CMS
law·tax·future

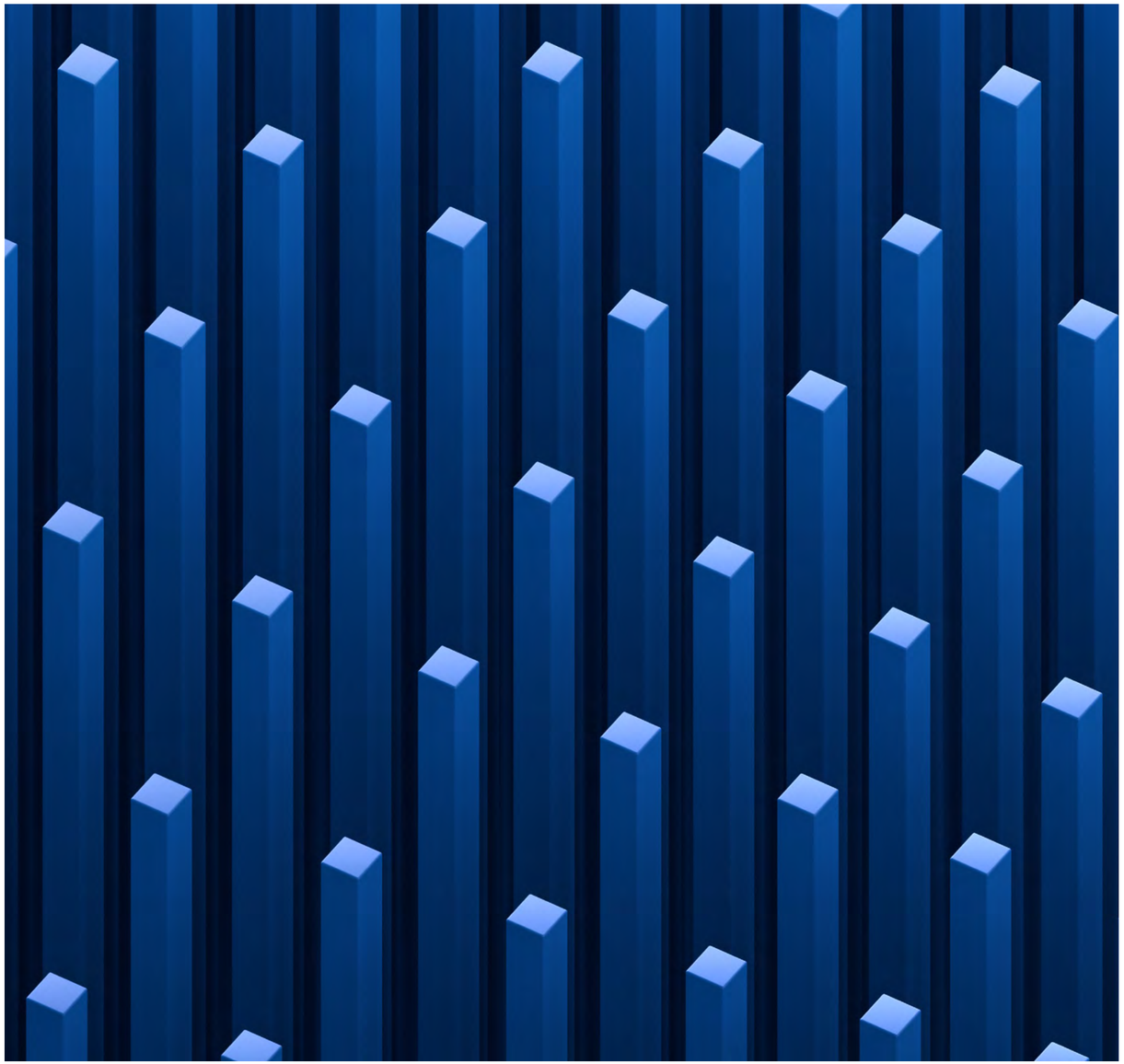
Digital Horizons

A series of reports exploring CEE's digital future

Digital regulation: a deeper dive into the DNA of the DMA and DSA

2022

Introduction



In keeping pace with the scope and scale of technology that affects its 450 million citizens, the European Union is at the forefront of implementing robust digital regulation.

Primarily, this is directed towards protecting consumers, ensuring fair competition and supporting innovation. In fulfilling these criteria, the Digital Services Package, consisting of the Digital Services Act (DSA) and the Digital Markets Act (DMA), was conceived in 2020 to regulate the digital space.

Together, these two Acts comprise a single set of new rules that will apply throughout the EU that are designed to create a safer and more open digital environment that protects users and establishes a level playing field for businesses.

Regulating everything from straightforward websites to internet infrastructure and online platforms, their stated objective is to foster innovation, growth and competitiveness, both in the European Single Market and globally.

By upgrading the current rules that govern digital services in the EU, they will also protect online users, establish governance with the protection of fundamental rights, and maintain a fair and open online platform environment across EU member states.

But despite sitting under the same digital umbrella, the DMA and DSA have distinctly different regulatory objectives: the DMA is intended to focus on the operation of digital platforms, while the DSA's broader scope creates obligations for digital services which act as intermediaries by connecting consumers with goods, services, and content.

Whereas the DMA is designed to ensure fairer digital markets by encouraging fair competition between digital suppliers, the DSA's focus is to ensure online safety and transparency for digital consumers. Both require significant attention from digital actors operating in the EU's tech space.

Digital Markets Act

The Digital Markets Act has two overriding objectives: ***"to ensure contestability and fairness for the markets in the digital sector in general"***. To address concerns about contestability and fairness, the DMA introduces assorted prohibitions and obligations on big tech companies that are designed to influence their commercial behaviour. ***"The purpose of the DMA is to prevent the distortion of competition,"*** says Marton Domokos, senior counsel at CMS.

Signed into law by the European Parliament and the Council of the EU in September 2022, it entered into force on 1 November 2022 and will become applicable on 2 May 2023.

The DMA only applies to companies that are designated as gatekeepers. According to objective criteria set out in the Act, these are big tech companies and major digital service providers: platforms that have a significant impact on the EU's internal market, serve as an important gateway for businesses to reach their end users, and which enjoy ***"an entrenched and durable position."***

Under the DMA, gatekeepers are prohibited from certain activities, such as ranking their products ahead of competitors, pre-installing apps or software, and forcing consumers to use their other services. In the case of non-compliance, significant sanctions can be imposed by the European Commission (EC): fines of up to 10 per cent of a gatekeeper's worldwide turnover, and 20 per cent for repeat infringements.

"The potential fines will get attract companies' attention, especially when they are linked to turnover. No matter how small a violation, the fine could be immense when you have billions of euros of turnover."

Olga Belyakova
Partner, co-Head of TMT in CEE, CMS

"The purpose of the DMA is to prevent the distortion of competition,"

Marton Domokos
Senior Counsel at CMS

Gatekeepers

Gatekeepers are defined by the DMA as providers of core platform services (CPS) in digital markets – a status that the EC will ultimately determine. By virtue of the thresholds being applied, only the very largest tech companies will meet the relevant criteria.

The definition of a CPS includes everything from online intermediation services, online search engines and online social networking services to video-sharing platform services, number-independent interpersonal communications services; operating systems, web browsers, virtual assistants, cloud computing services and online advertising services provided with any of the aforementioned.

Three qualitative criteria must apply for a company to be considered as a gatekeeper for which there are corresponding quantitative thresholds:

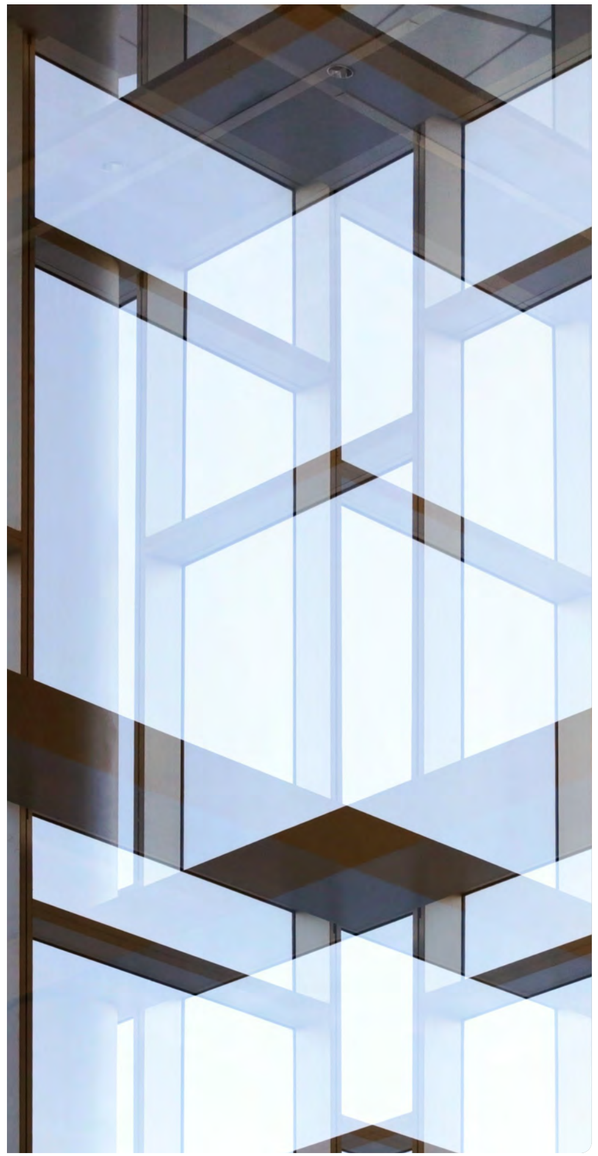
— It must have a ***"significant impact"*** on the EU market. In practice, this means an EU turnover of €7.5 billion or above during the last three financial years; or an average market capitalisation (or equivalent fair market value) of at least €75 billion in the most recent financial year. It must also provide the same CPS in at least three EU Member States.

— Its CPS must be an ***"important gateway"*** between businesses and end users in the EU. This is judged to be 45 million monthly active end-users (representing 10% of the population of the EU) or 10,000 active business users, located or established in the EU.

— It must already have, or is soon likely to have, ***"an entrenched and durable position"***, which is presumed to apply if the above user number thresholds were met in each of the last three financial years.

After the DMA begins to apply in May 2023, those CPS providers that meet these thresholds will have to submit notifications to the EC within two months. ***"At present, the assumption is that we're going to have 15 to 20 companies within the DMA's scope - not only the big US tech giants, it's also going to affect European companies,"*** says CMS competition partner Björn Herbers. Once designated as gatekeepers by the EC, they will then have six months to begin complying with the DMA obligations, summarised below, which is likely to be in March 2024.

Obligations and prohibitions



Under the DMA, the wide-ranging set of obligations and prohibitions relating to each CPS will have a significant impact on how they will be required to manage their products and services. To a considerable extent, these reflect the decisions of recent competition law infringement cases.

Compliance with these obligations and prohibitions will invariably affect multiple aspects of what gatekeepers do: restricting how they can deploy user data, requiring them to make messenger services concerning basic functionalities interoperable with third parties, and obliging them to provide information to advertisers and publishers.

The DMA provides two distinct categories of obligation and prohibition for gatekeepers. Under the first category, they can comply without the EC having to provide any more information. Under the second category, defined as those "susceptible to be further specified", the EC can provide judgment on whether a gatekeeper's proposed method of meeting an obligation will suffice, or if it needs to be enhanced.

The first category includes:

- **Use of personal data:** not processing for online advertising purposes the personal data of end-users (without their consent) of third-party services supplied through the gatekeeper's platform;
- **Use of business data:** not combining or cross-using end-users' personal data (without their consent) across or between CPS and other services or sign-in end-users to other services to combine personal data;
- **Most-Favoured-Nation (MFN) clauses:** not imposing either 'wide' or 'narrow' parity, the DMA prohibits wide and narrow (MFN) clauses - restricting business users from offering lower prices and better conditions on any other online or their own sales channels.
- **Interoperability:** gatekeepers must allow services and hardware providers with interoperability with hardware and software features accessed or controlled via its operating system or virtual assistant, and ensure interoperability for number-independent interpersonal communications services to its designated service.

Business users will be allowed, free of charge, to communicate and promote their products and services to end users acquired via the gatekeeper's CPS (or other channels) and to agree contracts with those end-users. Via the gatekeeper's CPS, end-users will be allowed to access and use content, subscriptions, features or other items by using the software application of a business user, including those acquired outside of the gatekeeper's CPS.

Gatekeepers will also have to provide (on request and free of charge) a list of advertisers and publishers to which they supply online advertising services daily information concerning the price and fees paid by the advertiser and publisher, the remuneration paid to the publisher, and how these figures are calculated.

Notable among the more far-reaching obligations in the second category are those that will allow users to download apps from the Internet and third-party app stores and enable developers to use their chosen in-app payment solution and promote offers to app users, and the requirement to offer access to the app store on fair, reasonable and non-discriminatory (FRAND) terms.

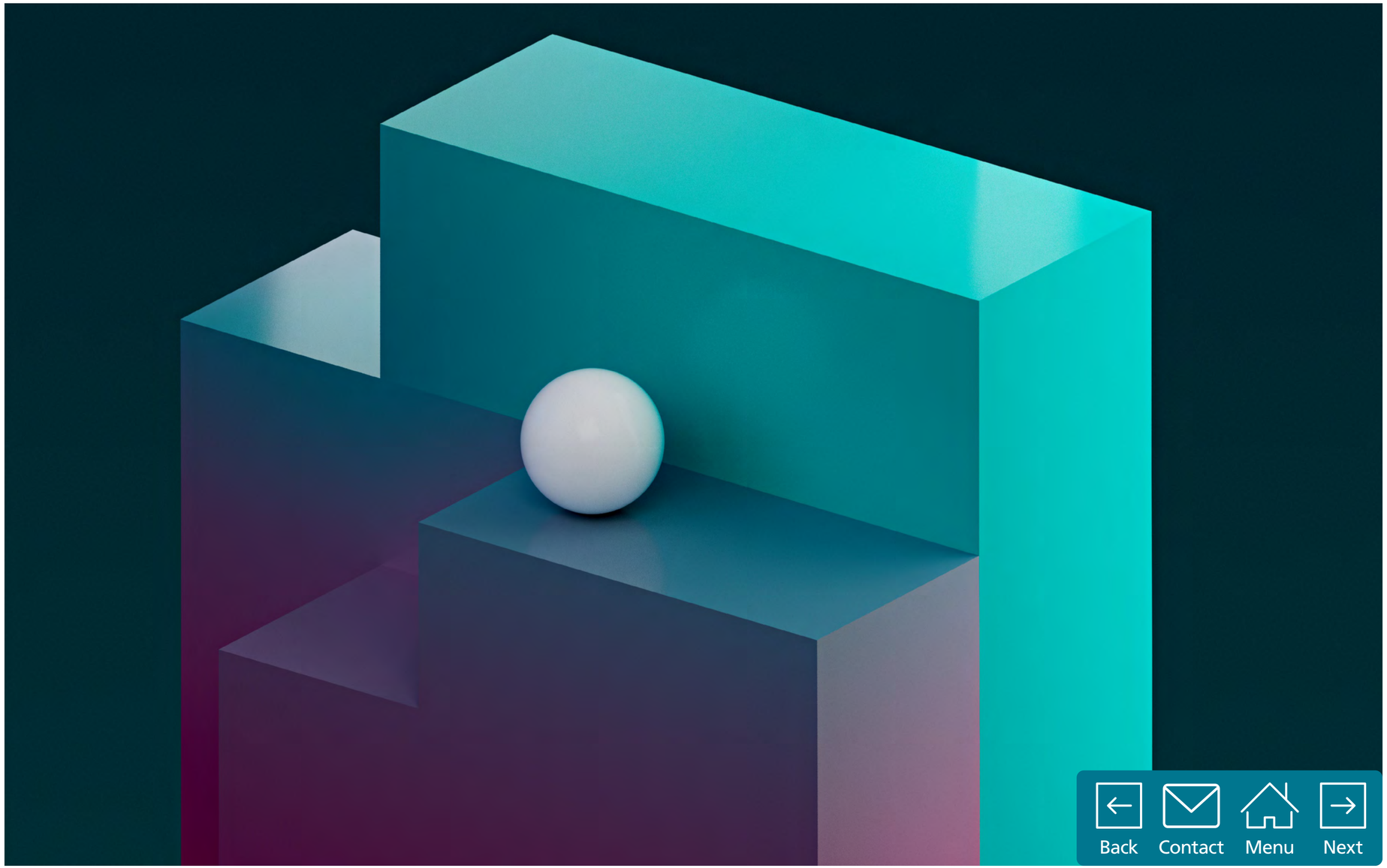
DMA Impact

Compliance with the DMA will compel big tech companies to make changes to their business model. Some have already begun the process. Gatekeepers will have to report measures that they have implemented to the EC, ensuring compliance with the DMA's obligations and establishing a compliance function that is independent from their operational functions.

The EC plans to adopt an implementing regulation in Q1 2023 that will deliver greater clarity on the DMA's requirements and procedural aspects, including the notifications of gatekeeper status and measures that should be adopted by gatekeepers to ensure compliance with obligations.

In common with the response to the GDPR, which became effective in May 2018, the DMA may lead to changes in how big tech platforms serve customers beyond the EU since some aspects of compliance are more easily implemented on a global basis. Equally, given its potential impact on the operation of designated gatekeepers, it is anticipated that some aspects of the DMA may become subject to legal challenges.

Either way, the DMA marks a very significant regulatory step by the EU and a major hurdle to overcome for big tech companies that are designated by the EC as gatekeepers.



Digital Services Act

"The DSA's overarching principle is consumer protection. Whenever you read something in the DSA, you always have to bear in mind: this is meant to protect consumers. The DSA's rules should therefore be interpreted in a way that is consumer friendly."

Dóra Petrányi
CEE Managing Director, Global Co-Head of the Technology, Media and Communications Group (TMC), CMS

Described by some commentators as the EU's new digital constitution, the Digital Services Act (DSA) is the second strand of the EU's Digital Services Package. ***"The DSA's overarching principle is consumer protection. Whenever you read something in the DSA, you always have to bear in mind: this is meant to protect consumers. The DSA's rules should therefore be interpreted in a way that is consumer friendly."*** says Dora Petranyi, Global Co-Head of the TMC group at CMS.

Sitting alongside its sister regulation the DMA, the DSA outlines the responsibilities of intermediary service providers (ISPs) that provide access to goods, services and content. The DSA will ***"harmonise the rules that apply in the online digital world within the EU, and possibly impact beyond the EU's borders,"*** says Arne Schmieke, senior associate at CMS. ***"So, for any operator located outside, but who offers its services or goods for consumers within the EU, they will also have to respect the rules."***

The DSA builds upon the existing e-Commerce Directive that was first adopted in 2000, ensuring greater accountability in how online ISPs operating in the EU moderate content, advertise, and utilise algorithmic processes. In doing so, it aims to create clear, harmonised rules for digital services, addressing illegal and harmful online content, while protecting digital innovation and free expression. ***"Under the DSA, the Internal Market will work in a unique and unified way, because up until now Member States have interpreted the e-Commerce Directive in very different ways,"*** says Katalin Horváth, senior counsel at CMS.

The DSA was published in the Official Journal of the EU on 27 October 2022 and entered into force on 17 November (20 days after publication). Most of its provisions will take effect in February 2024. It applies to digital services providers, including those based outside the EU which offer services to users in EU member states. In this extra-territorial scope, ISPs that are not established in the EU will have to appoint a designated legal representative in the EU who can be held liable for non-compliance with DSA obligations.

Although most companies will have until 17 February 2024, the biggest companies will have to act sooner. Very large online platforms (VLOPs) and very large online search engines (VLOSEs) will have to comply with their obligations four months after their designation by the EC. This will be determined by the number of users reported by VLOPs and VLOSEs - information they will have to provide to the EC by February 2023. At that point, the enforcement process will start to be implemented.

Digital Services Act

Categories

The DSA outlines basic obligations that will apply to all online ISPs, while the most burdensome will apply to the biggest companies. Four categories are defined:

CATEGORY 1	ISPs: online services that are either a "mere conduit" service, a "caching" service, or a "hosting" service. This would include online search engines, wireless local area networks, cloud infrastructure services, and content delivery networks.
CATEGORY 2	Hosting services: ISPs which store information at the service user's request, such as cloud services and services that enable sharing information and content online, including file storage and sharing.
CATEGORY 3	Online Platforms: hosting services that disseminate information which they store to the public at the user's request. Examples include social media platforms, app stores, message boards, online forums and marketplaces, metaverse platforms, as well as travel and accommodation platforms.
CATEGORY 4	VLOPs and VLOSEs that have more than 45 million active monthly users in the EU.

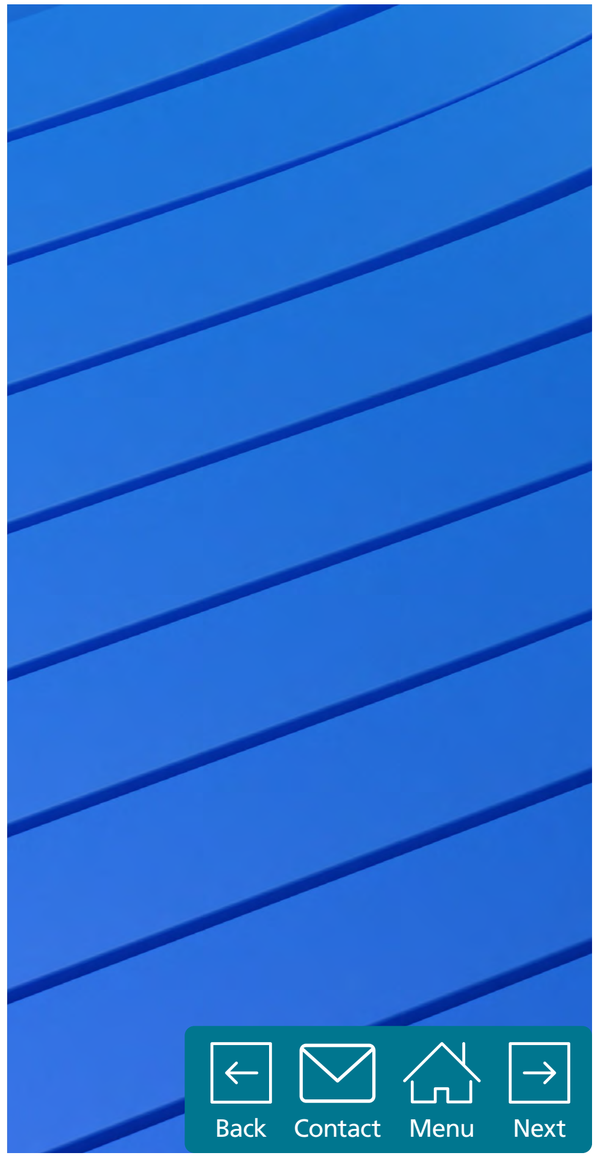
Obligations

Under the DSA, the exact range of obligations applying to individual ISPs will depend on the category that applies to each of them.

Some compliance obligations apply to all ISPs:

Transparency Reporting	they must publish annual transparency reports on their content moderation activities. This should include measures taken to apply and enforce their terms and conditions.
Terms and Conditions:	T&Cs relating to content moderation practices must be clear and provide easily accessible information on the right to terminate the use of their services.
Official Orders:	on receipt of an order either to act against illegal content or to provide information, they must inform the relevant supervisory authority of any follow up, specifying if and when they did so.
Single Point of Contact:	they must designate a single electronic point of contact for official communication with EU supervisory authorities and recipients of their services.

Obligations for ISPs in Categories 2-4:	
Notice & Action Mechanisms:	they must implement these mechanisms for content that users consider to be illegal. Content that targets victims of cyber violence must be removed "immediately", while other content deemed illegal must be removed "swiftly".
Statement of Reasons:	they must provide users with a statement of reasons whenever they delete or block access to their content for moderation purposes, when they restrict payments, or suspend or terminate their own service or the user's account.
Reporting Criminal Offences:	they must notify national law enforcement or judicial authorities if they suspect any serious criminal offences may have been committed.



Digital Services Act

Obligations for ISPs in Categories 3-4:	
Complaint & Redress Mechanism:	Users have new rights of redress - a right to complain to the platform, seek out-of-court settlements, complain to their national authority in their own language, or seek compensation for any damage or loss suffered due to an infringement of the DSA.
Trusted Flaggers:	Platforms must cooperate with designated 'trusted flaggers' to identify and remove illegal content, which includes any information that in itself or in relation to an activity, is not compliant with EU or Member State law.
Bans on Targeted Advertising:	Targeted advertising is significantly curtailed. This includes a ban on targeted advertising to children and those based on special categories of personal data - ethnicity; political views; sexual orientation; religion, or genetic or biometric data.
Advertising Transparency:	This includes a requirement to include meaningful information on why a user was targeted with a particular advertisement.
Recommender Systems:	ISPs that use recommender systems must outline in their T&Cs the main parameters that determine how they suggest or prioritise information, and any options for users to modify or influence these parameters.
Protection of Minors:	ISPs must implement "appropriate and proportionate measures" to ensure a high level of privacy, safety, and security of minors.
Interface Design:	A ban on Dark Patterns - designs that manipulate users into making choices they did not intend. This extends to targeted advertising that nudges users to purchase certain goods, or in recommender systems which use cognitive traits to present content designed to keep users on a platform for as long as possible.
Traceability of Traders:	If ISPs enable consumers to conclude contracts with traders (online marketplaces), they must ensure their traceability by collecting and assessing the veracity of basic trader information. If the platform becomes aware of an illegal product or service being offered, it must inform affected consumers.

"The DSA will harmonise the rules that apply in the online digital world within the EU, and possibly impact beyond the EU's borders. For any operator located outside, but who offers its services or goods for consumers within the EU, they will also have to respect the rules."

Arne Schmieke
Senior Associate at CMS

Digital Services Act

"Under the DSA, the Internal Market will work in a unique and unified way, because up until now Member States have interpreted the e-Commerce Directive in very different ways"

Katalin Horváth
Senior Counsel at CMS

VLOPs and VLOSEs

The strictest rules apply for VLOPs and VLOSEs. Their additional obligations include:

Audits:	They will be subject to enhanced transparency obligations, including paying for annual independent audits to assess their compliance with DSA obligations.
Annual Risk Assessments:	these must be undertaken and risk mitigation measures implemented regarding any systemic risks, including the dissemination of illegal content and negative effects on fundamental rights.
Compliance function:	they must establish an independent internal compliance function that reports directly to the board, comprised of suitably qualified professionals who are adequately trained. This is comparable to the Data Protection Officer role under the GDPR.
Data access & scrutiny:	they must provide regulators with access to any necessary data for assessing their DSA compliance. At the regulator's request, they must also provide vetted researchers with access to certain data to understand how online risks evolve.
Additional advertising transparency	they must provide a repository, where recipients can access information on online advertising displayed within the last year. This includes the content of the online advertisement, its principal, period and target groups - a potentially significant challenge to the protection of trade secrets.
Crisis Response Cooperation:	they must implement a crisis response mechanism and follow EC directions concerning specific actions on content during social and political emergencies.
Recommender systems:	VLOPs must provide users with at least one recommender system option that is not based on profiling.

Enforcement

Each Member State will designate a Digital Services Co-ordinator (DSC) to ensure supervision and enforcement of the DSA. Under the DSA, a new European oversight and advisory entity, the European Board for Digital Services (EBDS), will be comprised of national DSCs. The EBDS will be chaired by the EC, which has exclusive powers to supervise and enforce obligations that only apply to VLOPs.

Preparing for the DSA and DMA

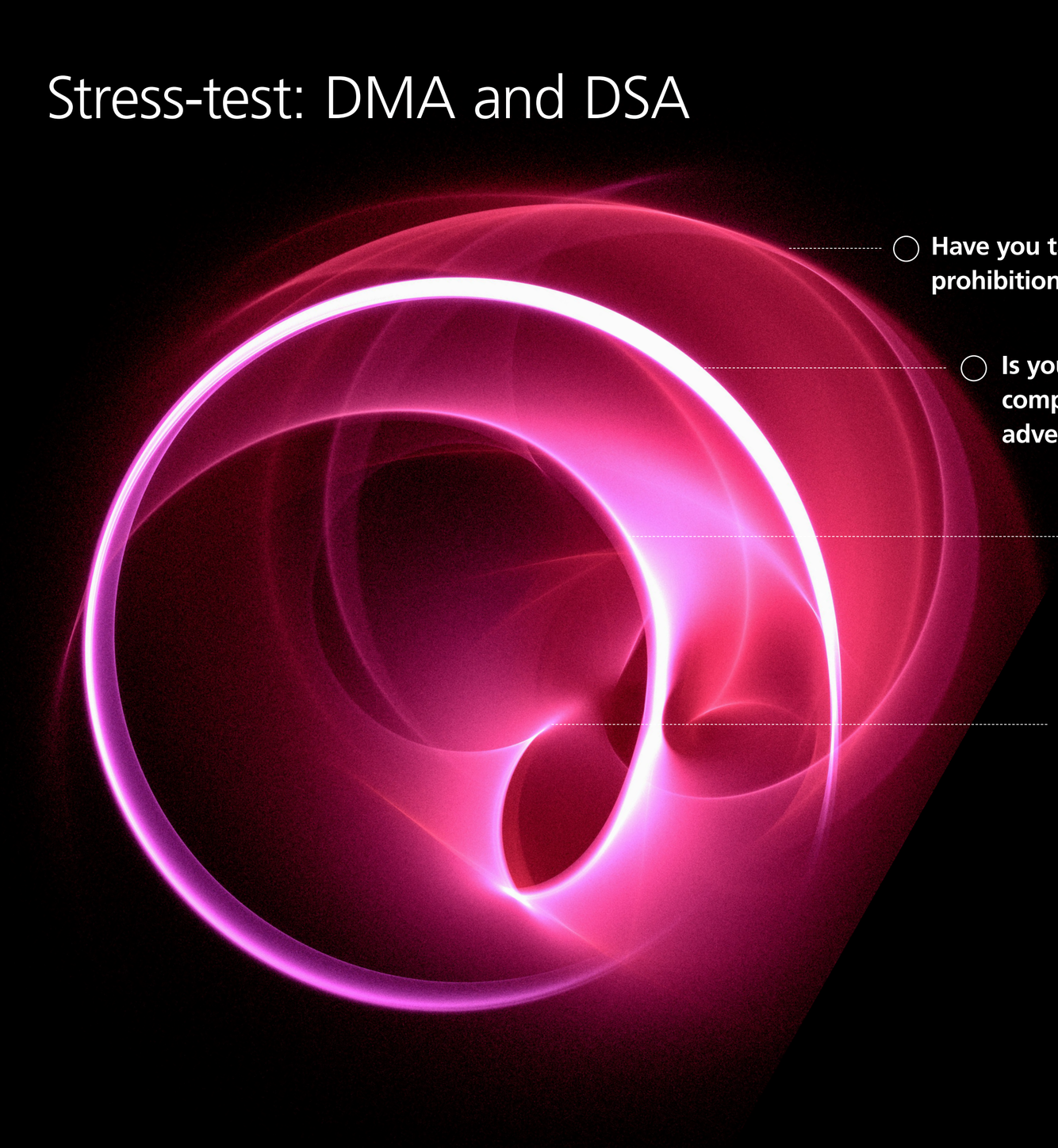
Businesses whose services may be broadly defined as ISPs should assess their services against the DSA and DMA definitions and comply with obligations concerning the designation of points of contact, legal representatives and compliance officers. More broadly, a strategic review of governance processes, documents, tools and interfaces should be undertaken in relation to the DSA and DMA obligations relating to content, format and accessibility, as well as new requirements for notification tools for illegal content and content moderation decisions, for example.

Assorted technical issues, such as dark patterns, also have specific new requirements. ***"Companies must be able to document that they have taken care to avoid dark patterns in the development phase - this is the general principle,"*** says Domokos.

Preparing for such new requirements will require significant effort and investment, underpinned by technical and legal capability at every stage.

The research and writing of this report was conducted in collaboration with Dominic Carman, journalist and writer.

Stress-test: DMA and DSA



- Have you taken all necessary steps to comply with obligations and prohibitions outlined by the EU’s Digital Services package?
- Is your team aware of the impact of the Digital Services Act affecting your company’s online advertising? Did you think about changes to your current advertising policies?
- Will increased enforcement against dark patterns lead to significant changes in your platform design?
- In response to the Digital Markets Act, how do you anticipate increasing innovation and the quality of your online services?

Talk through your digital strategy with us

If you would like to consult on or stress-test your business' digital strategy with your local CMS experts, please do get in touch with us.

CEE

Dóra Petrányi
Partner, CEE Managing Director,
Global Co-Head of the TMC, CMS
T +36 1 483 4820
E dora.petranyi@cms-cmno.com

Olga Belyakova
Partner, Co-Head of CEE TMT
T +380 44 391 7727
E olga.belyakova@cms-cmno.com

Eva Talmacsi
Partner, Co-Head of CEE TMT
T +44 20 7367 2435
E eva.talmacsi@cms-cmno.com

Bulgaria

Assen Georgiev
Partner
T +359 2 921 9936
E assen.georgiev@cms-cmno.com

Czech Republic

Tomáš Matejovský
Partner
T +420 296 798 852
E tomas.matejovsky@cms-cmno.com

Hungary

Dóra Petrányi
Partner
T +36 1 483 4820
E dora.petranyi@cms-cmno.com

Poland

Tomasz Koryzma
Partner
T +48 22 520 8479
E tomasz.koryzma@cms-cmno.com

Romania

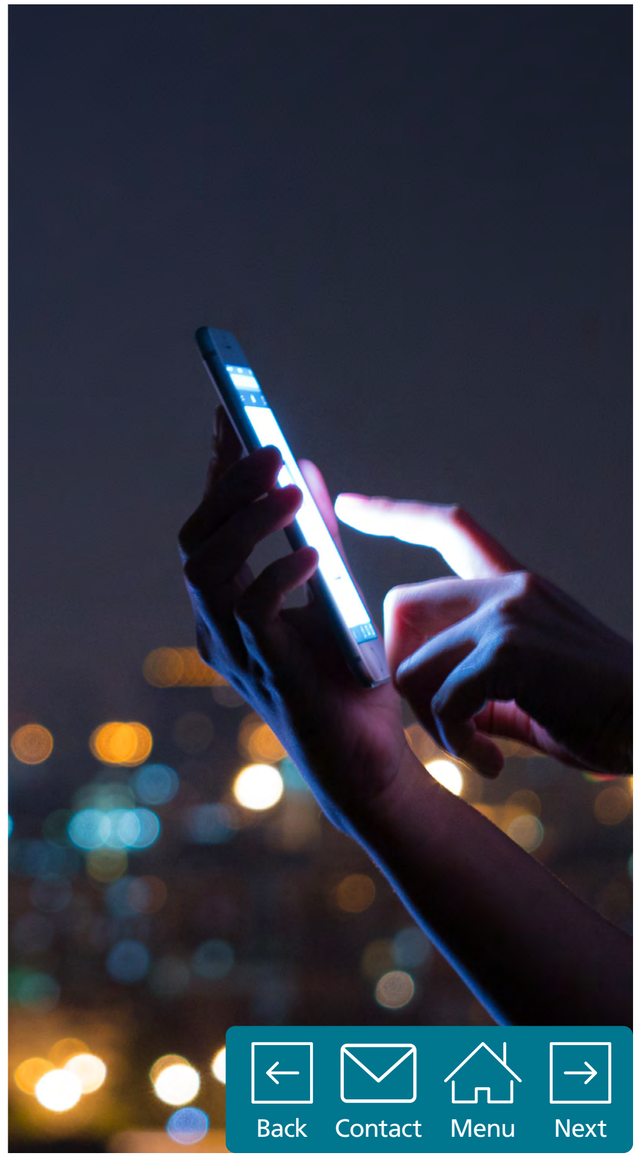
Horea Popescu
Partner
T +40 21 407 3824
E horea.popescu@cms-cmno.com

Ukraine

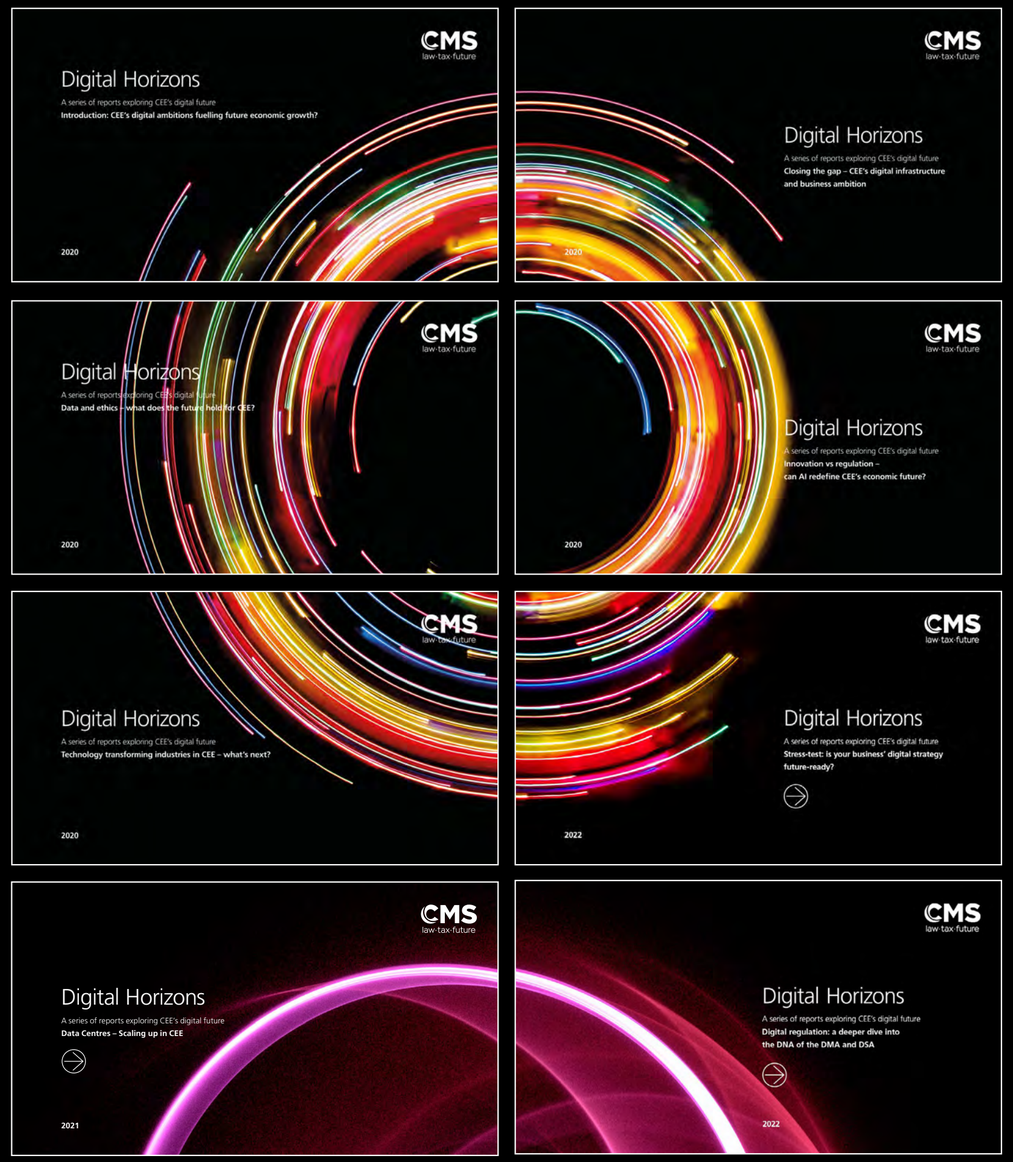
Olga Belyakova
Partner
T +380 44 391 7727
E olga.belyakova@cms-cmno.com

Austria and SEE

Gregor Famira
Partner
T +385 1 4825 600
E gregor.famira@cms-rrh.com



Digital Horizons: A series of reports exploring CEE's digital future



Read the rest of the Digital Horizons series here:

Introduction: CEE's digital ambitions fuelling future economic growth?

Closing the gap – CEE's digital infrastructure and business ambition

Data and ethics – what does the future hold for CEE?

Innovation vs regulation – can AI redefine CEE's economic future?

Technology transforming industries in CEE – what's next?

Stress-test: is your business' digital strategy future-ready?

Data Centres – Scaling up in CEE

Digital regulation: a deeper dive into the DNA of the DMA and DSA

CMS Law-Now™

Your free online legal information service.

A subscription service for legal articles on a variety of topics delivered by email.
cms-lawnow.com

CMS locations:
Aberdeen, Abu Dhabi, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Beirut, Belgrade, Bergen, Berlin, Bogotá, Bratislava, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Dubai, Duesseldorf, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Hamburg, Hong Kong, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Mexico City, Milan, Mombasa, Monaco, Moscow, Munich, Muscat, Nairobi, Oslo, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Rome, Santiago de Chile, Sarajevo, Shanghai, Sheffield, Singapore, Skopje, Sofia, Stavanger, Strasbourg, Stuttgart, Tel Aviv, Tirana, Utrecht, Vienna, Warsaw, Zagreb and Zurich.

cms.law

2009-0133931-7 DMA & DSA