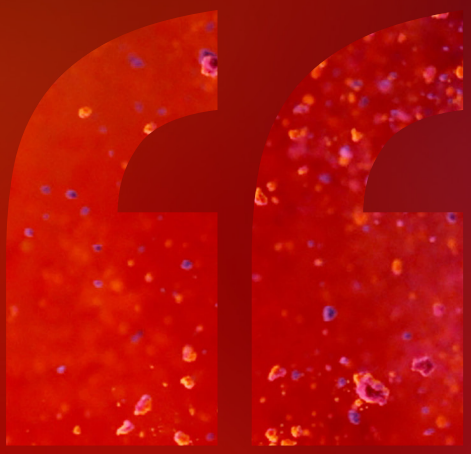
CLIFFORD
CHANCE



DIGITAL SERVICES REGULATION IN THE EU: AN EVOLVING LANDSCAPE

— THOUGHT LEADERSHIP

SEPTEMBER 2022

DIGITAL SERVICES REGULATION IN THE EU: AN EVOLVING LANDSCAPE

The regulatory landscape for digital services is being fundamentally redefined in the European Union (EU), with a boom in the number of legislative initiatives being progressively introduced and increasing extraterritorial reach. This briefing provides a bird's eye view of some of the most recent adopted and pending proposals: the Digital Services Act, the Data Governance Act, the Digital Markets Act, the Data Act, the Cybersecurity Directive (NIS2), the Artificial Intelligence Act and the e-Privacy Regulation.

Overview

The EU has made a name for itself when it comes to tech regulation and enforcement. As well as being active in enforcing existing competition, privacy and consumer protection laws, it is reviewing, proposing and adopting a range of new legislation that regulates the online environment including, notably, the activities of online service providers. As part of the European Commission's digital strategy, the EU is setting out markers for other jurisdictions to follow and defining global standards in the regulation of digital service providers. The EU's regulation of digital services harmonises or, in some cases, unifies existing disparate Member State rules or anticipates such diverging legislation, which is ultimately a benefit for businesses providing such services across the EU. However, as the new wave of legislation imposes significant new obligations while not necessarily eliminating the need to take into account the national laws of Member States, digital service providers are navigating an increasingly complex legal landscape.

Examples of EU regulation currently in force and affecting digital service providers include:

- The **various consumer protection directives** harmonising Member States' laws and significantly protecting EU consumers, including in their activities online, such as:
  - the Consumer Rights Directive (2011/83/EU), as amended by the 'Omnibus' Directive (2019/2161), which, for example, obliges EU Member States to provide in their laws a period of 14 days to withdraw from contracts for physical or digital goods concluded off premise or at a distance, including contracts concluded over the web, without giving any reason;
  - the Unfair Commercial Practices Directive (2005/29/EC), as amended by the 'Omnibus' Directive, providing specific transparency requirements for product ranking criteria and user reviews, and identifying new unfair commercial practices;[1] and
  - the Digital Content and Digital Services Directive ((EU) 2019/770) on the supply of digital services and goods to consumers, imposing conformity and liability obligations on suppliers of such services or goods;
- The raft of **directives on copyright** issued since 2014 that update EU Member States' copyright law for the online environment, such as the 2019 Digital Single Market Copyright Directive ((EU) 2019/790), which for example includes rules for the protection of news content and content used in online services such as content sharing platforms;
- The 2019 EU **Regulation on promoting fairness and transparency for business users** of online intermediation services ((EU) 2019/1150) – referred to as the "Platform-to-Business" regulation –

1 *See* Commission Notice C/2021/9320, Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market [2021] OJ C 526/1, including on these issues and on a number of other interesting questions, such as dark patterns.

which provides for extensive transparency obligations for platforms contracting with business users, for instance regarding the parameters used to determine ranking, and the extent to which platforms have access to data of business users or their customers; and

- The **2016 General Data Protection Regulation** ((EU) 2016/679) (GDPR), which applies since May 2018 and is, perhaps, the most famous example of extensive EU regulation. Applying to both online and offline activities, the GDPR has significantly impacted the activities of online service providers active in the EU through the imposition of limits on the processing and transfer of personal data and the adoption of a host of key user rights.

2022 has seen no let-up in EU legislative activity affecting digital services, with the (formal or informal) adoption of the Data Governance Act, the Digital Markets Act and the Digital Services Act – three regulations applicable directly, without the need for Member States to adopt them in their own laws – and the Member State law-harmonizing "NIS2" Cybersecurity Directive being provisionally approved, as well as the advancement of the Artificial Intelligence Act and a range of other proposals through the legislative process.

Legislative initiative	Focus area	Adoption*	Expected applicability**
Digital Services Act	Online content and intermediary services, including online platforms	Formal adoption expected Q4 2022	Early 2024
Data Governance Act	Data reuse	6/2022***	September 2023
Digital Markets Act	Gatekeeper obligations	7/2022	Early 2023
NIS2	Cybersecurity	Formal adoption by EU Parliament expected Q4 2022	Late 2024
Data Act proposal	Data use, access and portability	Expected 2023	Not before end 2023
AI Act proposal	AI systems	Not before Q4 2022/ Q1 2023	Not before end 2024
e-Privacy Regulation	Online privacy	Unknown	Unknown

* The fact that a text has been adopted does not necessarily mean that it is in force at this point. More generally, the information in this table is necessarily high-level and tentative.

** Indicates expected date for the entry into application of the majority of provisions. For some initiatives listed, some provisions may apply earlier by way of exception. For example, certain reporting obligations under the DSA are expected to apply upon entry into force.

*** Publication in the Official Journal of the EU.

The Digital Services Act (DSA)

Perhaps the most far-reaching of the recently emerging regulations for digital services is the Digital Services Act[2], due to its general applicability and the scope of obligations imposed. A political agreement on the DSA was reached in April 2022, and the European Parliament adopted it in July[3]. Its formal adoption by the Council, planned for September or October 2022, is expected to be a formality. (See our article: *The Digital Services Act – what is it and what impact will it have?*)

The DSA creates harmonised EU rules for the regulation of intermediary services and illegal online content. While it largely incorporates the liability limitations of the 2000 e-Commerce Directive for mere conduit, caching and hosting services (together termed "intermediary services" under the DSA), it elaborates the liability landscape including through requirements

2 For the initial proposal of the Commission, see Proposal of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final.

3 The version adopted by the Parliament on 5 July 2022 can be accessed **here**. A corrigendum dated 7 September 2022 can be accessed **here**.

for a more active role in content moderation. Some of the DSA's provisions apply to all intermediary services 'offered' in the EU, such as the duty to set out clear information in the terms and conditions on certain usage restrictions and in particular on the provider's content moderation policies and tools, the obligation to designate specific points of contact (and, for non-EU providers, a legal representative within the EU) and the obligation to report on content moderation activity as further described below. Other rules apply specifically to providers of "hosting services" (which include online platforms), for instance a notice and action regime for illegal content. Providers of "online platforms" are subject to yet more requirements, including a prohibition on designing, organising or operating their online interfaces in a manner that materially distorts or impairs recipients' ability to make informed decisions (so called "dark patterns"), restrictions on targeted advertising, informational requirements about the ads displayed, specific requirements concerning recommender systems including in terms of transparency on the main parameters involved and, in the case of online marketplaces, a duty to collect – and verify – information from traders to ensure traceability. Further obligations still are reserved for "very large online platforms" and "very large online search engines", with over 45 million average monthly active EU service recipients, including additional requirements concerning recommender systems and the obligation to compile and make publicly available, in a specific section of the online interface and for one year following the last display, a repository containing detailed information on advertisements displayed.

The DSA imposes considerable administrative and compliance burdens on online service providers offering intermediary services in the EU, such as: (i) the requirement for all intermediary service providers to publish regular reports on content moderation engaged in, including information on the use of automated means for content moderation, with the level of information and frequency for publication increasing according to the different types of service providers, with providers of very large online platforms and very large online search engines having to include the most information and to publish reports the most frequently; and (ii) the obligation on online platforms to regularly publish, on a publicly available section of their online interface, information on the average monthly active users of the service in the EU and to communicate related information to the authorities. The administrative and compliance burdens are even greater for very large online platforms, which must also appoint a competent compliance function reporting directly to management, conduct periodic, systemic risk assessments and adopt proportionate and effective risk mitigation measures, and subject to independent annual audits. Significant sanctions are foreseen in case of non-compliance with these obligations.

Whereas the original 2000 e-Commerce Directive sought to smooth the path for the provision of online services in the EU, the primary focus of the (soon to be formally adopted) DSA is clearly to include disciplining rules of the road to address risks and challenges of online activities that have increasingly come into focus since the turn of the millennium.

The Data Governance Act (DGA)

The Data Governance Act ((EU) 2022/868), adopted on 16 May 2022 and officially published on 3 June 2022, creates a legal framework for the reuse of protected public sector data (being confidential data, personal data or data protected by intellectual property rights) for public or commercial purposes and the voluntary sharing of data between businesses. Complementing the Open Data Directive, the DGA seeks to promote access to protected public sector data by creating harmonised conditions for its reuse and establishing a system of recognised data intermediation service providers who facilitate the exchange and use of data between data subjects, data holders and data users within the EU. The DGA, with an approach reminiscent of the GDPR, also restricts the international transfer of non-personal data originating with public sector bodies, imposing conditions and requiring appropriate safeguards (notably as regards the

protection of trade secrets and intellectual property rights) for the use of the data in the recipient jurisdiction, for example. (See our article: *An overview of the newly adopted EU Data Governance Act.*)

Although the aim of the proposal is to facilitate data reuse, the conditions imposed on the exchange of non-public data have been criticised as creating additional hurdles, with definitions that are imprecise and could allow, for example, for the blocking of transfers of valuable non-personal data to third countries.

The Digital Markets Act (DMA)

The Digital Markets Act, adopted in July 2022, is aimed at the largest consumer-facing technology companies viewed (and formally designated) as "gatekeepers" between businesses and end users (in practice, this is likely to include, among others, both Google and Apple). The DMA only affects the gatekeepers' competitors indirectly to the extent that it is aimed at establishing greater fairness and contestability in digital markets. The scope of addressees of the DMA is thus fairly narrow, but the types of "core platform services" regulated by it are fairly broad (from online intermediation services, online search engines, online social networking services and video-sharing platform services through to operating systems, browsers and virtual assistants to cloud computing services and online advertising services, each as defined in the DMA), and the obligations far-reaching. The DMA imposes, for example, new obligations for how gatekeeper platforms collect and process user and business data, how they offer online advertising services, and how they allow third-party providers on their platforms, as well as extensive additional administrative burdens, including a notification obligation for mergers and acquisitions, reporting duties and the creation of a compliance function. (See our article: *The Digital Markets Act: A new era for the digital sector in the EU.*)

Created as separate regulation existing in parallel with antitrust law and a separate body of enforcers, the DMA is aimed at addressing perceived speed and efficiency limitations of EU antitrust law by dispensing with the obligation to define markets or show anti-competitive effects, defining specific obligations at the outset, and imposing procedural deadlines on the enforcer.

NIS2 Directive

A provisional agreement among the EU institutions was reached in May 2022 for the second iteration of the Security of Network and Information Systems Directive (NIS2 Directive)[4]. Forming part of the EU Cybersecurity Strategy, the NIS 2 Directive sits alongside the EU Cybersecurity Act (which introduced a framework for cybersecurity certification of ICT products, services and processes and which has been in force since 2019) and the Cyber Resilience Act initiative (for which a proposal has been issued by the EU Commission on 15 September 2022, and which would introduce common cybersecurity rules for tangible and intangible digital products and ancillary services). The NIS2 Directive aims to provide further harmonisation of Member States' laws in the area of cybersecurity, replacing the original NIS Directive of 2016 ((EU) 2016/1148). In response to the surge in cyber-attacks and increased threats posed by digitalisation generally since 2016, the NIS2 Directive is aimed at strengthening security requirements. The draft directive would significantly extend the scope of NIS1 by adding new sectors such as telecoms and "digital providers", encompassing social media platforms and online marketplaces. The NIS2 Directive (a) lays down obligations on Member States to adopt national cybersecurity strategies, designate competent national authorities, single points of contact and computer security incident response teams (CSIRTs); (b) sets out cybersecurity risk management and reporting obligations for concerned organisations; and (c) provides obligations on cybersecurity information sharing. The NIS2 Directive provides for fines in case of non-compliance up to €10m or 2% of the total worldwide annual revenues, whichever is higher. Certain obligations apply to entities identified in the Directive as essential (including in relation to

4 For the initial proposal of the Commission, see Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM(2020) 823 final.

energy, water, health and public administration but also digital infrastructure providers such as cloud service providers and content delivery network providers), whereas other obligations apply to entities identified as important – the latter category includes online marketplaces, search engines and social networking services. Essential and important entities are subjected to the same cybersecurity management and reporting requirements, but the supervisory and penalty regimes applicable to both differ: an extensive, ex ante and ex post supervisory regime applies to essential entities, while important entities are subject to lighter ex post supervision in the event of indications of non-compliance. The NIS2 Directive is expected to be voted on by the European Parliament in Q4 2022.

The Immediate Pipeline

Further regulation with the potential to impact online services is already in the pipeline with the impending adoption of further rules on the use of data and AI.

The Data Act proposal[5], issued in February 2022, complements the DGA in seeking to ensure the flow of data. The proposed regulation has the declared objective of ensuring fairness in how the value of data is allocated among actors on different levels of the data value chain and thereby unlock the potential of the data economy. Its aims include regulating the use and access of certain types of data generated in the EU and facilitating switching between cloud and edge services providers. (See our article: *The Data Act: A proposed new framework for data access and porting within the EU*.)

The Data Act proposal requires "Internet of Things" (IoT) products and related services to be designed and manufactured such that data generated by use of the device is easily accessible by default to users (including business users), and otherwise such data must be made easily accessible by the data holder to users and, at the user's request, to third parties. Consistent with its approach to data as a non-rivalrous good, the proposal prohibits third-party data access on an exclusive basis, except when this is directly requested by the user. Moreover, when data sharing is mandated by national or EU rules, including pursuant to the Data Act itself, data holders will have to provide access on fair, reasonable and non-discriminatory terms. The Data Act proposal is linked to the DMA in that it explicitly excludes designated gatekeepers as beneficiaries of the access right to users' data generated by the use of a product. The reasoning behind this restriction is "*the unrivalled ability of these companies to acquire data*". Other aspects of the proposal apply to providers of data processing services more broadly and include restrictions on unfair terms regarding data access and use imposed on small and medium-sized enterprises. The Data Act proposal would also provide for measures aimed at facilitating customer switching and the enhancing of interoperability between cloud, edge and other related data processing services, and essential requirements regarding smart contracts. The proposed Data Act would also create requirements to share data with public bodies in exceptional circumstances and restrict certain data access by non-EEA governments to data held in the EU. The proposal is being debated at the European Parliament and the Council and is unlikely to be adopted before 2023.

The AI Act (AIA) proposal[6] seeks to regulate and provide a harmonised framework for artificial intelligence (AI) systems in the EU. Based on the initial European Commission (EC) proposal published in 2021, the AIA would ban a number of AI practices deemed particularly harmful, for instance with respect to systems that materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm. The AIA proposal would also regulate defined "high risk AI systems". (See our piece based on the Commission's initial proposal: *The Future of AI Regulation in Europe and its Global Impact*.)

5 Proposal for a Regulation of the Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) COM(2022) 68 final.

6 Proposal for a Regulation of the Parliament and of the Counsel laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) amending certain Union legislative acts, COM(2021) 206 final.

The very notion of an "AI system", the classification of high-risk AI systems, and the requirements intended to apply to them, are hotly debated issues in the context of the legislative procedure following the issuance of the EC's proposal. The EC's initial proposal defines an "AI system" as software based on techniques such as machine learning, logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems and statistical approaches, Bayesian estimation, search and optimisation methods, and "*that can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with*". Some EU Member States have made clear in the Council (which, with the Parliament, must approve the final text) that they consider this definition to be too broad, and the Czech presidency of the Council has proposed to narrow this definition by including the concept of autonomy in the definition and limiting it to machine learning techniques and knowledge-based approaches, in order to distinguish it more clearly from general software.[7]

As regards the definition of high-risk AI systems, the Commission's initial proposal classifies as "high-risk": (a) AI systems which are products or are safety components of products covered by specific sectoral legislation (such as toys or medical devices) identified in the AIA, where such products are subject to a third-party conformity assessment under that legislation; or (b) stand-alone AI systems, as listed in an annex to the proposal. The relevant annex focuses on AI usage in sensitive areas including in the EC's initial proposal of biometric identification, law enforcement, the management and operation of certain critical infrastructure, the administration of justice, and migration, as well as AI systems used in HR and recruitment or to assess the creditworthiness of individuals. The Czech presidency has suggested that the proposal be adapted to take into account the significance of the output of the AI system in relation to the decision or action taken by a human and the immediacy of the effect in classifying an AI system as "high-risk".

The Commission's initial proposal also envisages specific transparency obligations requiring providers of certain AI systems to ensure they are designed and developed in such a manner as to inform individuals that they are interacting with an AI system (such as a chatbot), unless this is obvious from the circumstances and the context of use. Other transparency obligations foreseen in the proposal include the obligation on users of digitally altered content ("deep fakes") to disclose that the content has been artificially generated or manipulated. Additional rules address, for example, the use of biometric systems or exceptions to the application of the AIA in specific contexts (such as military use). There are also measures to promote the development of AI, such as provisions for AI regulatory sandboxes to provide a controlled environment facilitating the development, testing and validation of innovative AI systems. Intense debate regarding the precise formulation of the AIA is expected to continue and adoption of a final text is not expected before late 2022 or early 2023 at the earliest.

e-Privacy Regulation proposal

Meanwhile, one significant initiative appears to have stalled in the legislative process. Proposed in 2017, the ***e-Privacy Regulation*** is particularly relevant to interpersonal communication services (such as email, messaging and VoIP services) provided to users in the EU, as well as to providers of services employing targeting and retargeting of users through the use of cookies for advertising purposes, and to other direct marketing practices. The ***e-Privacy Regulation proposal*** was aimed, among other things, at subjecting new means of (internet-based) communication to privacy rules previously exclusively applicable to telecommunications services, and to update the conditions under which tracking technologies such as cookies can be used (see our article: *E-Privacy check-in: where we are and where we're headed*). For years there was

7 Czech presidency compromise text of 15 July 2022 can be accessed **here**.

disagreement among the Member States over the proposal's rules on companies' use of metadata, the requirement for user consent for tracking cookies, and data retention for law enforcement purposes. Following extensive discussions, the Member States finally agreed on a compromise text in February 2021. However, the agreed text faces objections from the European Parliament and is significantly different from that institution's own text, which it adopted back in 2017. Efforts to reach a compromise position on the text do not appear to be a priority at this time, making it unlikely that the new e-Privacy rules will become applicable any time soon.

Looking Ahead

Not all of the new EU rules highlighted create a significant additional regulatory burden on most online service providers (save for perhaps the largest ones). Nonetheless, to varying degrees they will have an impact, imposing increased vigilance, governance and administrative requirements to ensure regulatory compliance. Even the DMA, although aimed at large gatekeeper platforms, creates a parallel system of EC investigatory powers that will no doubt multiply the generally burdensome requests for information sent to large numbers of market participants. The EC's drive to propose legislation is, by the nature of the institution (which exists to a significant degree for that very purpose), hardly over. Further areas of EU regulation expected in the future affecting online services are likely to include (instant) online payments, online digital identification, political advertising and blockchain technologies.

AUTHORS

Dieter Paemen
Partner
Brussels
T: +32 2 533 5012
E: dieter.paemen@cliffordchance.com

Dessislava Savova
Partner
Paris
T: +33 1 4405 5483
E: dessislava.savova@cliffordchance.com

Maarten Kennis
Lawyer
Brussels
T: +32 2 533 5957
E: maarten.kennis@cliffordchance.com

Alexander Kennedy
Counsel
Paris
T: +33 1 4405 5184
E: alexander.kennedy@cliffordchance.com

Rita Flakoll
Senior Associate
Knowledge Lawyer
London
T: +44 207006 1826
E: rita.flakoll@cliffordchance.com

CONTACTS

Thomas Voland
Partner
Düsseldorf
T: +49 211 4355 5642
E: thomas.voland@cliffordchance.com

Jaime Almenar
Partner
Madrid
T: +34 91 590 4148
E: jaime.almenar@cliffordchance.com

Jonathan Kewley
Partner
London
T: +44 207006 3629
E: jonathan.kewley@cliffordchance.com

Katrin Schallenberg
Partner
Paris / Brussels
T: +33 1 4405 2457
E: katrin.schallenberg@cliffordchance.com

Gunnar Sachs
Partner
Düsseldorf
T: +49 211 4355 5460
E: gunnar.sachs@cliffordchance.com

Simon Persoff
Partner
London
T: +44 207006 3060
E: simon.persoff@cliffordchance.com

Dr. Michael Dietrich
Partner
Düsseldorf
T: +49 211 4355 5542
E: michael.dietrich@cliffordchance.com

Kate Scott
Partner
London
T: +44 207006 4442
E: kate.scott@cliffordchance.com

Gail Orton
Head of EU Public Policy
Paris / Brussels
T: +33 1 4405 2429
E: gail.orton@cliffordchance.com

Susanne Werry
Counsel
Frankfurt
T: +49 69 7199 1291
E: susanne.werry@cliffordchance.com

Grégory Sroussi
Counsel
Paris
T: +33 1 4405 5248
E: gregory.sroussi@cliffordchance.com

Jaap Tempelman
Senior counsel and co-head of Tech Group
Amsterdam
T: +31 20 711 9192
E: jaap.tempelman@cliffordchance.com

Andrea Tuninetti Ferrari
Counsel
Milan
T: +39 02 8063 4435
E: andrea.tuninettiferrari@cliffordchance.com

Andrei Mikes
Senior Associate
Amsterdam
T: +31 20 711 9507
E: andrei.mikes@cliffordchance.com

Stavroula Vryna
Senior Associate
London
T: +44 207006 4106
E: stavroula.vryna@cliffordchance.com

Arnav Joshi
Senior Associate
London
T: +44 207006 1303
E: arnav.joshi@cliffordchance.com

Kelly Cannon
Avocat
Paris
T: +33 1 4405 5350
E: kelly.cannon@cliffordchance.com

Bram Van der Beken
Lawyer
Brussels
T: +32 2 533 5075
E: bram.vanderbeken@cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

2209-002518