Bird & Bird

The impact of the DMA and DSA on payments

10th PSE Merchant Acquiring Conference

6 December 2022

Anthony Rosen

Topics

- Overview of the Digital Markets Act
- Impact of DMA on Payments
- Related Competition Cases
- Overview of the Digital Services Act
- Security requirements – DORA and NIS2

Bird & Bird

The Digital Markets Act

Digital Markets Act

Re-setting the rules of the game

Regulatory pressure

Regulatory pressure on digital platforms has reached boiling point

Competition investigations

A number of competition investigations into "Big Tech" but not seen as enough…

Call for new tools

Regulators around the globe calling for new tools to complement competition law

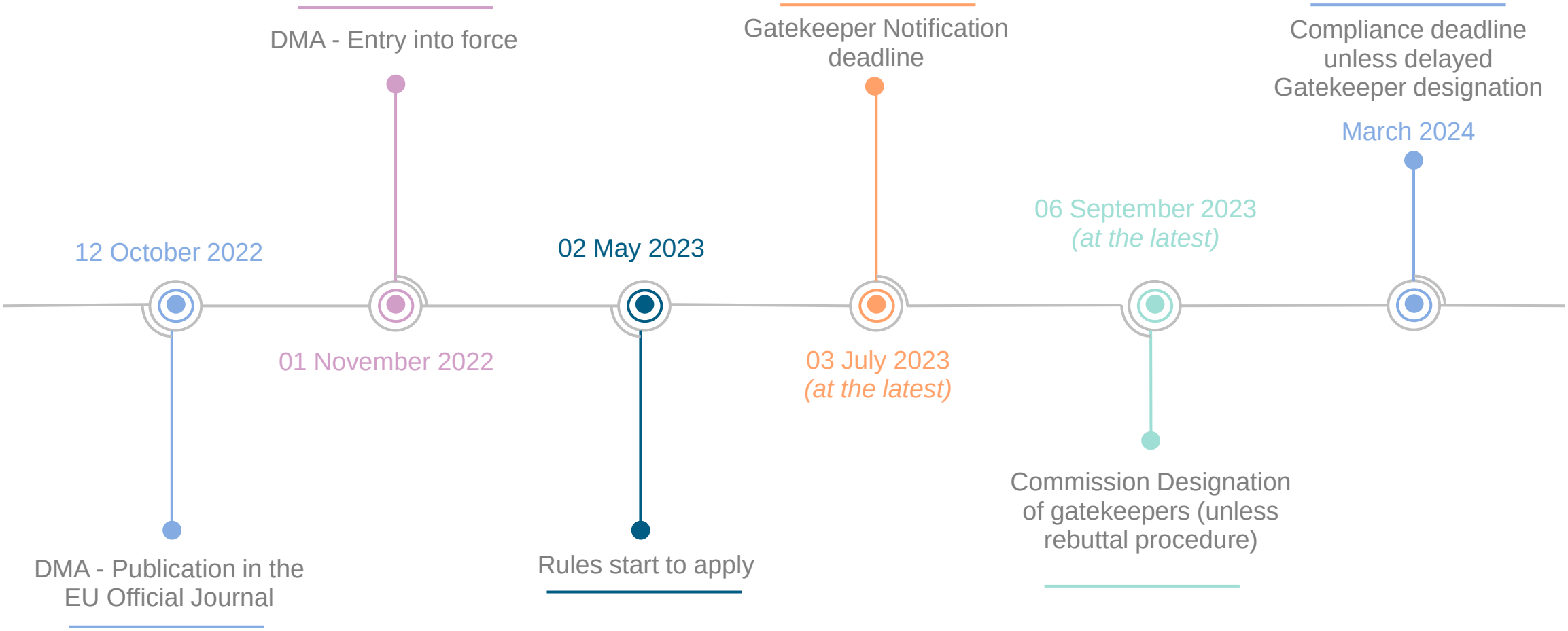
DMA

The DMA introduces new set of ex ante rules for "Gatekeeper" platforms

Other regimes

Other regimes also have new proposals - notably UK

Timeline for DMA compliance



What digital services are caught?

Core platform services

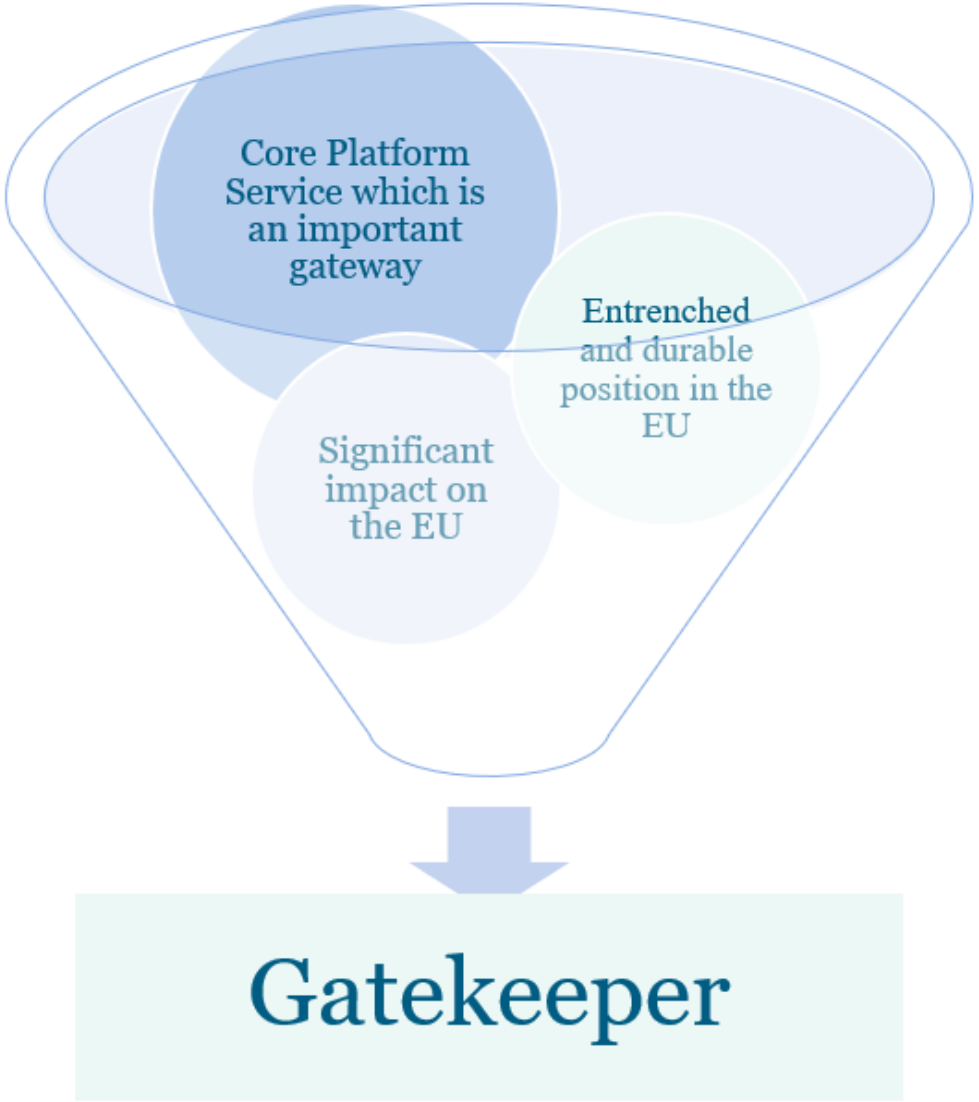
- Online intermediation services
- Online search engines
- Online social networking services
- Video-sharing platform services
- Number-independent interpersonal communication services

- Operating systems
- Web browsers
- Virtual assistants
- Cloud computing services
- Advertising services

! *Commission can add services following 18 month market investigation process*

! *Identification services, web browser engines, or technical services that support payment services if provided with a CPS, be captured indirectly by Gatekeeper obligations*

What is a 'Gatekeeper'?



Who are the Gatekeepers?

1. The undertaking has a **significant impact** on the internal market; AND — *Qualitative*

- *The above qualitative requirement (1) is met:*
  - *if the undertaking achieves an annual turnover in the EU of ≥ **€ 7.5 billion** in each of the **last three financial years**; OR*
  - *if the undertaking's average market capitalisation or its equivalent fair market value amounted to **≥ € 75 billion** in the **last financial year**; AND*
  - *it provides the same CPS in **at least three Member States**.*

Quantitative

2. The undertaking provides a CPS which is an **important gateway** for business users to reach end users; AND — *Qualitative*

- *The above qualitative requirement (2) is met if the CPS has at least:*
  - ***45 million monthly** active end users established or located in the EU; AND*
  - *At least **10.000 yearly** active business users established in the EU in the **last financial year***

Quantitative

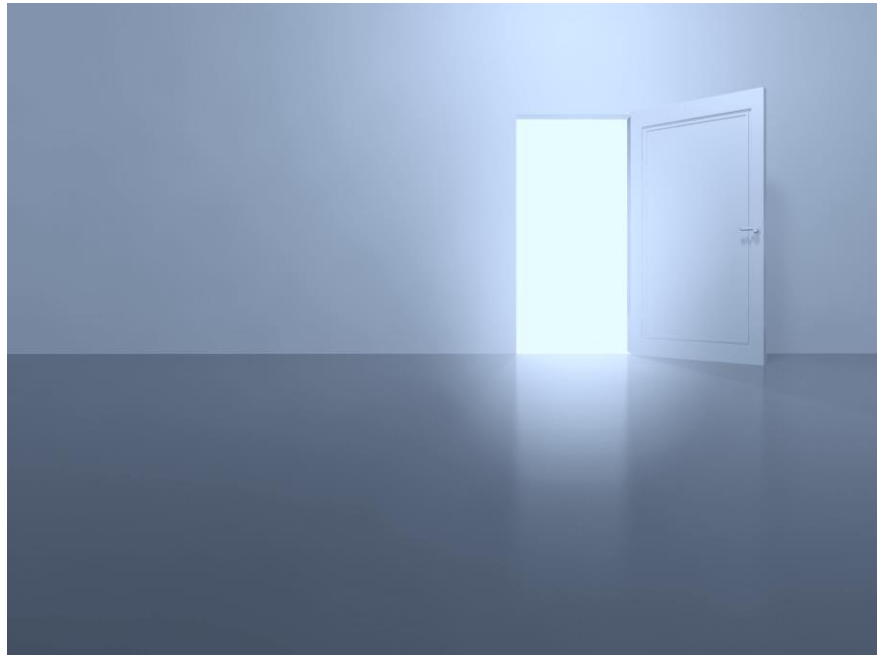
3. The undertaking enjoys an **entrenched and durable position** in its operations or it is foreseeable that it will enjoy such a position in the near future. — *Qualitative*

- *The above qualitative requirement (3) is met if the requirements under (2) are met in each of the **last three financial years**.*

Quantitative

Who are the Gatekeepers?

- The Commission can also **designate** other companies as gatekeepers based on a **qualitative assessment** following a 12 month market investigation and equally companies can try to rebut the status (based on qualitative assessment).
- The relevant qualitative assessment **criteria** include the **size and position** of the company providing the CPS, **the number of users, network effects and data driven advantages** and **scale and scope effects** the undertaking benefits from.
- Review every **3 years** (rapid change and technological innovation)



What are the rules?

*Three sets of obligations come into force within **6 months** of gatekeeper designation*

- The DMA imposes a range of obligations to ensure fair and open digital markets
- **Article 5 –** specific rules which are strict and no further guidance.
  - **Article 5(7)**: " The gatekeeper shall not require end users to use … a payment service, … such as payment systems for in-app purchase."
- **Article 6 –** more open-ended with possibility of further specification by the Commission.
- **Article 7 –** specific rules on interoperability of NI-ICS.
- The obligations under Articles 5, 6 and 7 are framed categorically.
- **No efficiency defence** – limited exemptions for public health and security

Some of the key obligations

Obligations

- Default applications and settings
- NI-ICS interoperability
- Services and hardware interoperability
- Advertising transparency
- Third-party software and side loading
- Lock-in
- Data portability and access
- FRND T&Cs

Prohibitions

- Self-preferencing
- Re-use of personal data
- Price parity
- Tying (identification, web browsers or payments)
- CPS bundling
- Switching
- Termination provisions
- Whistleblowing

DMA payments-related obligations

Recital 52: on the 'dual-role' of gatekeepers as developers and manufacturers

"a gatekeeper that is a manufacturer [has the ability to] restrict access to some functionalities in that device, **such as NFC**…which can be required for the effective provision of a service"

Article 6(7)(f): 'effective interoperability'

"The gatekeeper shall allow providers...free of charge, effective interoperability with the same hardware and software features …as are available to the gatekeeper."

Recital 43: 'freedom to choose alternative services'

"Gatekeepers should not use their position to require their…users to use any of the services provided together with core platform services" Payment services are specifically referenced.

Article 5(7): 'no requirement to use services of the gatekeeper'

"The gatekeeper shall not require end users to use… an ID service, browser engine, or payment services such as payment systems for in-app purchases…"

DG COMP investigation into Apple over access to NFC

16 June 2020: EC announced it was opening formal proceedings against Apple. 3 topics listed in the press release:

1. Near Field Communication (**NFC**) antenna
2. "*Apple's **terms, conditions** and other measures for integrating Apple Pay in merchant apps and websites on iPhones and iPads*"
3. Apple's "*alleged **refusals of access** to Apple Pay. … The investigation will also focus on alleged restrictions of access to Apple Pay for specific products of rivals on iOS and iPadOS smart mobile devices*"

On 2 May 2022, the EC announced it had issued a statement of objections (**SO**) to Apple:

> *"Today's Statement of Objections takes issue only with the **access to NFC** input by third-party developers of mobile wallets for payments in stores. It does not take issue with the online restrictions nor the alleged refusals of access to Apple Pay for specific products of rivals that the Commission announced that it had concerns when it opened the in-depth investigation into Apple's practices regarding Apple Pay on 16 June 2020.*

Germany: "Lex Apple Pay"

- Effective 1 January 2020, Germany passed legislation regulating access to the NFC antenna:
  - 'System Enterprises' (**SEs**) must grant PSPs *"appropriate access condition"* to technical infrastructures (e.g. NFC antenna) so as to enable them to provide payment/e-money services
  - In exchange, SEs may ask for an *"appropriate fee"*
  - No obligation on SEs if (1) there are justified and proven security concerns, or (2) the SE has less than 2m registered users, or (3) the SE's infrastructure is used by less than 10 PSPs

Epic v Apple – US judgment

10 September 2021 - Epic Games, Inc. v. Apple Inc., United States District Court for the Northern District of California

- Epic wanted to open its own store for Fortnite for iPhones/iPad, and to pay a 0% commission to Apple in relation to the Apple Store.
- The court found no breach of Section 1 Sherman Act, nor Section 2 Sherman Act
- However the court found that Apple violated California's Unfair Competition Law (UCL):

Remedy:

"*... a nationwide injunction shall issue enjoining Apple from prohibiting developers to include in their:*

Apps and their metadata buttons, external links, or other calls to action that ***direct customers to purchasing mechanisms, in addition to IAP.***

Nor may Apple prohibit developers from:

Communicating with customers through points of contact obtained voluntarily from customers through account registration within the app."

DG COMP and CMA investigations into Apple App Store Rules

30 April 2021: the EC sent a statement of objections (**SO**) to Apple, stating that:

"*… Apple has a **dominant position** in the market for the distribution of music streaming apps through its App Store. …*"

Two types of abuses alleged:

1. "*The **mandatory use of Apple's proprietary in-app purchase system (IAP)** for the distribution of paid digital content. Apple charges app developers a 30% commission fee on all subscriptions bought through the mandatory IAP … most streaming providers passed this fee on to end users by raising prices*"
2. "***"Anti-steering provisions"** which limit the ability of app developers to **inform users of alternative purchasing possibilities** outside of apps. While Apple allows users to use music subscriptions purchased elsewhere, its rules prevent developers from informing users about such purchasing possibilities, which are usually cheaper. …*"

CMA*: "These complaints also highlight that certain developers who offer 'in-app' features, add-ons or upgrades are **required to use Apple's payment system**, rather than an alternative system. Apple charges a **commission of up to 30%** to developers on the value of these transactions or any time a consumer buys their app."*

Dutch ACM and CMA also investigating Google Play Billing

CMA: "*The investigation concerns Google's distribution of apps on Android devices in the UK, in particular Google's Play Store rules which* ***oblige app developers offering digital content to use Google's own payment system (Google Play Billing) for in-app purchases***."

ACM*: "The [ACM] has decided to launch a preliminary investigation into a possible abuse of dominance by Google Play Store… Dating-app providers allegedly are* ***no longer able to use a payment system other than Google's payment system****… Dating apps claim they are no longer allowed to refer to other payment methods… Match Group has filed a request for enforcement with ACM, asking ACM to assess whether Google abuses its dominant position" - The EU has since opened an investigation.*

Google is taking steps to comply with the DMA and introduced new payment terms for the EEA in July and expanding to other countries (alternative billing systems and lower service fee) but limited scope of application to non-gaming apps

Compliance and enforcement

Compliance and investigative, enforcement and monitoring powers

- If an undertaking finds that it meets the Gatekeeper thresholds as set out in the DMA, it will have **two months** from when the DMA starts to notify the Commission. The Commission then has **45 working** days to designate a company as a "Gatekeeper" from receipt of the required information. Gatekeepers will then have **6 months** to comply with relevant obligations (anticipated early 2024).
- The European Commission will have **information gathering, monitoring** and **on-site inspection powers**.
- **Third parties** may **inform** the NRA/Commission about non-compliance
- Fines of **up to 20%** of world-wide turnover and periodic penalty payments of up to 5% average daily revenues
- **Commitments process**
- If systemic infringements, **additional remedies** may be imposed after market investigation (must be proportionate)
- **Break-up** and a **temporary merger ban** possible
- Possibility for **follow-on claims** for damages

UK – Strategic Market Status Regime

- **Priority digital activities** – online marketplaces, app stores, social networks, web browsers, online search, operating systems and cloud computing – not yet fixed….
- Only apply to firms with **Strategic Market Status**
- Enforced by new Digital Market Units within the CMA
- Three pillars:
  1. Enforceable code of conduct – objectives, principles and guidance
  2. Pro-competitive interventions - to address root cause of market power - data-related interventions, interoperability (such as between platforms) and common standards to open up competition and innovation
  3. SMS merger rules and mandatory reporting requirements
- New regime expected to come into law by May 2023.

What is SMS?

- Economic assessment – **substantial, entrenched market power in at least one digital activity**
  a. Substantial market power = unwilling or unable to switch to competitor
  b. Entrenched – not merely transitory
  c. No need for market definition exercise so wider discretion
  d. Assessment against **specific activity** so can be narrow rather than the entire firm

- Await guidance from DMU and prioritisation rules for SMS designation
  - Minimum revenue threshold to provide certainty
  - Open and transparent designation process
  - 5 year review period
  - SMS status apply to firm as a whole but remedies on specific designated activities

Bird & Bird

The Digital Services Act

Global benchmark for digital services

- Regulation - directly binding on 27 Member States (+ EEA)
- Principle: *'What is illegal offline is illegal online'*
- **Consumers:** less exposure to illegal content and products
- **Business users:** level playing field against providers of illegal content
- **Society at large:** reduce systemic risks, disinformation
- General monitoring still prohibited (E-Com Directive)

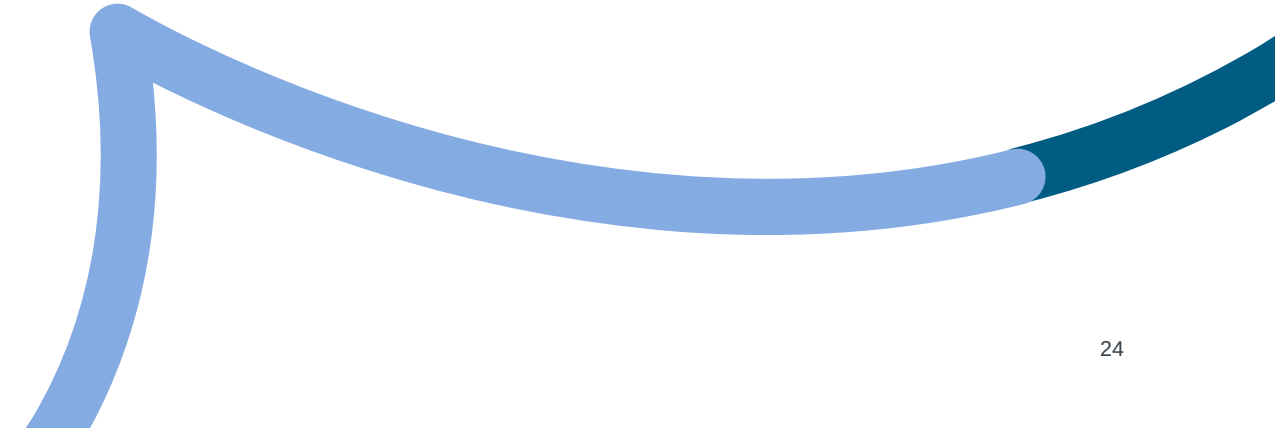
Who will be regulated?

- **Information Society Services**
- **Intermediaries**: 'mere conduit', caching, hosting services
- **Online Platforms** bringing together sellers and consumers e.g. online marketplaces, app stores, collaborative economy platforms and social media
- **Very Large Online Platforms and Very Large Online Search engines** >45 mil users
- Extra territorial effect!

"Irrespective of the place of establishment or location of the providers of those services" (Recital 7)

Legal representative *(Arts. 12 & 13)*

- A **single point of contact** allowing direct communication with authorities
- If no establishment in EU but offer services in the Union, to designate a **legal representative** in a Member State where you provide services
- Legal representative **can be held liable** for non-compliance (+ provider)



Content moderation

Transparency reporting (Arts. 15, 24, 42)

- Report orders from Member State authorities
- Notices submitted **by type of illegal content**
- Number of complaints received via internal system
- Number of suspensions
- Transparency reporting of moderation decisions

Notice-and-action mechanism

Illegal material online (Arts. 16, 17, 20, 21, 22)

- Users can notify illegal content via notice & action mechanism
- Hosting service removing access must **provide reasons**
- Internal **complaint-handling system** free of charge
- Provide for possibility of **out-of-court settlements**
- Notices from **'trusted flaggers'** to be given priority
- Flaggers should **have expertise** in identifying and notifying illegal content
- E.g. NGOs, consumer groups, industry associations, national lotteries?

Advertising transparency for VLOPs

(Arts. 26, 27, 39)

- Online providers to make clear **information displayed is an ad**
- **On whose behalf** an ad is displayed
- **Parameters used** to decide why an ad is displayed
- Main parameters used in **recommender systems**
- Targeted ads based on **sensitive data** banned (religion, ethnicity)
- **Repository of ads** to be publicly available

Oversight and penalties

(Arts. 49, 52, 86)

- **Digital Services Coordinator** per Member State
- **Country of main establishment** has jurisdiction
- **Liability** provisions enforced under national laws
- **European Board for Digital Services** to act as advisory body
- **Fines:** up to **6% global turnover** in previous year
- **Enhanced enforcement** by Commission for **VLOPs** (Arts. 73, 75)

> *"Penalties shall be effective, proportionate and dissuasive" (Art. 52)*

Next Steps

- Entry into force: 16 November 2022
- Number active users: 17 February 2023
- VLOPs/VLOSEs designation: Mid-March – Early April 2023
- Entry into application (VLOPs/VLOSEs): July 2023
- DSCs Designation/Entry into application (all services): 17 February 2024

➢ Enforcement done via DSCs
➢ Commission to enforce obligations for VLOPS/VLOSEs

Bird & Bird

The Digital Operational Resilience Act (DORA)

What is DORA?

- DORA refers to the EU Digital Operational Resilience Act. The Act is designed to strengthen the financial sector's resilience to ICT-related incidents by bringing in a set of compliance requirements to be applied across EU member states.
- DORA sets uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector as well as critical third parties which provide ICT (Information Communication Technologies) - related services to them, such as cloud platforms or data analytics services.
- DORA was adopted by the European Council on 28 November 2022. Aspects requiring national transposition will be passed into law by each EU member state.
- Applies to financial institutions including credit and payment institutions, crypto service providers, insurance intermediaries and auditors.
- The act will provide criteria, templates and instructions directing how DORA compliance obliged organisations should manage ICT and cyber risks
- At the core of DORA are five areas of focus: ICT Risk Management; ICT Supplier Risk and Vendor Management; Operational Resilience testing Incident Reporting; and Information Sharing.

Bird & Bird

Network and Information Security Directive (NIS2)

NIS2 Directive

- NIS2 was adopted by the European Council on 28 November 2022 and Member States will have 21 months to implement the new requirements.
- NIS2 creates an enhanced baseline of cybersecurity, reporting measures and institutional oversight across the EU
- Expanded scope
  - energy, transport, banking, financial market infrastructures, healthcare, drinking water, waste water, digital infrastructure (data centres, CDNs, telecoms), public administration, and space, postal services, waste management, chemicals, food processing, manufacturing, digital providers (online marketplaces, search engines, social networks).
- Trend towards mandatory deployment of certified ICT products and services
- Stronger enforcement and higher fines
- Member states can come up with additional national measures

Contacts

Anthony Rosen

Legal Director, Commercial (Telecoms and Competition)
London

anthony.rosen@twobirds.com