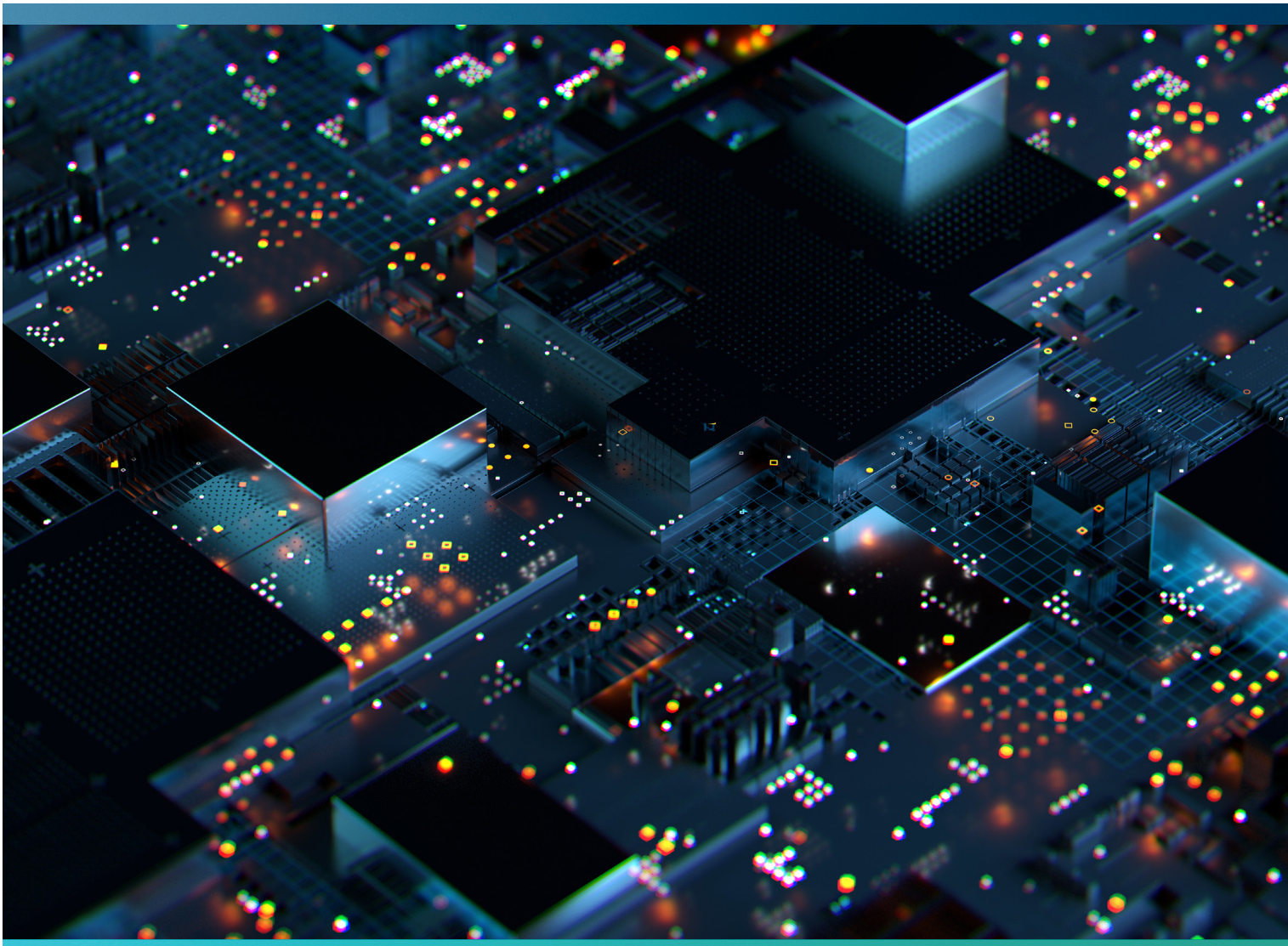
protiviti®
Global Business Consulting



The Global Consequences of Europe's New Digital Regulatory Regime

Why technology companies should care about the EU's Digital Services Act

Face the Future with Confidence®

Table of Contents

Executive Summary

A new and dramatic approach to regulating big technology firms is coming into force across the European Union. The Digital Services Act (DSA), which the European Council signed into law on September 15, 2022, aims to protect the digital space against the spread of illegal content, particularly on social networks, content-sharing platforms and e-commerce sites. The DSA carries significant financial penalties and enforcement actions against infringing companies, including potential sanctions of up to 6% of global annual sales or even a complete ban on operating in the EU single market for repeat offenders.

EU lawmakers believe the new rules will address longstanding concerns about online trading of illegal goods and services, the sharing of harmful content, the use of manipulative algorithmic systems to spread misinformation, and the control of essential ecosystems in the digital economy by a few large platforms. The European Commission also insists that the new rules will protect users, drive growth in digital services and create a level playing field for smaller players.

However, like most new regulations of its scale, the DSA has many complex requirements that could impact its enforceability. Ambiguities in definitions and methodologies are also a concern to industry leaders as they could create new liability and risks for companies.

This white paper provides an overview of the DSA and key obligations. It also contains recommendations on what companies can do now to prepare. The broad scope of the DSA, both in terms of organisations to which it is applicable and the steps required to reach and maintain compliance, means that preparations should begin sooner rather than later. While the industry and supervisors need to do more work to understand the full scope of the rules, companies should use these recommendations as a blueprint to prepare for the new regulations and to gain a head start on bringing their current digital content management and governance practices closer to compliance.

On the Horizon: Sweeping Impact

The DSA is one of two significant pieces of digital legislation (the other is known as the Digital Markets Act or DMA) that, combined, will likely reverberate beyond Europe. Together, these rules will provide a concrete regulatory blueprint for policymakers in other jurisdictions who also seek to regulate the digital space and big technology firms. A perfect example is the so-called Digital India Act, proposed legislation modelled on the DSA and the DMA that is expected to be introduced in India during the upcoming winter session of parliament.

Approved by the Council of the European Union and published in the Official Journal of the European Union in October 2022, the DSA entered into force November 16, 2022. Very large online platforms and search engines have only four months after the rules are in effect to comply, while smaller companies can apply for an exemption from certain requirements. Most companies will have to comply with many of its provisions beginning February 2024."

The new rules will directly impact hosting services, large online platforms, and search engines. But, given the global nature of the internet and the business of large technology companies, the DSA also has broad implications for technology firms of all types, both small and large, and some nontech enterprises. In a statement following the Council's formal approval, Jozef Sikela, minister for industry and trade, said he is convinced the DSA "has the potential to become the gold standard for other regulators in the world."[1]

Notably, many DSA obligations are commensurate with companies' offerings (e.g., hosting services, online platforms) and size (e.g., micro, small, large, very large). For instance, the DSA contains specific rules for platforms reaching more than 10% of Europe's 450 million consumers. Micros and small companies, as defined by the DSA, have separate and proportional obligations, including exemption from specific costly requirements.

Complexities in the rules

While the DSA has been adopted by the European Parliament and will apply broadly across Europe, there are some aspects that may differ between countries. For example, one of the core objectives of the DSA is to prevent the spread of illegal content online; the text broadly defines illegal content to be "information relating to illegal content, products, services, and activities," and the nature of illegality is defined by EU law and/or national law. Therefore, companies will need to understand how each country defines illegal content, products, services, and activities and adjust processes to monitor and manage content as needed across jurisdictions.

Skepticism across the industry

Reaction from the global tech industry to the DSA agreement has been broad and mixed. While the industry supports the overarching objectives of the new rules (to make the internet safer for all), many are skeptical about the technical details and the required implementation. For example, there's some concern about the rules exposing platforms to liability from illegal content of which they are not aware. Concerns have also been raised about how the law defines harmful content, which the industry argues is culturally subjective and often legally ambiguous, whether the transparency measures in the DSA would also protect user privacy, and the feasibility of the implementation timeline.

[1] www.consilium.europa.eu/en/press/press-releases/2022/10/04/dsa-council-gives-final-approval-to-the-protection-of-users-rights-online/

How will the DSA be enforced?

The DSA imposes significant financial penalties on infringing companies; they could be fined up to 6% of their total worldwide annual turnover. A five-year review of historical EU fines shows that potential DSA fines would be significantly higher or consistently in the multibillion-dollar range if levied against some of the largest global service providers.

For regulators, enforcing these financial penalties and other mandates of the DSA will require significant investment in investigative resources and time. They need more funding and people with the right expertise to effectively police the internet (i.e., investigating, supervising, enforcing, and monitoring compliance) across many jurisdictions.

While the European Commission has announced funding to acquire additional investigative resources, critics fear that limited resources and manpower will result in ineffective enforcement of the DSA. To remedy this criticism and effectively enforce the DSA, the European Commission put forth a layered enforcement approach that involves partnering with national regulators or Digital Service Coordinators and relying on the support of a newly established entity known as "the Board."

Below is a summary of the responsibilities for the enforcement regime.

DSA Enforcement Regime

Digital Services Coordinators (DSCs)

- A national authority assigned by each EU member state
- Responsible for all supervision and enforcement of the DSA at the national level
- Has authority to: request and seize documents; inspect premises; impose fines or periodic penalty payments; adopt interim measures

European Commission

- Primary regulator for very large online platforms and very large online search engines. Can initiate investigations on its own or at the recommendation of a DSC
- Responsible for streamlining enforcement and preventing lax enforcement by member states
- Has authority to (in addition to those available to DSCs): perform due diligence activities, including risk assessments; initiate independent audits; issue noncompliance decisions; impose legally binding commintments on companies.

The European Board for Digital Serviceds Coordinators

- Advisory group tasked with ensuring consistent application of the DSA
- Responsible for drafting Codes of Conduct and supporting joint investions between DSCs and the European COmmission
- Has authority to: Advise the European Commission and DSCs on enforcement measures and adopt opinions addressed to DSCs.

Key Obligations in a Nutshell

The legislation is exhaustive, with several key obligations well defined. It contains general obligations that apply to all intermediary service provider groups, and a more specific set of requirements for certain types of companies, like hosting services providers and very large online platforms.

Summary of key obligations

PROVIDER	OBLIGATION
All Intermediary Services Providers [e.g., internet access providers, domain name registrars]	• Service contracts (terms and conditions) must meet certain minimum requirements to ensure clarity, transparency and fairness. • Terms and conditions should include information on any policies, procedures, measures and tools used for content moderation. • Companies must publish an annual transparency report. • A company without EU establishment must appoint a local representative in one of the EU member states where it operates.
Hosting Services Providers (Including Online Platforms and Very Large Online Platforms) [e.g., companies offering cloud computing and web hosting services]	• User-friendly notices and take-down mechanisms must be provided to allow notification of illegal content by third parties. • Notice of illegal content should be processed swiftly, and prompt actions taken to address the issue (i.e., remove or disable access to the content). • Anonymity of content reporters should be protected, except in cases involving violation of image rights and intellectual property rights. • Serious criminal offences involving threat to life or safety of persons must be reported to law enforcement or judicial authorities.
Online Platforms (all) [e.g., online marketplaces, app stores, social media platforms]	• An internal complaint-handling system should be created to enable service recipients affected by content moderation decisions to lodge complaints within a given period. • Companies shall provide transparency reports detailing the number of complaints received, disputes submitted to out-of-court dispute settlement bodies, numbers of suspensions and advertisements removed, and use of automated content moderation tools. • Companies are prohibited from using "dark patterns," a range of potentially manipulative user interface designs used on websites and mobile apps. • Qualified staff should be assigned to review the complaints and ensure compliance with standards. • Platform operators must remove traders offering illegal products or content and maintain a record of removal. • Companies are required to clearly identify parameters used to determine advertisement recipients. • Providers that use software to predict user preferences must disclose to the user how the system operates and the options available to modify preferences.
Very Large Online Platforms (only) [e.g., platforms with a reach of more than 10% of the 450 million consumers in the European Union.]	• Companies must identify systemic risks stemming from the use of their services, particularly those related to the sharing of illegal content. • Mitigation measures must be implemented to deal with the system risks. • Independent audits, performed by independent firms, should be conducted to assess providers' compliance with the DSA and related obligations. • Providers using recommender systems must provide at least one that is not based on profiling and allows users to set their preferred options for content ranking. • Providers are required to publish information on advertisements that have been displayed on their platform, including the targeted audience, relevant parameters and number of recipients reached. • Content deemed to be "deep-fakes" shall be clearly labelled. • Companies will be required to share data with authorities so they can monitor and assess compliance with the DSA. Vetted researchers must meet stipulated requirements.

Actions Companies Should Take Now

As the DSA's effective date looms, global technology organisations will need to make a strategic decision regarding how they plan to align to its jurisdictional requirements. A similar conundrum surfaced in 2016 with the passing of the EU's General Data Protection Regulation (GDPR). International organisations had to decide whether to limit the scope of the GDPR remediation work to EU data only, saving costs up front, or apply the remediation enterprise-wide and add efficiency for future privacy regulations that will inevitably come. As such, global technology organisations will need to decide if they are going to take a lowest-common-denominator approach in developing enterprise programs to meet the DSA's European-specific requirements.

The DSA's broad mandates and varying implications for different types of organisations mean there is no one-size-fits-all solution for preparing; however, there are overarching strategic approaches and more tactical operational actions that business leaders should consider.

The Digital Services Act... has the potential to become the gold standard for other regulators in the world. By setting new standards for a safer and more accountable online environment, the DSA marks the beginning of a new relationship between online platforms and users and regulators in the European Union and beyond.

– Jozef Síkela, Minister for Industry and Trade, Czech Republic

Strategic Considerations

When planning for 2023 and beyond, organisations should consider the impacts that the DSA may have on the overall strategy of their operations.

- **Innovation and product development** — Balancing compliance with the DSA's new obligations while continuing to drive innovation and fuel growth is a challenge that all organisations will face. As the new requirements impose certain constraints on how an organisation's platforms and products function and operate, companies will need to consider how they will continue to innovate and develop new products. Businesses should consider DSA requirements and impacts as part of their existing product-development and change-management processes.
- **Market entry** — Organisations will need to determine their market-entry and merger-and-acquisition strategies, particularly as they consider entering European markets or acquiring companies that serve the European customer base.
- **Ownership and accountability** — Organisations will need to assign internal ownership and determine accountability of the DSA. With its requirements touching all parts of an organisation, from legal to risk and compliance to engineering, creating a governance structure that supports an integrated approach to compliance will be essential.

- **Skill set assessment** — To understand the complexity of the programs that will be needed to support compliance with the DSA, organisations should consider how their current staff is equipped to evaluate, implement and monitor the programs required under the DSA. For instance, when considering the large shift in transparency of artificial intelligence models and required self-assessments, compliance and audit teams may need additional technical skill sets to meet the DSA's obligations. On the contrary, product and engineering teams may benefit from employing risk and control professionals in the first line to instill a risk and controls mindset more proactively and seamlessly across the organisation.

Immediate Operational Actions

Organisations should consider taking action to prepare for DSA compliance as soon as possible. There are several actions organisations can take immediately:

- All organisations should perform **an impact assessment** of the DSA to understand which requirements will apply to the company immediately upon the DSA effective date and in the future, based on growth projections.
- Organisations should **review applicable requirements against their current governance framework and structure**, including policies, processes, and tools, to understand where the most significant compliance gaps are. This may include evaluating current activities and identifying how to strengthen efficiency of compliance efforts, (e.g., utilisation of artificial intelligence/machine learning for content monitoring).
- Organisations should **initiate a centralised governance structure to mobilise and operationalise efforts** to address compliance gaps and generally prepare for the DSA effective date. This may require regular touch points with senior leadership and escalation of impact on the company's strategic decisions, such as new market or product entry and/or organisational structure. Specific activities that the centralised governance structure may manage include:
  - Assessing how the organisation conducts investigations aimed at detecting, identifying, and removing illegal content from its platforms;
  - Assessing and preparing a clear written explanation about the company's use of algorithmic decision-making, artificial intelligence, and human review of online content
  - Reviewing all relevant contracts in force and establishing process to identify gaps in processes, controls, monitoring, resources, training and communication as they relate to content management.
  - Seeking independent auditors to evaluate DSA preparedness efforts with the goal of ensuring that proper processes and standards are clearly established and consistent with DSA requirements;

Conclusion

While the short-term enforceability remains opaque, it is indisputable that the long-term impact of the DSA will fundamentally change how some companies approach doing business online and, more specifically, how they approach online content moderation. The impact will undoubtedly result in multiyear efforts by many organisations to rebuild or reengineer existing internal processes and control functions.

Many non-EU regulators are likely to follow the European Council in introducing similar stringent measures to fight so-called harmful content. In the United States, establishing such a regulatory framework at the federal level will require treading carefully between enabling free expression and access to information and fostering a digital environment that is safe for all people but does not stymie competition and innovation. In the absence of a DSA-like federal law, individual U.S. states are likely to continue the trend to regulate internet content.

The sheer complexity of the obligations in the DSA means that companies should be starting their journey in building their strategy and operational approaches to compliance. Now is the time to evaluate your organisation's current practices and legal obligations, and to develop a comprehensive approach that is able to detect, notify, remove and prevent illegal content. Developing such a program, one that aligns with where global regulatory trends are headed, will allow organisations to build trust with their consumers and regulators — and go a long way to ensure they act with integrity and the highest ethical standards when it comes to corporate behaviour in a digital environment.

ABOUT PROTIVITI

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach, and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, governance, risk and internal audit through its network of more than 85 offices in over 25 countries.

Named to the 2022 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

CONTACTS

Gordon Tucker
Managing Director and
Global Head of Technology,
Media and Telecommunications
+1.415.402.3670
gordon.tucker@protiviti.com

Matthew Moore
Managing Director and
Global Head of Risk and
Compliance practice
+1.704.972.9615
matthew.moore@protiviti.com

Jonathan Wyatt
Managing Director and European
Regional Market Leader
+44.207.024.7522
jonathan.wyatt@protiviti.co.uk

Kaitlin Kirkham-Cooper
Managing Director
+1.630.780.8942
kaitlin.kirkham-cooper@protiviti.com

Christine Halvorsen
Managing Director
+1.703.299.3504
christine.halvorsen@protiviti.com

Tjakko de Boer
Managing Director
+31.20.346.0400
tjakko.deboer@protiviti.nl

Roxanne Miller
Associate Director
+1.815.228.2471
roxanne.miller@protiviti.com

Joseph Emerson
Director
+1.772.485.1814
joseph.emerson@protiviti.com

THE AMERICAS

UNITED STATES
Alexandria, VA
Atlanta, GA
Austin, TX
Baltimore, MD
Boston, MA
Charlotte, NC
Chicago, IL
Cincinnati, OH
Cleveland, OH
Columbus, OH
Dallas, TX
Denver, CO
Ft. Lauderdale, FL
Houston, TX
Indianapolis, IN
Irvine, CA
Kansas City, KS
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
Nashville, TN
New York, NY
Orlando, FL
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
Portland, OR
Richmond, VA
Sacramento, CA
Salt Lake City, UT
San Francisco, CA
San Jose, CA
Seattle, WA
Stamford, CT
St. Louis, MO
Tampa, FL
Washington, D.C.
Winchester, VA
Woodbridge, NJ

ARGENTINA*
Buenos Aires

BRAZIL*
Belo Horizonte*
Rio de Janeiro
São Paulo

CANADA
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE, MIDDLE EAST & AFRICA

BULGARIA
Sofia

FRANCE
Paris

GERMANY
Berlin
Dusseldorf
Frankfurt
Munich

ITALY
Milan
Rome
Turin

THE NETHERLANDS
Amsterdam

SWITZERLAND
Zurich

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

EGYPT*
Cairo

SOUTH AFRICA *
Durban
Johannesburg

ASIA-PACIFIC

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*
Bengaluru
Chennai
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM

protiviti®