MAYER | BROWN

KEY FORTHCOMING EU LEGISLATION ON CYBERSECURITY, ARTIFICIAL INTELLIGENCE, DATA AND DIGITAL MARKETS

CYBERSECURITY			
	NETWORK AND INFORMATION SECURITY 2 DIRECTIVE (NIS2)	**DIGITAL OPERATIONAL RESILIENCE ACT (DORA)**	**DRAFT CYBER RESILIENCE ACT (CRA)***
WHO WILL BE IN SCOPE?	**Operators of essential and important services** across various sectors including energy, transport, banking, health, medical devices, chemicals and digital. In-scope entities in the digital sector include infrastructure providers (including cloud computing) as well as other digital providers such as online marketplaces, search engines and social networks. **Extraterritorial Application:** NIS2 applies to in-scope operators if they offer 'Essential' or 'Important' goods and services to the EU, irrespective of their place of establishment.	**Financial entities** and **FinTechs**, including credit and payment institutions, e-money institutions, crypto-asset service providers, alternative investment funds managers and insurance undertakings. Third party **providers** of critical internet and communication technology **(ICT)** services to in-scope financial entities. **Extraterritorial Application:** DORA applies to financial entities that provide services in the EU, irrespective of their place of establishment.	**Manufacturers** of **products with digital elements**, including software, IoT and hardware devices and their remote data processing solutions. Certain products that are already subject to cybersecurity requirements in sectoral legislation are outside the scope of the CRA, such as medical devices, aviation or certain connected vehicles. **Extraterritorial Application:** The CRA will apply to products with digital elements sold in the EU, irrespective of where the manufacturers are established or where the products are manufactured.
WHAT ARE THE KEY OBLIGATIONS?	NIS2 outlines **cybersecurity risk management obligations**, including supply chain due diligence and amended incident notification obligations. **Board Responsibilities:** Senior management will be responsible for **approving and overseeing** the cybersecurity framework, and can be held liable for non-compliance.	Obligations include requirements for **operational resilience**, third-party risk management (including IT outsourcing), testing of ICT tools (including threat-led penetration testing), and incident notification obligations. **Board Responsibilities:** Senior management will be responsible for **approving and overseeing** the cybersecurity framework, and can be held liable for non-compliance.	New **cybersecurity requirements**, including cybersecurity risk assessments, supply chain due diligence, security and functionality updates and vulnerability management processes.

CYBERSECURITY

	NETWORK AND INFORMATION SECURITY 2 DIRECTIVE (NIS2)	DIGITAL OPERATIONAL RESILIENCE ACT (DORA)	DRAFT CYBER RESILIENCE ACT (CRA)*
TIMELINE	EU Member States are required to implement NIS2 by **October 18, 2024**, with significant penalties for non-compliance. National implementing legislation will likely start applying on or around that date.	DORA will generally start applying by **January 17, 2025**, with significant penalties for non-compliance.	Formal adoption pending; obligations would likely apply by **2025-2026** at the earliest, with significant penalties for non-compliance.
THOUGHT LEADERSHIP	NIS2 Directive: New EU Cybersecurity Rules Now In Force. *Read more...*	Draft Technical Standards for DORA Now Available. *Read more...* EU Cyber Legislation puts emphasis on board responsibility. *Read more...*	EU Cyber Resilience Act Moves Closer to Adoption. *Read more...*

ARTIFICIAL INTELLIGENCE (AI)

	DRAFT EU AI ACT*
WHO WILL BE IN-SCOPE?	The AI Act will apply to providers, deployers, importers and distributors of certain AI systems models. The AI Act will not apply to traditional software systems that operate solely based on human-defined rules. **Extraterritorial Application:** The AI Act will apply to AI systems used in the EU or if the output produced by the AI system is intended to be used in the EU, regardless of the place of establishment of the provider or deployer.
WHAT ARE THE KEY OBLIGATIONS?	Certain AI systems will be **banned** (e.g., social scoring based on social behavior or personal characteristics; AI systems that manipulate human behavior to circumvent their free will). Systems considered **high-risk** (such as AI in civil aviation, medical devices, biometrics, management and operation of critical infrastructure, education, employment, among others) will be subject to **strict documentation, risk and quality management requirements** pertaining to **data governance, cybersecurity, testing, logging, transparency and human oversight**, among others. **General-purpose AI (GPAI) models** (i.e., models designed to produce a wide and general variety of outputs) will be subject to obligations around **transparency, risk management, incident reporting** and **cybersecurity**, among others. Transparency obligations will include producing documentation showing compliance with EU copyright law (e.g. when training the model) and disseminating detailed summaries of the content used for training.
TIMELINE	Formal adoption expected by April 2024; key obligations around GPAI models will likely start applying by **Q2 2025**, obligations for high risk AI systems likely by **Q2 2026**, with significant penalties for non-compliance.
THOUGHT LEADERSHIP	EU AI Act: European Parliament and Council Reach Agreement. *Read more...* The EU AI Act Will Transform Practices for AI Governance in the U.S. *Read more...* EU AI Act Special Update. *Read more...*

DATA AND DIGITAL MARKETS

	DIGITAL SERVICES ACT (DSA)	DIGITAL MARKETS ACT (DMA)	DATA ACT (DA)
WHO WILL BE IN SCOPE?	Digital services that act as **intermediaries** connecting consumers with goods, services and content (e.g., social networks, cloud providers, online marketplaces). The obligations under the DSA are tailored to the specific categories of intermediary services and are intended to match each category's role, size and impact in the online ecosystem. The most stringent obligations apply to so-called Very Large Online Platforms (VLOPs) and Very Large Search Engines (VLOSEs) providers reaching 45 million EU users monthly. 17 VLOPs and 2 VLOSEs have to date been designated, with appeals pending. **Extraterritorial Application**: The DSA applies to intermediaries that provide services in the EU, regardless of where they are based.	**Gatekeepers**, which provide key digital platform services such as web browsers search engines, advertising and social network services including messenger tools, app stores, social network services, and video sharing platforms. 6 gatekeepers and 22 core platform services operated by gatekeepers have now been formally designated as being within the scope of the DMA. More might follow and appeals are pending against some of these decisions. Ongoing debate as to how cloud services and AI might be brought within the scope of the DMA. **Extraterritorial Application:** The DMA applies to all platforms (gatekeepers) that have a significant impact on the European digital market, irrespective of their place of establishment.	The DA generally applies to manufacturers of **connected products** and to certain providers of **related services**. Connected products are items that obtain, generate or collect data concerning their performance, use or environment and that are able to communicate data via electronic communication. **Extraterritorial Application:** The DA applies to manufacturers of connected products sold in the EU and providers of related services, irrespective of their place of establishment.
WHAT ARE THE KEY OBLIGATIONS?	Transparency and reporting obligations as well as requirements to remove illegal content on the request of authorities. The **transparency obligations** target advertising on online platforms and in particular include transparency around **recommender systems**, including **algorithmic transparency**, and the prohibition on using **dark patterns**. **Targeted advertising** to users based on sensitive data such as race, religion, and political opinions is prohibited.	The obligations under the DMA comprise a list of significant **dos and don'ts**. Key examples include obligations to allow **interoperability** between gatekeeper and third party services; increasing **access to data** generated by use of the gatekeeper's services; strengthening **consent** requirements for use of data; and a **prohibition on treating services and products offered by the gatekeeper itself more favorably** than similar services or products offered by third parties.	Obligation to design connected products or related services in a way that the product data and related service data are easily and directly **accessible** to the user. Upon user request, product data and related service data may need to be made available to **third-parties**, subject to exceptions (e.g., trade secrets). The Data Act includes requirements regarding **smart contracts** for executing data sharing agreements.

DATA AND DIGITAL MARKETS			
	DIGITAL SERVICES ACT (DSA)	**DIGITAL MARKETS ACT (DMA)**	**DATA ACT (DA)**
	Board Responsibilities: Senior management of VLOPs and VLOSEs are responsible for **implementing, approving and overseeing** the organization's DSA compliance framework, and can be held liable for non-compliance.	Traditional competition law rules continue to apply in parallel. **Board Responsibilities:** Senior management will be responsible for defining, approving and overseeing the organization's DMA compliance framework, and can be held liable for non-compliance.	
TIMELINE	The DSA has applied to VLOPs and VLOSEs since **August 25, 2023** and to all other in-scope providers since **February 17, 2024**. The DSA sets out significant penalties for non-compliance.	The DMA will generally start applying by **March 7, 2024, when the first compliance reports need to be filed.** Significant penalties for non-compliance including potentially structural remedies.	The DA will generally start applying by **September 12, 2025**, with significant penalties for non-compliance.
THOUGHT LEADERSHIP	EU Digital Services Act's effects on Algorithmic Transparency and Accountability. *Read more...* German Authority and EU Bodies Target "Dark Patterns" in trading apps and online interfaces. *Read more...* Countdown to the Digital Services Act. *Read more...* The new EU digital regime: already in Court. *Read more...*	Regulating Digital Platforms: What's Changing in EU and UK. *Read more...* Cloud computing market: Dark Clouds Ahead or a European Silver Lining? *Read more...* DMA & DSA Judicial Review: Litigating the Implementation? *Read more...*	EU Data Act: New Rules on Data Sharing and Portability of Cloud Services now in force. *Read more...*

CONTACT US

PARTNER
ANA BRUDER
CYBERSECURITY & DATA PRIVACY, TECHNOLOGY
+49 69 7941 1778
ABRUDER@MAYERBROWN.COM

PARTNER
ULRICH WORM
IP, TECHNOLOGY, CYBERSECURITY & DATA PRIVACY
+49 69 7941 2981
UWORM@MAYERBROWN.COM

PARTNER
AYMERIC DE MONCUIT
ANTITRUST & COMPETITION, TECHNOLOGY
+32 2 551 5968
ADEMONCUIT@MAYERBROWN.COM

PARTNER
OLIVER YAROS
IP, TECHNOLOGY, CYBERSECURITY & DATA PRIVACY
+44 20 3130 3698
OYAROS@MAYERBROWN.COM

PARTNER
MARK PRINSLEY
FINANCIAL SERVICES M&A, IP & DATA MONETIZATION
+44 20 3130 3900
MPRINSLEY@MAYERBROWN.COM

COUNSEL
KONSTANTIN VON WERDER
IP, LIFE SCIENCES, TECHNOLOGY
+49 69 7941 1080
KVONWERDER@MAYERBROWN.COM

SENIOR ASSOCIATE
BENJAMIN BECK
IP, TECHNOLOGY, CYBERSECURITY & DATA PRIVACY
+49 211 86224 124
BENJAMIN.BECK@MAYERBROWN.COM

FOREIGN QUALIFIED LAWYER
LIVIA CREPALDI WOLF
CYBERSECURITY & DATA PRIVACY, TECHNOLOGY
+49 69 7941 1176
LCREPALDI@MAYERBROWN.COM

PROFESSIONAL SUPPORT LAWYER
SARAH WILKS
ANTITRUST & COMPETITION
+44 20 3130 8330
SWILKS@MAYERBROWN.COM

MAYER | BROWN

Mayer Brown is a leading international law firm positioned to represent the world's major corporations, funds, and financial institutions in their most important and complex transactions and disputes.

Please visit mayerbrown.com for comprehensive contact information for all our offices.