offering data marketplaces; and
- (possibly) consent management platforms

could well be in-scope.

- Organisations offering services which facilitate access to personal data should, therefore, review the provisions in Chapter III carefully. If in scope, they have 24 months from the date the Act becomes applicable to meet the requirements in the Act.

# Competition vs. Regulation: the case of the DGA

**Data altruism**

The Act defines "data altruism" as "the consent by data subjects to process personal data pertaining to them, or permissions of other data holders **to allow the use of their non-personal data without seeking a reward that goes beyond a compensation related to the costs they incur making their data available, for purposes of general interest**, …, such as healthcare, combating climate change, improving mobility, facilitating the establishment of official statistics, improving public services, public policy making or scientific research purposes in the general interest".

The provisions in the Act on data altruism are relatively light touch. The Act notes that Member States may wish to promote altruism (including by allowing individuals to make personal data held by public sector bodies more widely available), but **there is no obligation to do so**. Likewise, the Act sets out a registration scheme for data altruism organisations, but – unlikely data intermediaries – **registration is voluntary**. Member States must designate a competent authority to manage the registration process and, as with data intermediaries, there are arrangements for organisations operating in multiple member states to register via their main establishment and for those with no EU establishment to nominate a representative.

# Competition vs. Regulation: the case of the DGA

## Data altruism

Under the Act, the lawful basis for altruistic use of a data subject's data **is consent given by the data subject**. The Commission is to **develop an European consent form for the altruistic transfer of data**, in order to **reduce the costs involved in obtaining consent and to facilitate data portability** (when the data to be transferred are not in the possession of the data subject).The form is to be modular, allowing for customisation for sector-specific consent templates. Some sector-specific working groups have already been working along these lines in order to explore this concept of data altruism, e.g. in the area of health and scientific research. Particularly relevant for this purpose is the project "Towards European Health Data Space" which develops European principles for the secondary use of health data and has recently produced a first set of data altruism definitions, use cases and conclusions that can be taken as a reference document when establishing a methodology for carrying out impact assessments aimed at mitigating possible risks that may arise.

# Competition vs. Regulation: the case of the DGA

## Data altruism

The term altruism seems to imply that **data should be given without expectation of anything in return**, and to suggest that the provisions are of relevance solely to not-for-profit organisations, but this is not necessarily the case. Many public bodies will probably participate in this data exchange without receiving anything in return in the first instance, but with the intention of being rewarded in the future with a much larger and more diverse set of information than they currently handle, which will likely bring them some kind of benefit. On the other side are projects that seek to directly benefit society and that seek to make a profit. In the era of Big Data, some projects are not entirely effective due to the lack of a truly large volume of information that allows for reliable data analysis. Being able to access wider sources of information will be a benefit. Such projects would not be able to become recognised data altruism organisations but could potentially still benefit from wider data altruism initiatives, facilitated by data subject consent and portability initiatives. These altruistic exchanges share certain features with free distribution systems regarding copyrighted works, such as Creative Commons or Copyleft licensing schemes. In both cases, the proliferation of information is based on the principles of altruism, collaboration, and the removal of restrictions for access to resources.

Under the GDPR, an informed consent form must be express and specific. It seems that this Act may allow a **more generic consent that opens the door to broader, future, purposes**. It is worthy of note that a similar provision already exists in Recital 33 of the GDPR, which recognises that it may not be possible to fully identify the purpose of particular scientific research purposes at the time of data collection and which allows consent to be given more broadly, to certain areas of scientific research, in line with recognised ethical standards.

# Competition vs. Regulation: the case of the DGA

**Data transfer**

The Act starts **to extend restrictions on transfers of data into non-personal data**. Accordingly, while the restrictions do not apply to personal data (because the GDPR already contains similar, or more extensive, restrictions), they may still be of relevance.

Most restrictions are introduced into re-use of public sector body data. **If a re-user intends to transfer non-personal data to a third country, then it has to notify the public sector body of this at the time that it requests re-use of the data**. The public sector body, in turn, must notify the parties who may be affected by this – and may only grant the re-use request if those parties give permission for the transfer.

Where transfers are permitted, then the re-user must give contractual assurances to comply with IPR & confidentiality requirements post transfer and to accept the jurisdiction of the courts of the Member State where the public sector body is based. **The Act also introduces a possibility for the Commission to adopt model contractual clauses and to declare certain countries to offer adequate protection for non-personal data, or to introduce additional restrictions for certain categories of non-personal data which pose a high risk**. The recitals to the Act set out the types of factors which the Commission must consider when assessing the adequacy of the level of protection offered – **these will be familiar from Schrems II**.

# Competition vs. Regulation: the case of the DGA

## Data transfer

- So far, the non-personal data transfer restrictions may sound of limited relevance: primarily affecting public sector bodies, or those receiving data form such bodies. However, Art. 30 extends these restrictions. This **introduces a general obligation on public sector bodies, those allowed data for re-use, as well as data intermediation and data altruism organisations to take all reasonable measures to prevent international transfers of or government access to non-personal data held in the Union, where this would conflict with EU or Member State law**.
- The Act also contains a provision equivalent to GDPR Art. 48 – noting that third country judgments or decisions requiring access to data are only recognised in the EU if based on an international treaty. Further, any re-user of public sector data, an intermediation service provider and any recognised data altruism organisation who receives a third country request for non-personal data that would conflict with EU or Member State law **must provide the minimum possible data in response to such a request and may only co-operate with it**, where either the request is recognised under an international treaty etc. or where conditions set out in the Act (addressing proportionality; court authorisation; and recognition of interests protected under EU or Member State law) are met. **The provider must also notify data holder of request – unless request is for law enforcement purposes (not national security) and where this is necessary to preserve effectiveness of the law enforcement activity. Providers of intermediation services, or data altruism services, which relate to non-personal data will, therefore, have to use transfer risk assessments and processes for dealing with public authority requests to access data**.

# Competition vs. Regulation: the case of the DGA

## Creation of a European Data Innovation board, compliance and enforcement

The Act requires an **European Data Innovation Board**, made up of a group of experts in the field, to be created. The Board should consist of representatives of the Member States, the Commission and relevant data spaces and specific sectors (such as health, agriculture, transport and statistics). The European Data Protection Board should be invited to appoint a representative.

**Member States must designate one or more competent authorities to administer the register of data altruism organisations and of data intermediaries and to enforce the legislation**. These **designated competent authorities must coordinate with other authorities that may have an interest, such as data protection authorities, national competition authorities, cybersecurity authorities and other relevant sectoral authorities**.

Article 31 of the Act states that fines are to be set and implemented by each Member State. Unlike the GDPR, **the Act does not prescribe the specific amounts and weighting factors applicable to the corresponding monetary sanctions**. However, similarly to Article 83 GDPR, the Act provides that Member States must ensure that the decided penalties are "effective, proportionate and dissuasive".

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

# COMPETITION VS. REGULATION IN DIGITAL MARKETS

# THE DIGITAL SERVICES ACT PACKAGE: THE CASE OF THE DATA ACT («DA»)

# Competition vs. Regulation: the case of the DA

On 23 February 2022, the European Commission unveiled its proposal for a Data Act (DA). As declared in the Impact Assessment, the DA complements two other major instruments shaping the European single market for data, such as the Data Governance Act and the Digital Markets Act (DMA), and **is a key pillar of the European Strategy for Data in which the Commission announced the establishment of EU-wide common, interoperable data spaces in strategic sectors to overcome legal and technical barriers to data sharing**.

The DA also represents the latest effort of European policy makers to ensure free flows of data through a broad array of initiatives which differ among themselves in terms of scope and approach: some interventions are horizontal, others are sector-specific; some mandate data sharing, others envisage measures to facilitate the voluntary sharing; some introduce general data rights, others allow asymmetric data access rights.

# Competition vs. Regulation: the case of the DA

The proposed DA aims to achieve five objectives:

- **to facilitate access to and the use of data by consumers and businesses**, while preserving incentives to invest in ways of generating value through data;
- to **provide for the use by public sector bodies and EU institutions of data held by enterprises** in certain situations where there is an exceptional data need;
- to **facilitate switching between cloud and edge services**;
- to **put in place safeguards against unlawful data transfer without notification by cloud service providers**;
- and to **provide for the development of interoperability standards for data to be reused between sectors**, in a bid to remove barriers to data sharing across domain-specific common European data spaces and between other data that are not within the scope of a specific common European data space.

# Competition vs. Regulation: the case of the DA

These goals reflect the main problem that the initiative detects, which is **the insufficient availability of data for use and reuse**. Notably, although the use of connected products increasingly generates data which in turn may be used as input by services that accompanied these products, **consumers and companies (especially start-ups, small and medium-sized enterprises - SMEs) have limited ability to realize the value of data generated by their use of products and related services, since they lack effective control over the data**.

In many sectors, manufacturers are often able to determine, through their control of the technical design of the product or related services, what data is generated and how it can be accessed, even though they have no legal right to the data. In situations where the data is generated by machines through the use of products and related services by businesses and consumers, it is indeed unclear whether the acquisition of an object includes the benefit of having a share in the value of the data. Legal uncertainties regard the question of the applicability of the Database Directive to machine-generated data and also pertain to the portability and interoperability of data. Moreover, with regards to data subjects, the **GDPR is considered insufficient to alleviate the problem of limited control over the data, because the right to data portability does not apply to non-personal data and it is confined to personal data processed for the performance of a contract or based on consent**. In a similar vein, sectoral legislations ensure that only in certain areas (e.g., electricity, banking, cars) third parties can have access to relevant data.

# Competition vs. Regulation: the case of the DA

Finally, **data sharing within and between sectors requires an interoperability framework**. Indeed, the absence of common and compatible standards for both semantic and technical interoperability represents the main barrier to data sharing and reuse, and a very relevant problem for the effective portability of data and for switchability between cloud and edge services.

In summary, alongside the general goal of empowering users to gain and exert control over their data, the **DA is also pursuing other objectives, such as safeguarding and promoting competition, innovation, and fairness in the digital economy**.

The concept of fairness is interpreted in **broad terms and refers to the allocation of economic value from data among actors**. This concern stems from the observation that data value is concentrated in the hands of relatively few large companies, while the data produced by connected products or related services are an important input for aftermarket, ancillary and other services.

Therefore, to achieve a greater balance in the distribution of such value, the fairness of both contractual terms and market outcomes are addressed. Indeed, the creation of a cross-sectoral governance framework for data access and use aims to ensure contractual fairness, namely to rebalance the negotiation power for SMEs in data sharing contracts and prevent vendor lock-in in cloud and edge services. As a result, fairer and more competitive market outcomes shall be promoted in aftermarkets and in data processing services.

# Competition vs. Regulation: the case of the DA

**Such a broad notion of fairness has also been applied in the DMA** and this may not be without legal risks. In the DMA, the unfairness is related to the inability of market participants to adequately capture the benefits resulting from their innovative efforts because of gatekeepers' gateway position and superior bargaining power. Moreover, contestability and fairness are considered intertwined, given that the lack of the former can enable a large player to engage in unfair practices and, similarly, unfair practices by a gatekeeper can reduce the possibility of rivals to contest its position. Concerns about fair dealing in online markets have also motivated the platform-to-business (P2B) Regulation, which noted that, given the increasing dependence of business users on online intermediation services, the providers of those services often have superior bargaining power which enables them to behave unilaterally in a way that can be unfair.

Università Europea di Roma

Co-funded by the Erasmus+ Programme of the European Union

# COMPETITION VS. REGULATION IN DIGITAL MARKETS

# THE CASE OF THE ARTIFICIAL INTELLIGENCE ACT («AI ACT»)

# The case of the AI Act

**On 21 April 2021, the European Commission presented the Artificial Intelligence Act.**

The draft regulation seeks to codify the high standards of the EU trustworthy AI paradigm. It sets out core horizontal rules for the development, trade and use of AI-driven products, services and systems within the territory of the EU, that apply to all industries.

The EU AI Act introduces a sophisticated 'product safety regime' constructed around a set of 4 risk categories. It imposes requirements for market entrance and certification of High-Risk AI Systems through a mandatory CE-marking procedure. This pre-market conformity regime also applies to machine learning training, testing and validation datasets.

The AI Act draft combines a risk-based approach based on the pyramid of criticality, with a modern, layered enforcement mechanism. This means that as risk increases, stricter rules apply. Applications with an unacceptable risk are banned. Fines for violation of the rules can be up to 6% of global turnover for companies.

The EC aims to prevent the rules from stifling innovation and hindering the creation of a flourishing AI ecosystem in Europe, by introducing legal sandboxes that afford breathing room to AI developers.

# The case of the AI Act

**On 21 April 2021, the European Commission presented the Artificial Intelligence Act.**

The EU AI Act sets out horizontal rules for the development, commodification and use of AI-driven products, services and systems within the territory of the EU. The draft regulation provides core artificial intelligence rules that apply to all industries.

The EU AI Act introduces a sophisticated 'product safety framework' constructed around a set of 4 risk categories. It imposes requirements for market entrance and certification of High-Risk AI Systems through a mandatory CE-marking procedure. To ensure equitable outcomes, this pre-market conformity regime also applies to machine learning training, testing and validation datasets.

The Act seeks to codify the high standards of the EU trustworthy AI paradigm, which requires AI to be legally, ethically and technically robust, while respecting democratic values, human rights and the rule of law.

# The case of the AI Act

**Objectives of the EU Artificial Intelligence Act**

The proposed regulatory framework on Artificial Intelligence has the following objectives:

1. ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values;

2. ensure legal certainty to facilitate investment and innovation in AI;

3. enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;

4. facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.

# The case of the AI Act

**Subject Matter of the EU AI Act**

The scope of the AI Act is largely determined by the subject matter to which the rules apply. In that regard, Article 1 states that:

Article 1

Subject matter

This Regulation lays down:

(a) harmonised rules for the placing on the market, the putting into service and the use of artificial intelligence systems ('AI systems') in the Union;

(a) prohibitions of certain artificial intelligence practices;

(b) specific requirements for high-risk AI systems and obligations for operators of such systems;

(c) harmonised transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content;

(d) rules on market monitoring and surveillance.

# The case of the AI Act

**Pyramid of Criticality: Risk based approach**

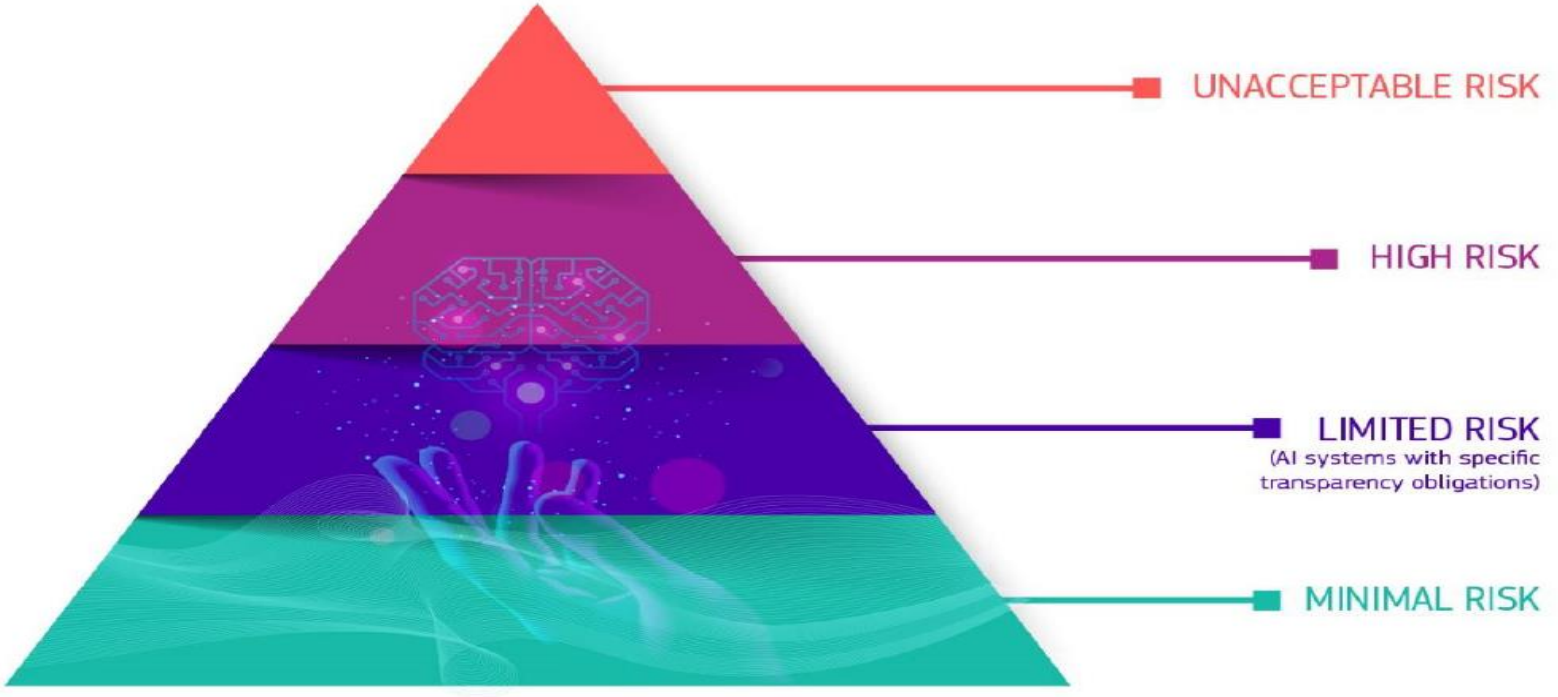
To achieve the goals outlined, the Artificial Intelligence Act draft combines a risk-based approach based on the pyramid of criticality, with a modern, layered enforcement mechanism.

This means, among other things, that a lighter legal regime applies to AI applications with a negligible risk, and that applications with an unacceptable risk are banned.

Between these extremes of the spectrum, stricter regulations apply as risk increases. These range from non-binding self-regulatory soft law impact assessments accompanied by codes of conduct, to heavy, externally audited compliance requirements throughout the life cycle of the application.

# The case of the AI Act

## Pyramid of Criticality: Risk based approach




The Pyramid of Criticality for AI Systems

# The case of the AI Act

**Unacceptable Risk AI systems**

Unacceptable Risk AI systems can be divided into 4 categories: two of these concern cognitive behavioral manipulation of persons or specific vulnerable groups. The other 2 prohibited categories are social scoring and real-time and remote biometric identification systems. There are, however, exceptions to the main rule for each category. The criterion for qualification as an Unacceptable Risk AI system is the harm requirement.

Examples of High-Risk AI-Systems

Hi-Risk AI-systems will be carefully assessed before being put on the market and throughout their lifecycle. Some examples include:

- Critical infrastructures (e.g. transport), that could put the life and health of citizens at risk
- Educational or vocational training, that may determine the access to education and professional course of someone's life (e.g. scoring of exams)
- Safety components of products (e.g. AI application in robot-assisted surgery)

# The case of the AI Act

**Unacceptable Risk AI systems**

- Employment, workers management and access to self-employment (e.g. CV sorting software for recruitment procedures)
- Essential private and public services (e.g. credit scoring denying citizens opportunity to obtain a loan)
- Law enforcement that may interfere with people's fundamental rights (e.g. evaluation of the reliability of evidence)
- Migration, asylum and border control management (e.g. verification of authenticity of travel documents)
- Administration of justice and democratic processes (e.g. applying the law to a concrete set of facts)
- Surveillance systems (e.g. biometric monitoring for law enforcement, facial recognition systems)

# The case of the AI Act

## Market Entrance of High-Risk AI-Systems: 4 Steps

- In a nutshell, these 4 steps should be followed prior to Hi-Risk AI-Systems market entrance. Note that these steps apply to components of such AI systems as well.

1. A High-Risk AI system is developed, preferably using internal ex ante AI Impact Assessments and Codes of Conduct overseen by inclusive, multidisciplinary teams.
2. The High-Risk AI system must undergo an approved conformity assessment and continuously comply with AI requirements as set forth in the EU AI Act, during its lifecycle. For certain systems an external notified body will be involved in the conformity assessment audit. This dynamic process ensures benchmarking, monitoring and validation. Moreover, in case of changes to the High-Risk AI system, step 2 has to be repeated.

3. Registration of the stand-alone Hi-Risk AI system will take place in a dedicated EU database.

4. A declaration of conformity must be signed and the Hi-Risk AI system must carry the CE marking (Conformité Européenne). Now the system is ready to enter the European markets.

# The case of the AI Act

**But this is not the end of the story...**

In the vision of the EC, after the Hi-Risk AI system haven obtained market approval, authorities on both Union and Member State level 'will be responsible for market surveillance, end users ensure monitoring and human oversight, while providers have a post-market monitoring system in place.

Providers and users will also report serious incidents and malfunctioning. In other words, continuous upstream and downstream monitoring.

Since people have the right to know if and when they are interacting with a machine's algorithm instead of a human being, the AI Act introduces specific transparency obligations for both users and providers of AI system, such as bot disclosure. Likewise, specific transparency obligations apply to automated emotion recognition systems, biometric categorization and deepfake/synthetics disclosure. Limited Risk AI Systems such as chatbots necessitate specific transparency obligations as well. The only category exempt from these transparency obligations can be found at the bottom of the pyramid of criticality: the Minimal Risk AI Systems.

In addition, natural persons should be able to oversee the Hi-Risk AI-System. This is termed the human oversight requirement.

# The case of the AI Act

## Open Norms

The definition of high-risk AI applications is not yet set in stone. Article 6 does provide classification rules. Presumably, the qualification remains a somewhat open standard within the regulation, subject to changing societal views, and to be interpreted by the courts, ultimately by the EU Court of Justice. A standard that is open in terms of content and that needs to be fleshed out in more detail under different circumstances, for example using a catalog of viewpoints. Open standards entail the risk of differences of opinion about their interpretation. If the legislator does not offer sufficient guidance, the courts will ultimately have to make a decision about the interpretation of a standard.

This can be seen as a less desirable side of regulating with open standards. A clear risk taxonomy will contribute to legal certainty and offer stakeholders with appropriate answers to questions about liability and insurance.

# The case of the AI Act

## Enforcement

The draft regulation provides for the installation of a new enforcement body at Union level: the European Artificial Intelligence Board (EAIB). At Member State level, the EAIB will be flanked by national supervisors, similar to the GDPR's oversight mechanism. Fines for violation of the rules can be up to 6% of global turnover, or 30 million euros for private entities.

'The proposed rules will be enforced through a governance system at Member States level, building on already existing structures, and a cooperation mechanism at Union level with the establishment of a European Artificial Intelligence Board.'