CMS
law·tax·future

Grasping the opportunity in digital regulation

Digital regulation is shaping the future of Europe's economy. Now is the time to prepare.

November 2023

Foreword

Europe stands on the cusp of a new era in the digital revolution. An ongoing wave of digital regulation – some already in place, some still in development – will shape how the European economy uses digital technology for decades to come.

With GDPR, the EU has shown that it can set new standards that shape global markets. But the current wave of regulation being implemented by the EU and other jurisdictions such as the UK goes deeper, creating a comprehensive new framework for the digital era.

It is unfolding faster than any previous regulatory intervention. And while governments across the globe are building new regulatory platforms for the digital economy, the EU approach is the most ambitious, and will arguably set the agenda for the rest of the world.

As a result, regulatory dynamics will completely redefine companies' business models and operations – and those of their competitors.

Crucially, business leaders must recognise that the current wave of digital regulation in Europe is more than a matter of compliance. Together, new regulations on non-personal data, AI, digital platforms and cyber safety will establish new commercial dynamics, new risks and opportunities and, in some cases, new markets, all of which demand a global strategic response.

Adaptation is a necessary precondition of survival. Those that live up to the challenge will also be better placed to capture first mover advantages, to bolster their competitiveness in digital markets, to reduce their technology costs and to enhance the resilience of their digital systems.

To explore the views of business leaders on this wave of digital regulation, we surveyed 450 senior in-house legal counsel from across the EU and UK.

The survey revealed that, although regulation presents commercial threats and compliance challenges, European businesses also see opportunities in this wave of regulation to gain competitive advantage – and not just in Europe, but around the globe as well.

This is encouraging. Regulation need not always be seen as a threat. In Europe, the comprehensive framework and the legal certainty provided by proactive regulation offers businesses an opportunity to get a head start in the next wave of digital innovation. Companies that recognise this opportunity, and act upon it, will be the ones that thrive in the coming decade.

María González Gordon
Managing Partner

Head of Intellectual Property, Industrial Property and Digital Business

T +34 91 187 19 06
E maria.gonzalezgordon@cms-asl.com

Björn Herbers
Partner
Co-Head of Digital Business

T +32 2 6500 428
E bjoern.herbers@cms-hs.com

Contents

Key findings

An unprecedented wave of digital regulation is underway in Europe. To investigate its impact, we conducted a survey of 450 senior in-house legal counsel operating in a number of different sectors of the economy across the EU and the UK. Here's what we found:

How businesses respond to regulation will determine their success in the digital age

76%
agree that only those who adapt to digital regulation will succeed in this new economy.

73%
agree that acting quickly on new regulation is essential to keep pace with digital innovation.

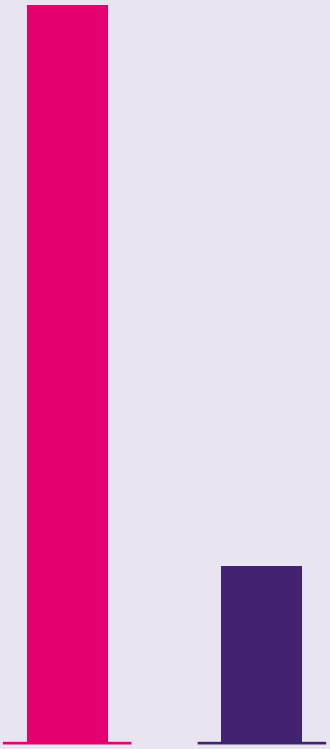
Businesses are underestimating the impact of the EU's non-personal data strategy

The EU is laying the foundations of a new data economy, but only:

9%
consider non-personal data (NPD) to be 'highly' strategic to their business.

13%
believe NPD regulation offers significant opportunities.

In-house counsel are optimistic about their prospects



71%
perceive that they are better prepared than their competitors.

Only **17%**
believe digital regulation poses a strategic threat, despite its far-reaching implications.

AI regulation presents more opportunities than threats

94% believe that AI regulation offers 'significant' or 'moderate' opportunities, including the ability to compete on a safe playing field with legal certainty.

Meanwhile, 80% think AI regulation poses 'significant' or 'moderate' commercial threats, suggesting some concerns of 'overregulation'.

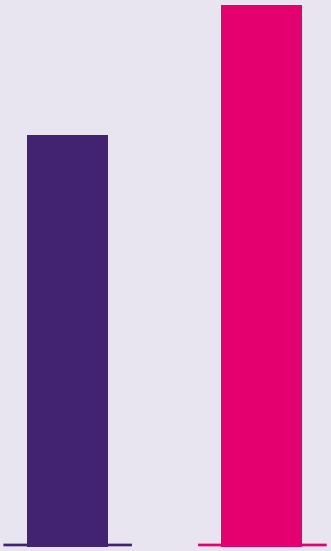
Cyber safety regulations will bring costs as well as opportunity, in-house counsel believe

Cyber safety regulation will bring commercial opportunities, most respondents believe, including improved ability to utilise data. It will also enable long-term technology strategy. But they also perceive commercial threats:

47%
Increased need for investment in technology adoption.

40%
Reduced ability to innovate. This may be an outdated view, as security can help unlock adoption.

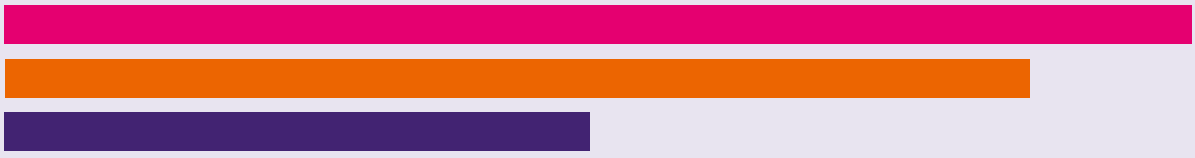
The majority of in-house lawyers see digital platform regulation as a 'significant' opportunity



54%
expect 'significant' commercial opportunities to arise from digital platform regulation.

This includes 71% of content providers, who have much to gain from regulation aimed at curbing the market power of large online platforms.

Most businesses have assessed the impact of digital regulation. Now it's time to act.



73%
have taken steps to assess the risks of digital regulation.

63%
have consulted external counsel.

But only 36% have revised their digital transformation plans, despite looming deadlines. Falling behind schedule is not an option.

A new era for the global digital economy

The EU is positioning itself as the global pacesetter in digital regulation. Its Digital Agenda for the current decade aims to create safer digital spaces, improve competitiveness, strengthen Europe's digital sovereignty, and reduce the continent's digital and carbon footprint.

By placing the region ahead of the curve on issues such as artificial intelligence (AI), access to non-personal data, online platform conduct and fair competition in digital markets, among others, it hopes to shape the next era of global digital innovation.

This ambition lies behind an unprecedented wave of digital regulation that has been recently enacted or is in development. With its Data Act[1] and Data Governance Act[2], for example, the EU hopes to unlock untapped economic potential by requiring businesses to share non-personal datasets. Through the AI Act,[3] the EU wants to be the first to define and mitigate the risks of AI, while unlocking its opportunities.

The Digital Services Act (DSA)[4] regulates online intermediaries and platforms for offering a safer environment for users and consumers and also to prevent illegal and harmful activities online and the spread of disinformation. The Digital Markets Act (DMA),[5] meanwhile, aims to curb the dominance of 'gatekeepers' in the digital economy, boosting fairness and competition. And with various new cyber safety regulations, the EU is shoring up protections against increasingly destructive threats that permeate our digital lives.

New regulations such as these are already shaping the global landscape. Every business that has contact with the EU must comply with them, whether is it because they are based in the EU or they target the EU public. As international businesses tend to align with the strictest regulatory standards, EU rules often become global standards. And countries outside the EU are already following its example with comparable legislation.

The UK, for example, is likely to largely mirror the EU's regulatory regime, but with some key differences that businesses need to be aware of to prevent their regulatory obligations from becoming too burdensome. For instance, the Digital Markets, Competition and Consumers Bill,[6] which introduces a new regulatory regime for large digital platforms in the UK, will differ from its EU counterpart in some respects including the criteria for companies to which it applies and how it will be enforced. In-house counsel across sectors need to be aware of these disparities and understand the implications for their organisations.

Digital regulation on the agenda

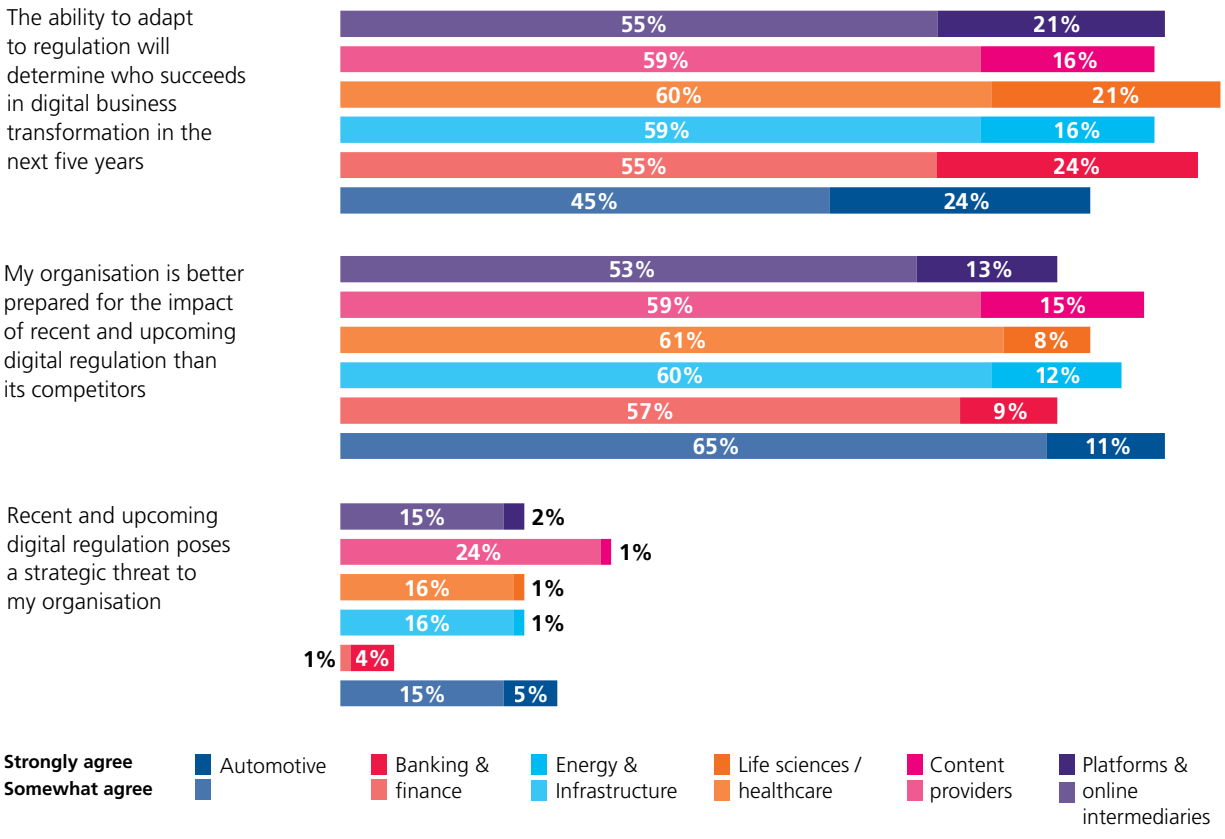
Legal counsel recognise what's at stake. Over three quarters of our survey respondents (76%) agree that the ability to adapt to regulation will determine who succeeds in digital business in the next five years. And they know they can't wait: 73% agree that acting quickly on new regulation is essential to keeping pace with digital innovation.

In-house legal counsel are generally optimistic about digital regulation. Only 17% believe that it poses a strategic threat to their organisation. This belief was most common among online platforms and intermediaries, but still only a quarter of these agree.

And respondents are remarkably confident of their ability to adapt: more than seven in ten believe their organisation is better prepared for the impact of digital regulation than its competitors. This confidence is highest among respondents in the automotive sector (see **Figure 1**.)

As we'll see in the following chapters, recent and upcoming regulation in four areas – non-personal data, AI, digital platforms and digital safety – presents opportunities and challenges. Understanding these will help businesses prepare for success.

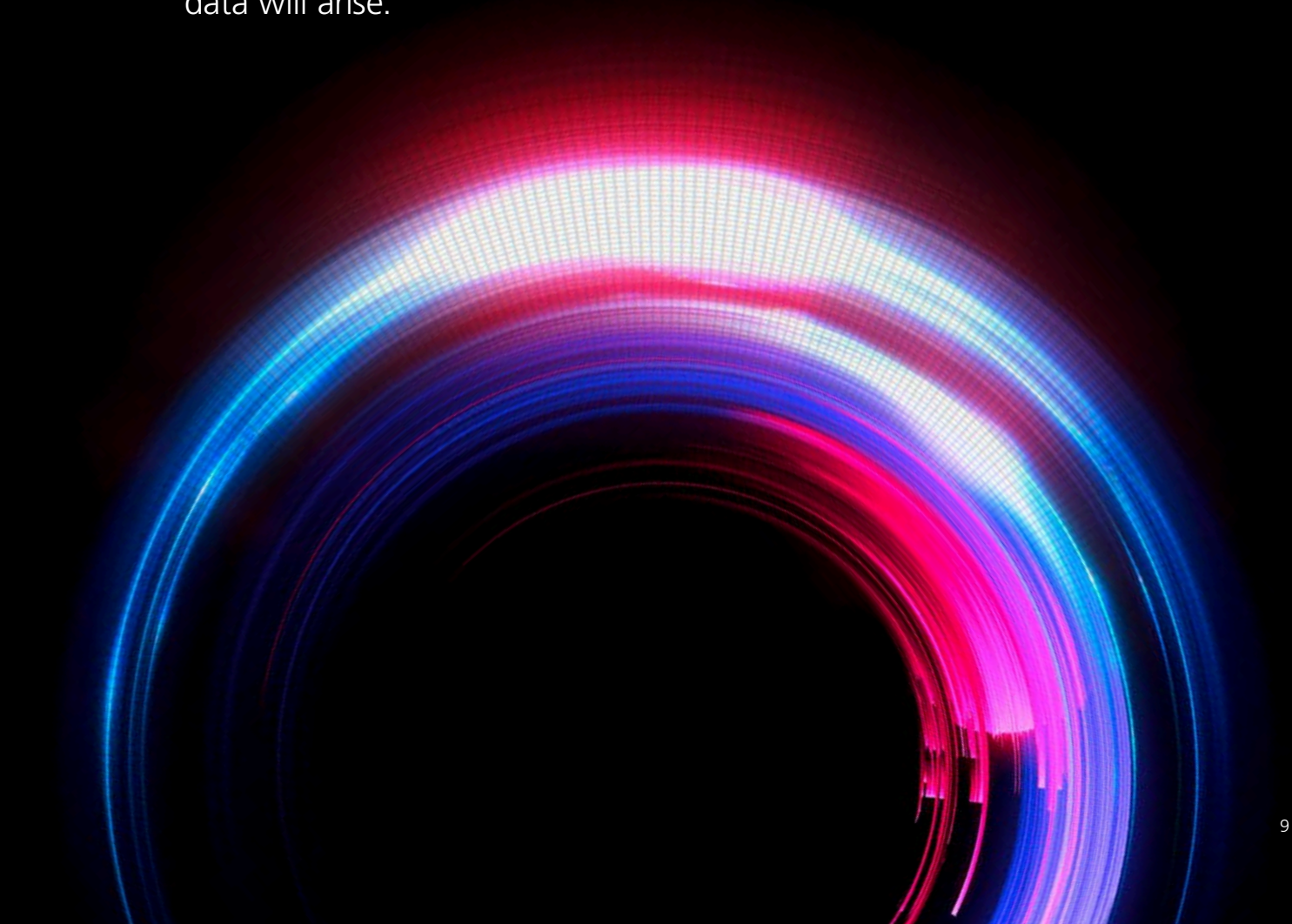
Figure 1. What's at stake in digital regulation
% of respondents who somewhat or strongly agree, by sector



The dawn of a new data-centric economy

With GDPR, the EU changed the way businesses handle personal data, not just within its borders but across the world. It obliges any business handling an EU citizen's data to uphold their data rights and provided a blueprint for data protection regulations around the globe.

Now, the EU is turning its attention to the data that sits outside GDPR's purview: the datasets that reside in company databases, devices and equipment. This data represents an untapped economic opportunity, the EU believes: if users and other companies could access and share it, a whole new economy based on non-personal data will arise.



The EU's Data Act aims to unlock this potential by affirming new rights for businesses and individuals to access non-personal data (NPD) from the devices and equipment they use. And its Data Governance Act will facilitate NPD sharing between businesses, establishing new technical standards, legal mechanisms and infrastructure for data intermediaries.

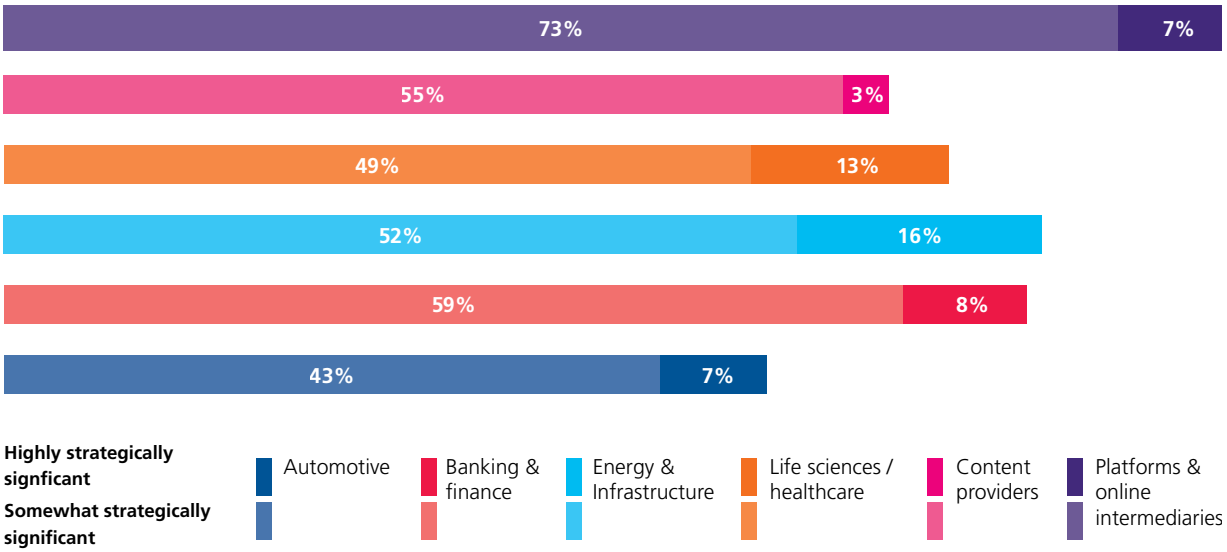
The UK's National Data Strategy, meanwhile, includes a 'Mission' to "unlock the value of data across the economy".[7] In November 2021, the government published a 'framework for action' designed to facilitate greater data sharing. The UK is also expected to extend the Open Banking model it pioneered, which allowed start-ups to access the data held by major banks, to other sectors such as energy.

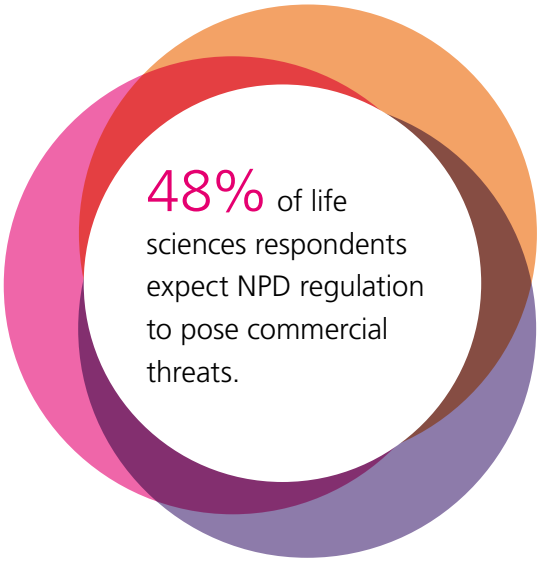
Despite these efforts, and somewhat surprisingly, NPD is viewed as the least strategically significant of the four technology areas included in our survey. Only 65% consider it to be in any way significant, and just 9% view it as 'highly' strategic for their organisations.

This is at odds with the EU's ambitions in the NPD space. It hopes to create nothing less than a new data-based ecosystem, in which sharing is not only enabled but encouraged. If successful, this has the potential to disrupt entire markets, with strategic consequences for many businesses.

Attitudes vary considerably by sector: 80% of respondents from digital platforms and intermediaries say that NPD is of strategic significance, compared with just 56% of respondents from the automotive industry (see **Figure 2**).

Figure 2. The strategic significance of non-personal data
% of respondents rating 'highly' or 'somewhat' strategically significant, by sector





"This is in contrast to technological developments in the industry," says Martin Wodraschke, head of the CMS Automotive Group. "Cars today are packed with digital devices and produce an increasing amount of non-personal data, such as data on tyre pressure, fuel consumption and battery charge status.

"At first glance, the personal data, such as the driver's biometric data, driving behaviour and driving habits, seem to be more valuable, but the non-personal data will be crucial for the functioning of driving and vehicle safety in the future. Further, this vehicle data is also of great interest to other players in the automotive sector, particularly in the field of after-sales service."

Even so, the majority has yet to acknowledge the significance of NPD, our survey indicates. When Europe regulation mandates NPD sharing, many in sectors where the use of sensors is key, including energy, life sciences and automotive, might find themselves missing opportunities when accessing data from competitors.

The impact of NPD regulation

Respondents are also less likely to see NPD regulation as presenting opportunities, threats, or even legal implications than the other three technology areas.

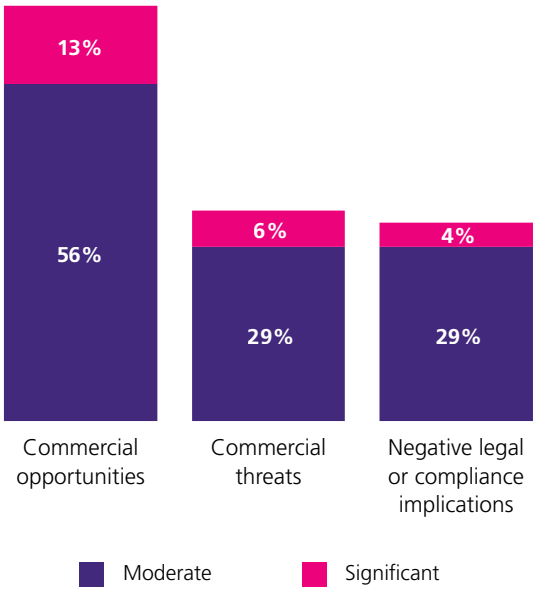
Only 69% view NPD regulation as a source of opportunity, with increased organisational efficiency and an increased ability to compete in the digital markets the most widely anticipated commercial opportunities (see **Figure 3**).

This proportion rises to 80% among respondents in the energy and infrastructure sector. Energy is a highly data-driven field, and opening up access to NPD could unlock innovation, efficiency and integration in national energy systems (see **Towards energy platforms** on page 21).

Just over a third of respondents (35%) see NPD regulation as a commercial threat. Across sectors, the top-ranked commercial threats arising from NPD regulation are reduced market share, reduced ability to disrupt competitors and increased technology adoption costs.

These fears are unfounded, says María González Gordon, a managing partner at CMS specialising in intellectual property and digital business. "The intention of the NPD regulations is to achieve the opposite effect to that which is feared by the survey respondents. The measures are intended to level the playing field and provide greater access to data across all sized business in fair, reasonable and non-discriminatory terms, providing efficiencies and a more competitive landscape."

Figure 3. Opportunities and threats from non-personal data regulation
% of respondents expecting each to arise



Opening possibilities for Europe's data

A key pillar of Europe's data strategy is the creation of various sector-specific 'data spaces'. These combine data standards, governance mechanisms and infrastructure to facilitate data sharing within a given industry.

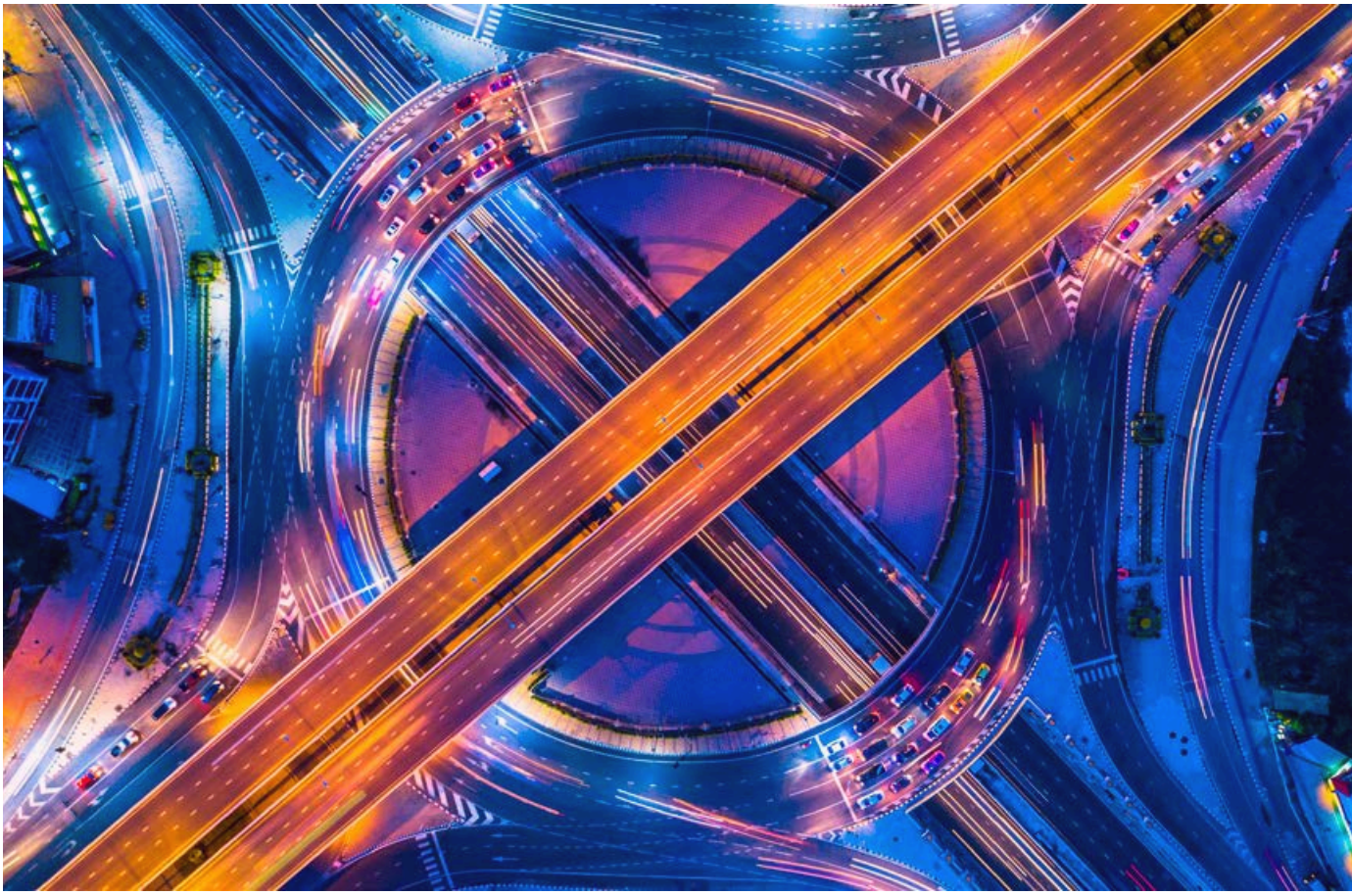
One of the most widely anticipated is the European Health Data Space.[8] This promises to grant patients greater control over their medical data, while also giving researchers access to anonymised data.

This has the potential to revolutionise Europe's healthcare sector, explains Roland Wiring, a partner at CMS specialising in the life sciences sector. "Since pharma and medtech companies, as well as insurers and healthcare providers, have substantial data, this industry has a wealth of raw data waiting to be unlocked," he says.

But, given the sensitivity of medical data, the European Health Data Space is subject to its own regulation, currently in development. Policymakers from around the EU are currently debating how the need for patient privacy can be balanced against the potential value of their data to medical research.

Their answer to that question will have far-reaching consequences for the future of the industry. "This is a core issue both for the industry and healthcare providers," adds Wiring.

> "The healthcare industry has a wealth of raw data waiting to be unlocked."
>
> **Roland Wiring**
> Partner, CMS



The highest level of concern is registered by respondents in the life sciences/healthcare sector, 48% of whom see commercial threats arising. Among other concerns, these companies may fear that open access to data from connected healthcare devices will threaten their ability to use it to their competitive advantage or that data collected using considerable resources would need to be provided to third parties.

Respondents' muted optimism about NPD regulation, compared with other areas included in the survey, suggests that in-house counsel across industries are underestimating its impact. The Data Act in particular promises to open new frontiers in the digital economy by allowing users of any connected device to access the data it contains. With data now widely recognised as a strategic asset, this is certain to have dramatic economic effects across sectors.

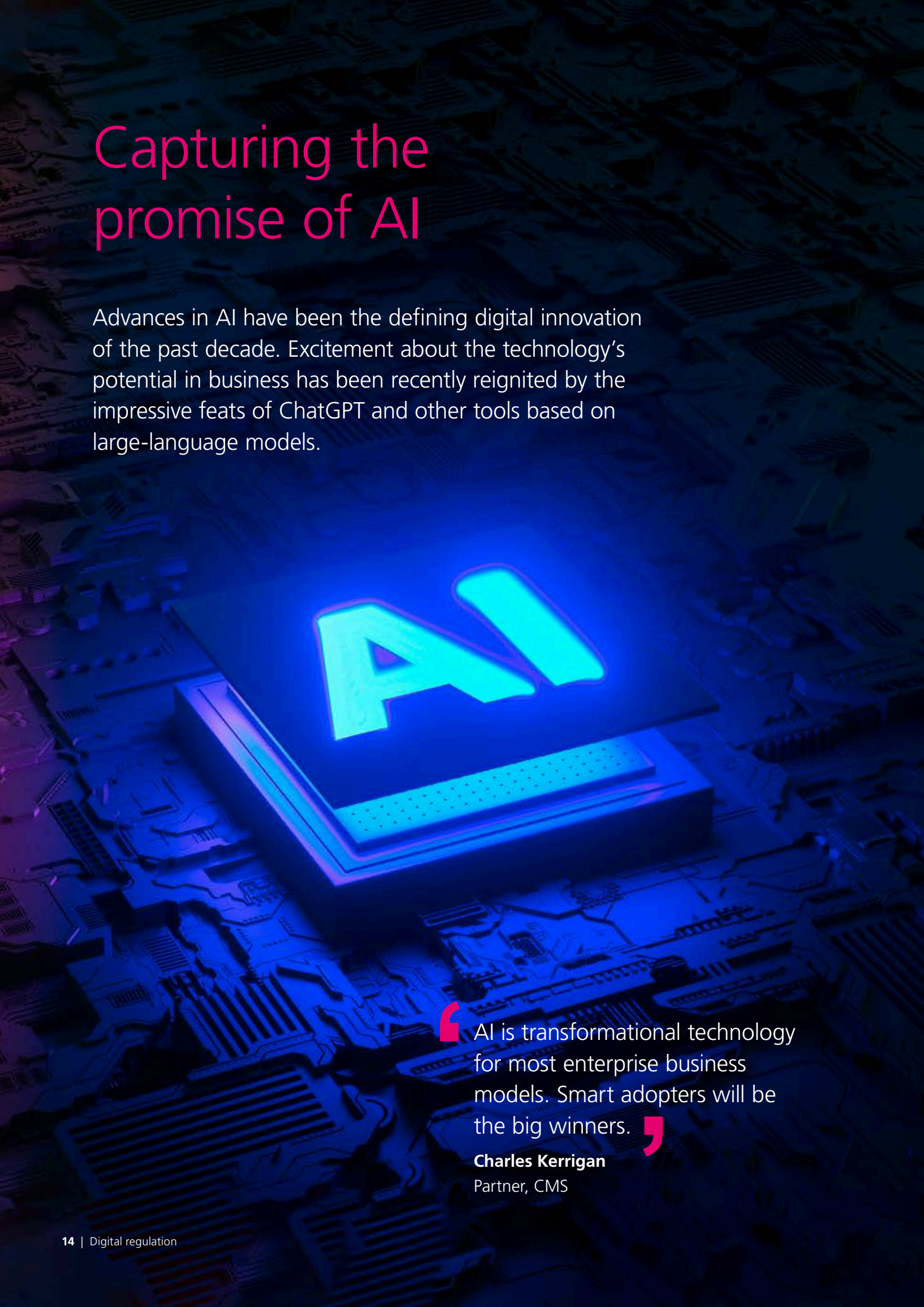
The EU may be a victim of its own success: GDPR has succeeded in making companies cautious about the use of data. It may also run counter to in-house legal teams' instincts on competition law. "The Agencies generally warn companies not to share any sensitive data between competitors because it might lead to collusion," says Björn Herbers, a partner at CMS specialising in competition law and digital business.

But both EU and UK policymakers are committed to unlocking the economic value of unshared and underused industrial data. Companies must understand both the obligations this will place upon them – in particular, how they must respond to data access requests – and the opportunities it presents to gain more data, and therefore more insight, on customers and competitors.

> "Inhouse legal teams need to get used to the new NPD rules: The Agencies generally warn companies not to share any sensitive data between competitors."

Capturing the promise of AI

Advances in AI have been the defining digital innovation of the past decade. Excitement about the technology's potential in business has been recently reignited by the impressive feats of ChatGPT and other tools based on large-language models.



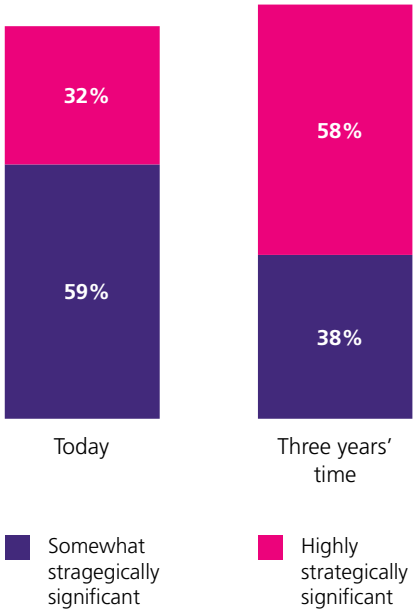
> AI is transformational technology for most enterprise business models. Smart adopters will be the big winners.
>
> **Charles Kerrigan**
> Partner, CMS

Even so, most survey respondents still view AI as a future concern. When respondents were asked how important AI is for their organisation today, fewer than a third currently describe it as 'highly strategically significant'. Content providers are most likely to identify it as such (43%), and respondents working in energy and infrastructure are the least (17%).

The strategic significance of AI will increase rapidly in the coming years, respondents expect: 58% of respondents expect AI to be highly significant in three years' time, including 68% of platforms and online intermediaries (see **Figure 4**).

But the time to grasp the AI opportunity is now, says Charles Kerrigan, a partner in CMS' Finance team. As consumers and business buyers become more familiar with AI, the more they will expect the companies they buy from to adopt the technology, he adds. "We're in a time when all customers use AI, so their expectations in dealing with businesses will be raised."

Figure 4. AI's growing strategic significance
% of respondents rating AI's strategic significance today and in three years



AI and the future of financial regulation

The banking and finance sector expects AI to be a gamechanger within just a few years: 55% of in-house counsel from the industry predict that it will be 'highly strategically significant' in three years' time.

"This is transformational technology for most enterprise business models," says Kerrigan. "Smart adopters will be the big winners."

In fact, regulated firms already have thousands of AI deployments, he adds, with applications in HR, risk management, fraud prevention, trading and more.

Not only will this change the business, Kerrigan expects, it will change the way in which it is regulated. "Just as firms can't use analogue methods to check compliance with digital systems, nor can regulators," he explains.

As a result, 'regtech' – technology that supports or measures regulatory compliance – and 'suptech' – technology that enables supervisors to check compliance – will become increasingly vital to the financial services sector, Kerrigan predicts. "Digital economies need digital regulators."

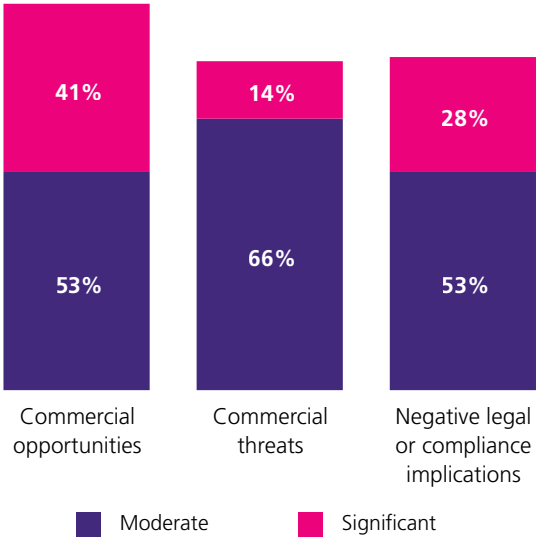
Leading the way in AI regulation

As excitement about the potential of AI has gathered pace in the last decade, so too have calls for its regulation.

The EU has made most progress towards regulating AI. Its AI Act is among the first concerted efforts to build a comprehensive framework for managing the risks and maximising the opportunities that AI presents. In November 2023, both the UK[9] and the US[10] also announced new institutes to lead their efforts on making AI innovation safe for all.

Figure 5. Opportunities and threats from AI regulation

% of respondents expecting each from AI regulation

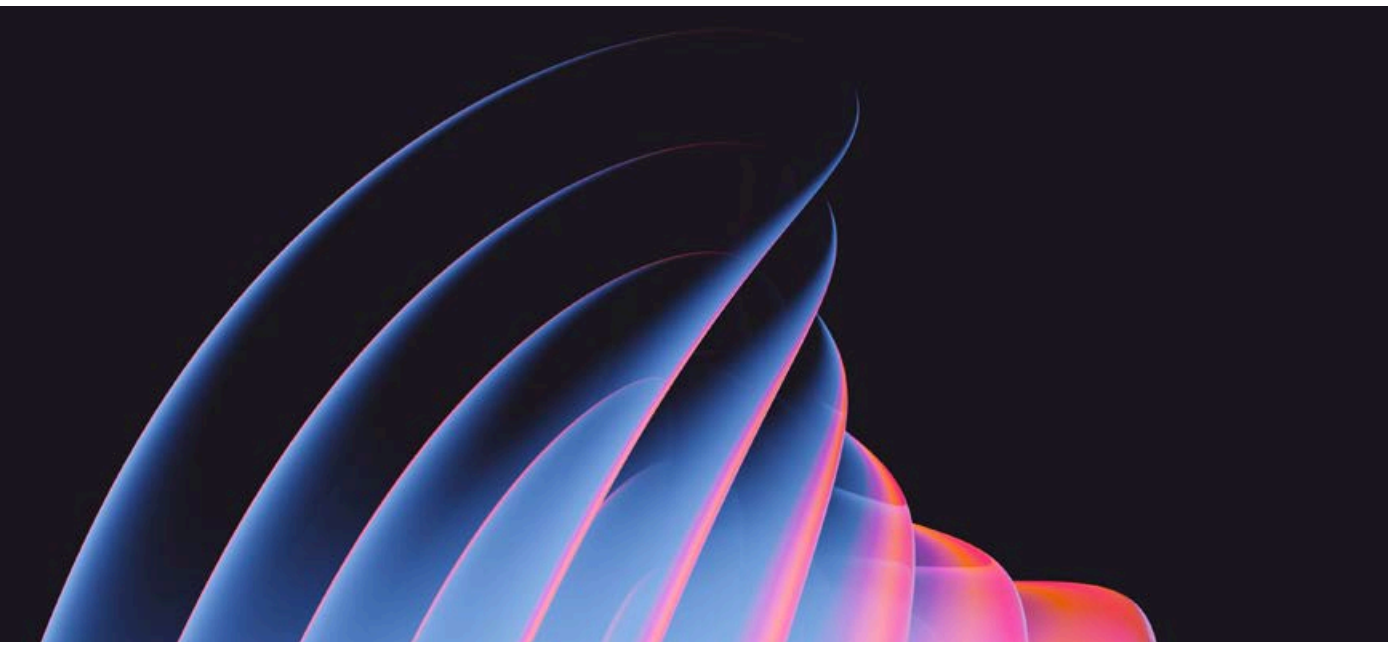


The EU AI Act categorises AI applications according to the risk they pose. Applications that present an "unacceptable risk" will be banned outright. Those deemed high risk will be subject to stricter controls than low-risk AI tools. Businesses will need to understand what risks their AI applications pose, requiring internal expertise that many organisations may currently lack.

Of the four areas of digital regulation included in our survey, respondents see the most widespread benefits in AI regulation, with 41% anticipating 'significant' and 53% 'moderate' opportunities. However, survey respondents also seem to show a certain fear of overregulation of AI. While only 14% see AI regulation as presenting 'significant' commercial threats, 66% envision moderate threats (see **Figure 5**).

The most widely anticipated opportunity from AI regulation is 'improved resilience and security of technology systems', which 45% of respondents rank in their top three expected opportunities. By imposing risk-based controls of AI applications, this suggests the EU's AI Act may reassure businesses that their systems are stable and secure.

Another widely anticipated opportunity from AI regulation is the increased ability to compete in digital markets, which is ranked in the top three by 41% of respondents. This implies that by providing legal certainty, AI regulation will give businesses the confidence to innovate.



AI Act: the costs of compliance

Still, AI regulation is not without its drawbacks, respondents say. The chief commercial threat posed by AI regulation, the survey suggests, is a reduced ability to compete compared with Big Tech (this is ranked in the top three threats by 42% of respondents). Smaller organisations may fear that larger rivals are better equipped to meet the regulatory requirements of the AI Act, although it is the risks posed by an AI application that determine how it will be regulated, not the size of the organisation behind it.

Meanwhile, the majority of respondents (81%) expect the AI Act to have legal or compliance implications for their companies, including 28% who expect these to be significant. The most widely anticipated legal implications are an increased complexity of contracts (69% rank this in their top three) and increased legal costs to ensure compliance (62%) (see **Figure 6**).

But while compliance may incur some costs, it is usually cheaper than litigation in the event of a dispute. To date, there have been relatively few legal claims arising from AI technologies, but there is a general expectation that there will be a considerable increase in claims of this nature over the next few years, warns Lee Gluyas, a partner at CMS who specialises in IT-related disputes.

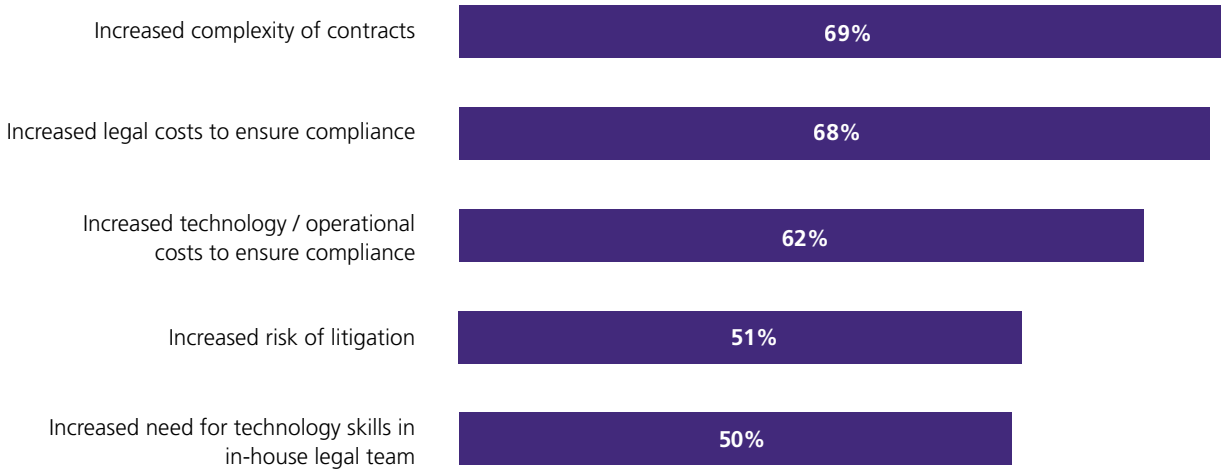
Like all legal claims, these will be heavily dependent on the facts. Many will be complex, especially in circumstances where several factors contribute to the dispute. For example, there may be contention around whether the failure of an AI system is the fault of the producer, the user or a party that supplied or input the data, or a combination of those parties.

This added complexity will no doubt lead to increased legal costs of managing the dispute, and businesses should take steps to understand technologies they are deploying and the associated commercial, legal and financial implications.

"Our experience suggests that whilst businesses recognise the importance of AI in a competitive market, many are yet to understand the risks involved, and in particular the increased risk of disputes," Gluyas says. "We recommend that businesses adopting AI technologies consider carefully the legal and commercial risks."

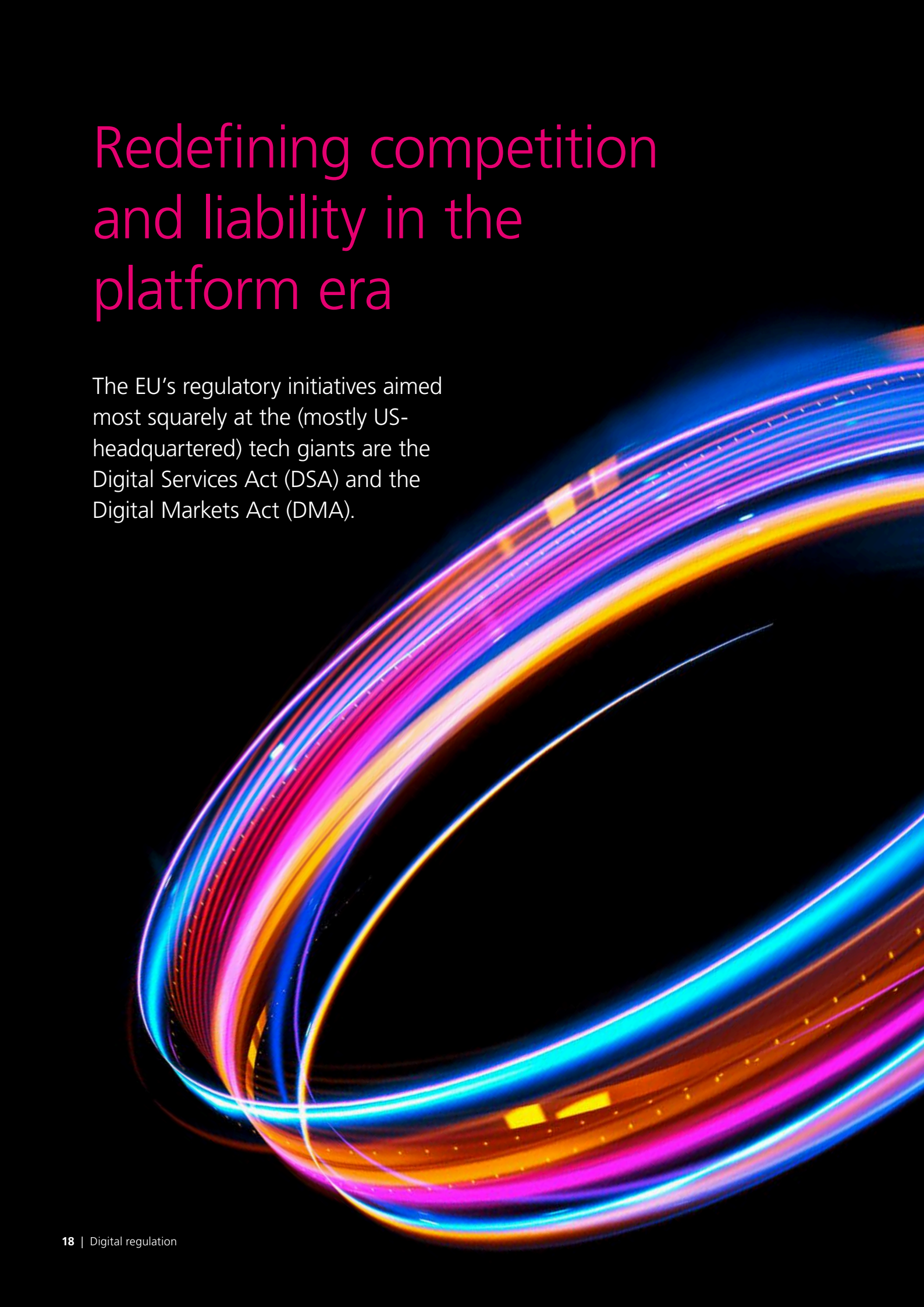
By being proactive in their engagement with AI regulation, businesses can greatly reduce the commercial and legal risks of AI adoption. If they haven't already done so, in-house legal should be drawing up plans for compliant AI adoption, so their business has the confidence to innovate ahead of its competitors.

Figure 6. The legal and compliance impact of AI regulation
% ranking in top three negative legal/compliance implications



Redefining competition and liability in the platform era

The EU's regulatory initiatives aimed most squarely at the (mostly US-headquartered) tech giants are the Digital Services Act (DSA) and the Digital Markets Act (DMA).



The DMA takes aim at the market power of so-called 'gatekeepers', companies that operate large digital platforms – whether they be operating systems, social networks, app stores, search engines or more besides – that have accumulated unprecedented competitive advantages and, as a result, serve as gateways between consumers and businesses. It includes measures to prevent them from applying unfair practices, obliging them to give third-party services fair treatment on their platforms.

In September 2023, the Commission issued an initial list of six nominated 'gatekeepers' to which these new rules apply: Alphabet (the parent company of Google), Amazon, Apple, ByteDance (TikTok's Chinese-headquartered parent), Meta and Microsoft.[11] The designated platforms include these companies' social networks, operating systems, browsers and marketplaces, and their messaging, search and video sharing services.

For other market players, the new rules for gatekeepers – which apply as of March 2024 – bring significant new opportunities, for example, through the opening of walled gardens and the diversification of app store competition.

The DSA, meanwhile, aims to tighten the regulation of illegal content and improve the transparency of user tracking and advertising. While the DSA includes some measures aimed at 'very large online platforms' – which include many of the DMA's designated services, plus Wikipedia, Alibaba's AliExpress, Zalando and Booking.com[12] – it is more universal than the DMA. Some of its measures apply to any online service provider with more than 50 employees and €10m in annual sales operating in the EU.

The UK's counterpart to the DMA – the Digital Markets, Competition and Consumer Bill[13] – has been making its way through the House of Commons. The bill seeks to offer a template for regulation of digital marketplaces and also includes provision for UK competition law reform, as well as an overhaul of consumer rights protection.

A universal opportunity

Given the breadth of commercial services that are delivered or marketed through digital platforms, it is unsurprising that 92% of businesses consider them to be somewhat or highly strategic, second only to cyber safety. This includes 42% who consider digital platforms to be 'highly strategically significant' today, with banking and finance respondents most likely to identify them as such (52%).

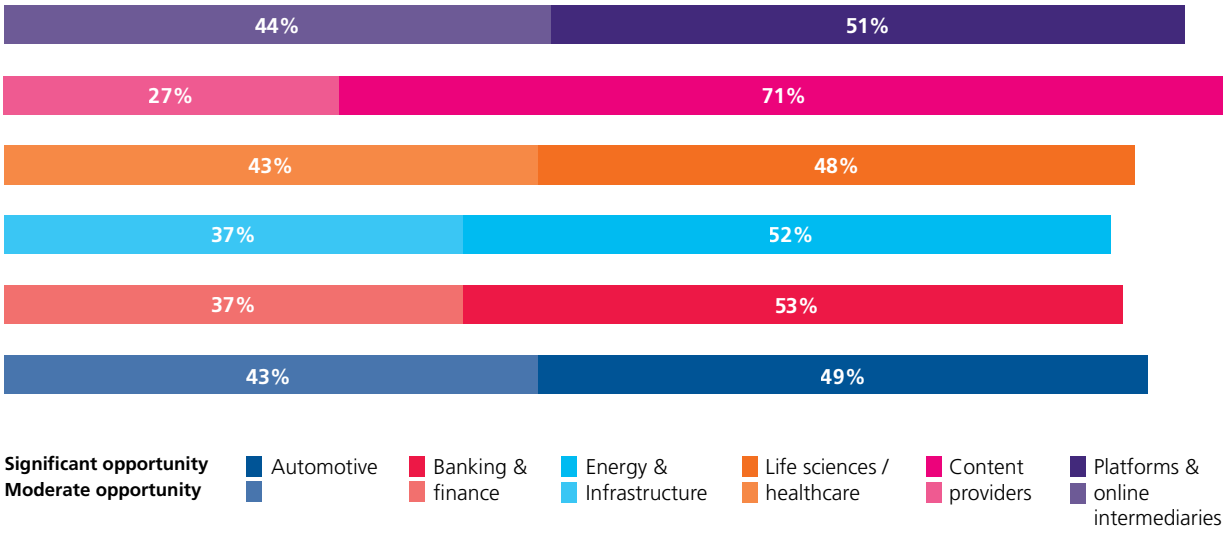
Respondents are largely positive about recent and upcoming regulation of these platforms in Europe, with 92% of respondents expecting a moderate or significant commercial opportunity to arise. The most widely anticipated opportunities are the ability to develop a long-term technology strategy, an increased ability to disrupt competitors, and enabling new products, services or business models such as introducing direct distribution through sideloading or opening own app stores on previously closed mobile operating systems.

"If we look only at the Apple App store, this means that a market of approximately USD $383m will now be open to third parties and new regulation will prevent any future platform fees from being imposed in most cases," says Pietro Fringuelli, co-head of the Global Technology, Media and Communications Group.

Content providers are especially positive about digital platform regulation, with 71% expecting 'significant opportunities' to arise (see **Figure 7**). App developers in particular may be among the chief beneficiaries of the DMA, as it prohibits gatekeepers from 'self-preferencing' – ie, giving privileged position to their own apps – or forcing developers to use bundled services, such as in-app payment systems.

Figure 7. The commercial opportunity in digital platform regulation

% of respondents who expect 'moderate' or 'significant' commercial opportunities from digital platform regulation



But more than eight out of ten respondents (80%) also view digital platform regulation as a source of commercial threats. This proportion was also highest among content providers (87%), who clearly anticipate major changes to their industry – both positive and negative.

The top-voted threats are reduced resilience/security of technology systems, reduced capacity for a long-term technology strategy, and a reduced ability to compete with Big Tech companies.

This last concern was most pronounced among respondents from the life sciences and healthcare and energy and infrastructure sectors. These companies might have digital platform ambitions of their own and may fear that regulation will diminish their ability to realise them.

Concern over legal and compliance obligations from digital platform regulation is also relatively high, with more than three-quarters of respondents (78%) expecting it to have moderate or significant legal or compliance implications, such as increased technology/operational costs to ensure compliance and increased complexity of contracts.

A particular compliance concern surrounding digital platform regulation is that it is not always obvious what constitutes a platform, especially in the context of large online services. In some cases, businesses may be operating as a platform without knowing it, exposing them to the risk of regulatory penalties.

After many years of discussion, Europe's regulatory regime for digital platforms is now falling into place. If in-house counsel have not yet assessed its impact on their organisations, now is the time to do so.

Towards energy platforms

Digital platforms are still emerging in the energy sector, but they have the potential to boost the efficiency and flexibility of energy markets by connecting supply and demand more effectively than today's grids.

"Within the energy sector, digital platforms are perceived as an opportunity to achieve sector priorities such as energy efficiency and ensuring security of supply, despite the volatility of renewable energy generation," explains Shaghayegh Smousavi, a partner at CMS specialising in the energy sector.

"Sharing data via digital platforms can lead to operational efficiencies," she adds. "Digital platforms can also be a tool to achieve decentralisation", allowing more energy to be generated closer to the point of consumption. While only a third of survey respondents from the energy sector say platforms are 'highly strategically significant' to their organisations today, nearly twice as many (63%) expect them to reach this significance in three years' time.

Digital platforms rely on data sharing – energy producers must share details of their output and capacity so the market can adjust. Energy respondents are the most likely to acknowledge the strategic significance of non-personal data (NPD): 16% say it is highly strategically significant today and 29% believe it will be in three years' time.

"NPD is viewed in the energy sector as a high potential source for new client-orientated services, especially among the larger utilities," says Smousavi. "They recognise that data is the new gold."

> "Within the energy sector, digital platforms are perceived as an opportunity to achieve sector priorities such as energy efficiency and ensuring security of supply."
>
> **Shaghayegh Smousavi**
> Partner, CMS

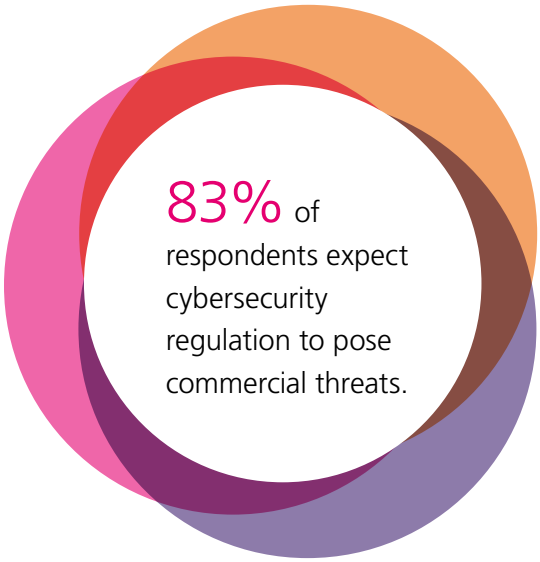
Safety in the digital economy

In December 2020, the European Commission unveiled a new cybersecurity strategy for the current decade. The evolution of cyber risks and advancing digitalisation of critical infrastructure called for an urgent update of its rules and standards, the Commission said at the time.[14]

Since then, digital threats to citizens, businesses and government organisations have only increased. Organisations have been tormented by a wave of ransomware attacks, while the war in Ukraine "has mobilised many hacktivists, cybercriminals and state-sponsored groups", according to the Commission.[15]

The strategy has led to new regulation, with new requirements for businesses on the horizon. In September 2022, the Commission presented a proposal for a new Cyber Resilience Act,[16] which would introduce "mandatory cybersecurity requirements for products with digital elements", including any software or connected hardware products.

Then, in January 2023, the EU adopted its revised Networks and Information Security Directive (NIS2).[17] NIS2 significantly expands the scope of the rules to encompass digital and managed service providers and introduces new incident reporting requirements for regulated bodies, among other new obligations. EU member states are required to implement NIS2 into law by October 2024. The UK government, meanwhile, is now in consultation over its adoption of the NIS2 regulations.[18]



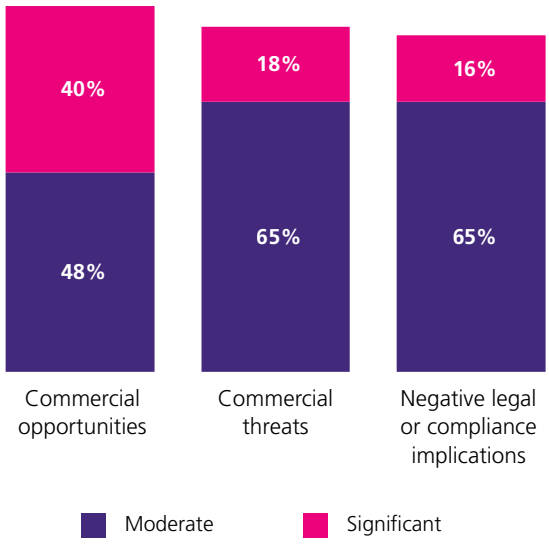
Cyber safety regulations: a double-edged sword

Although cyber safety regulation is primarily focused on eliminating risk, nearly nine out of ten respondents (87%) believe that these recent and upcoming rules offer commercial opportunities (see **Figure 8**). This is especially true of content providers and respondents in the banking and finance sector.

The greatest commercial opportunity from cyber safety regulation, respondents believe, is improved access to data and analytics. There are many ways in which cyber safety regulation might increase this access. For example, if the Cyber Resilience Act succeeds in making digital products secure, consumers and businesses may be more inclined to use them, offering greater opportunities for data collection and use.

But this regulation also poses commercial threats, according to 83% of respondents – more than any other area of digital regulation included in the study – including 18% who expect these threats to be significant. Platform providers are the most alert to this, with 91% expecting commercial threats to arise from cyber safety regulation, while the automotive sector is the least concerned (68%).

Figure 8. Opportunities and threats from cyber safety regulation
% of respondents expecting each from AI regulation



Increased technology adoption costs are the most widely anticipated threat. Respondents expect increased controls to require investment in technology and personnel, this demonstrates. This is followed by a reduced ability to innovate, suggesting a fear that new security rules will make it harder to develop and launch new products and processes (although this perhaps overlooks the crucial role of trust in user adoption of new technology innovations).

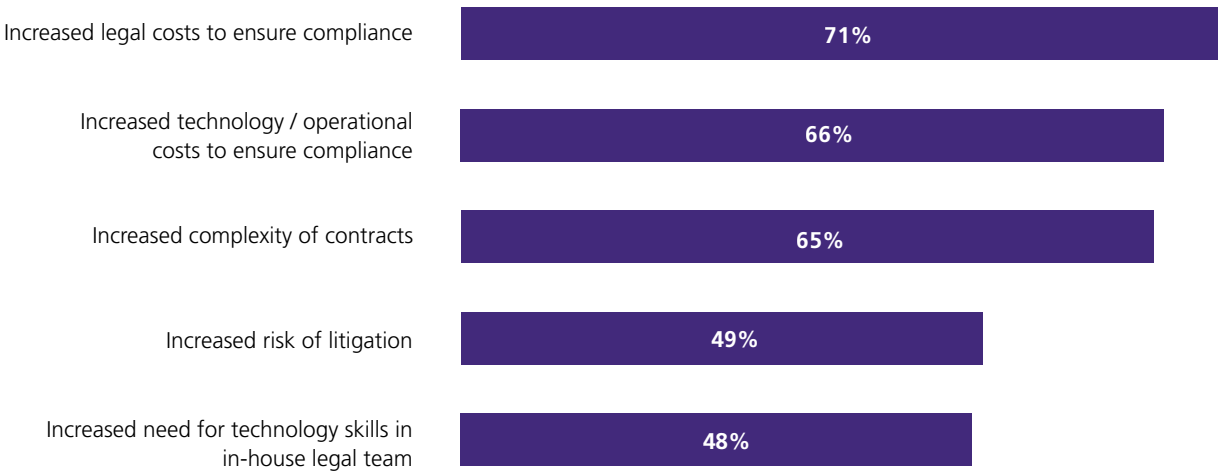
More than eight out of ten respondents also expect cyber safety regulation to have negative legal implications. Increased legal costs to ensure compliance are again the most widely anticipated legal implication, followed by increased technology costs (see **Figure 9**)

The Commission estimates that the aggregated compliance costs of the Cyber Resilience Act will be €29bn, against a total market value of qualifying products of €1.4trn.[19] As a result, it warns, consumers and citizens may face higher prices for products with digital elements.

Businesses stand to gain a lot from safer digital economy in Europe. The annual, global cost of cybercrime was an estimated €5.5trn in 2020, twice the amount in 2015.[20] But every organisation has a role to play in improving cyber safety, and businesses understand that the EU's proposed regulatory approach will incur costs.

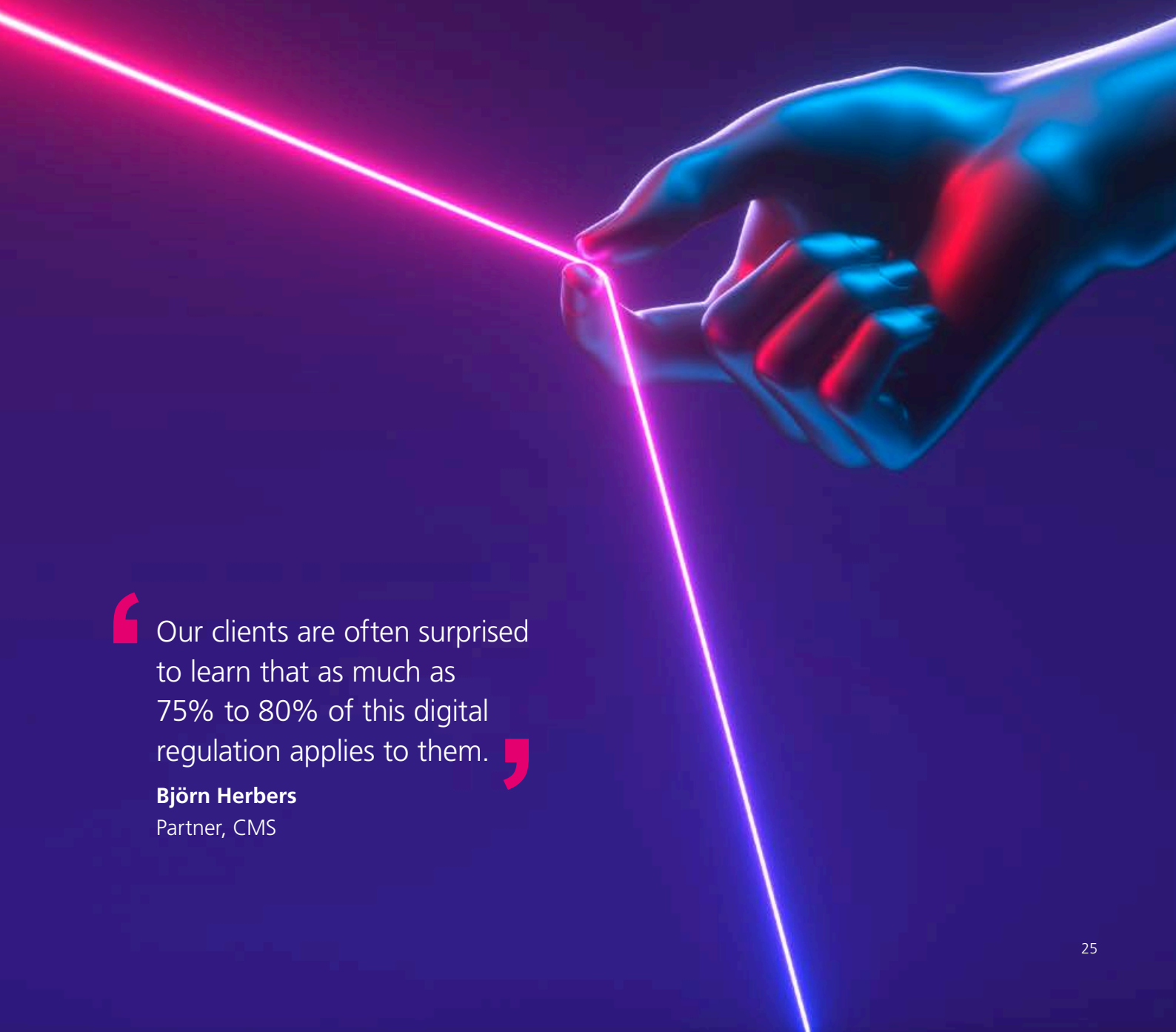
Those companies that make a plan for compliance with cyber safety regulations, and incorporate it into the digital transformation strategies, will be better placed to accommodate those costs and capture opportunities to offset them.

Figure 9. The legal/compliance implications of cyber safety regulation
% of respondents ranking in top three negative legal/compliance implications



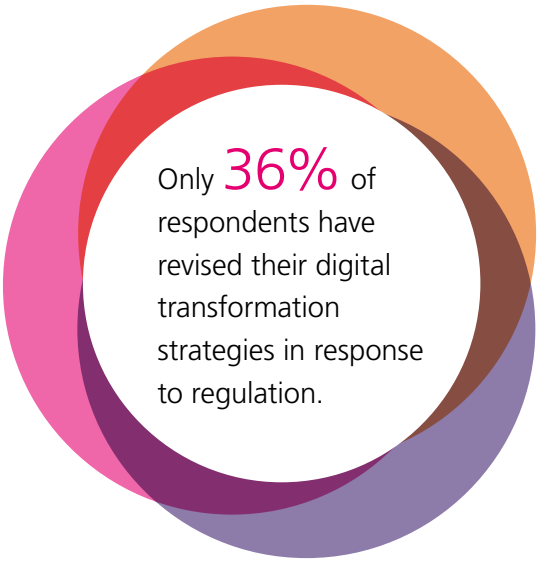
Robust strategies for navigating digital regulation

As we've seen, the current wave of digital regulation in Europe offers businesses ample opportunities if they prepare effectively. If they don't, there are just as many commercial threats and negative legal implications on the road ahead.



> Our clients are often surprised to learn that as much as 75% to 80% of this digital regulation applies to them.

Björn Herbers
Partner, CMS



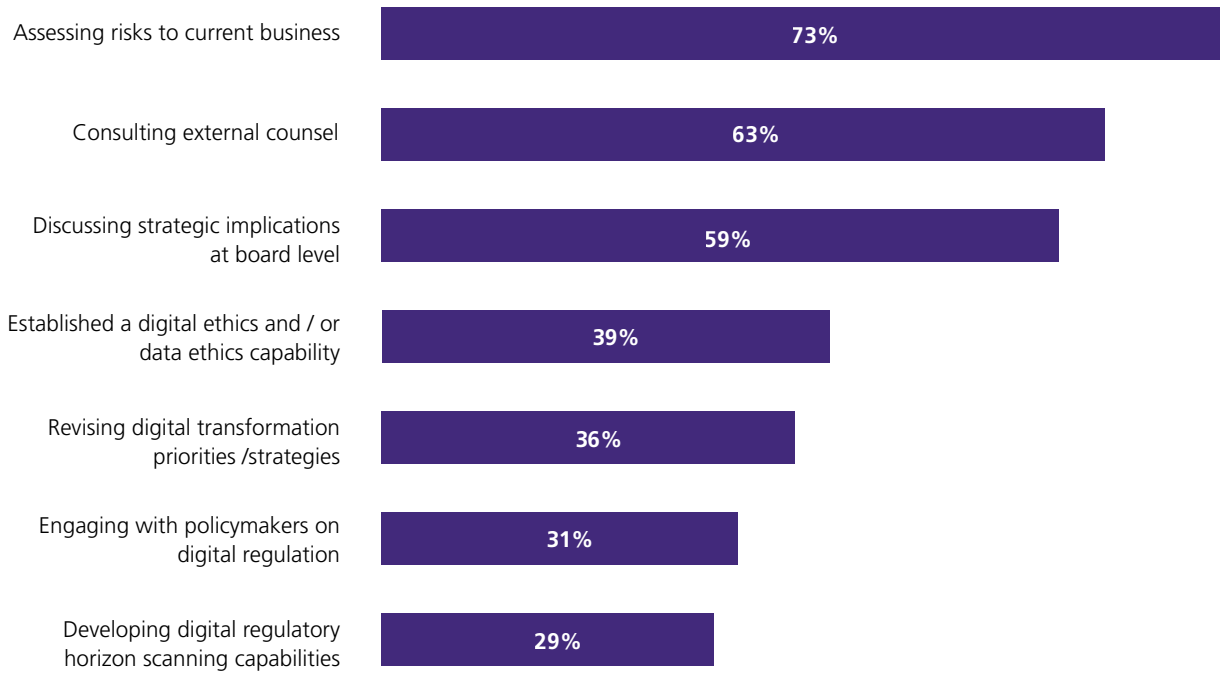
Survey respondents are cautiously confident they are up to the challenge. As we have seen, more than seven out of ten (71%) believe their organisation is 'better prepared for the impact of recent and upcoming digital regulation than its competitors', although only 11% 'strongly' agree with this statement.

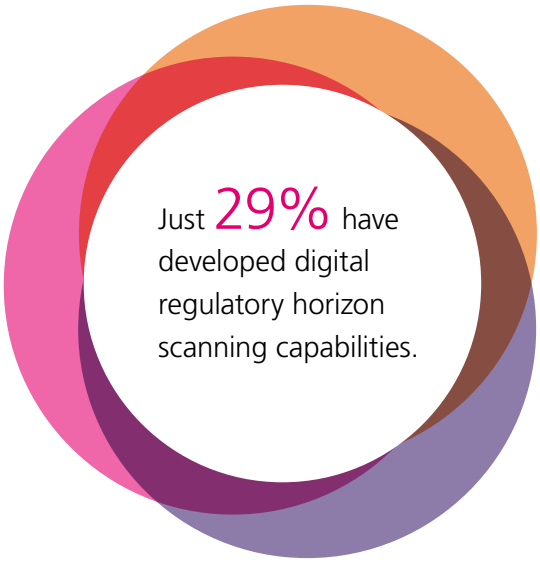
For some, this confidence may be misplaced. "Our clients are often surprised to learn that as much as 75% to 80% of this digital regulation applies to them," says Herbers.

Nevertheless, digital regulation is at least on the agenda for the majority of companies we surveyed. Nearly three quarters (73%) have assessed the risks it poses to their current business, making this the most widely adopted response. Sixty-three percent have consulted external counsel on digital regulation and 59% have discussed the strategic implications at board level (see **Figure 10**).

However, concrete actions are less widespread. Only 36% have revised their digital transformation priorities/strategies, for example, a figure at odds with the paradigmatic shift that some of these regulations will bring about in digital markets.

Figure 10. How businesses have responded to digital regulation
% of respondents that have adopted in response to digital regulation





Slightly more (39%) have hired in-house legal staff with specialist expertise. This strategy is especially common among respondents from the energy and infrastructure (47%) and automotive (45%) sectors.

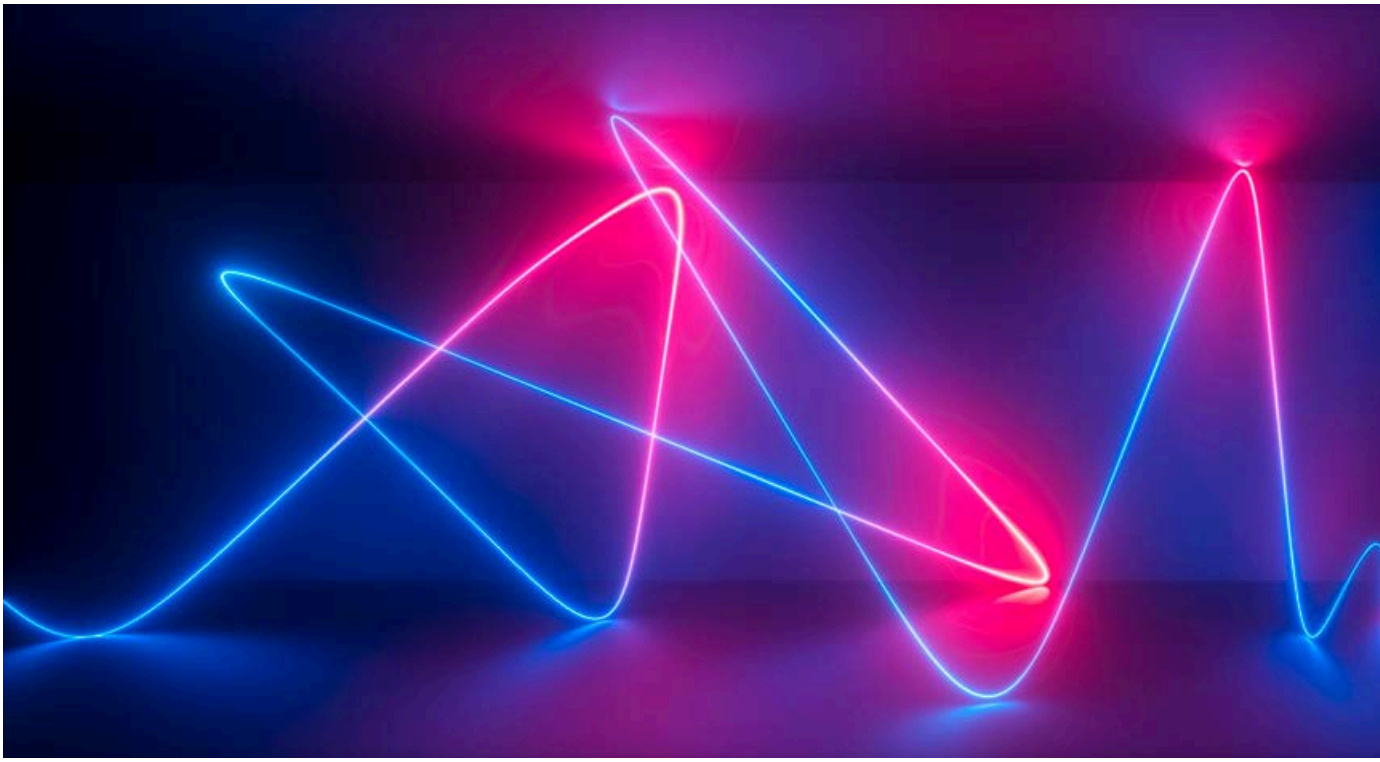
And just 29% have developed digital regulatory horizon scanning capabilities. Understanding what regulation is on its way and its implications for the business is a crucial part of an in-house legal team's contribution. When it comes to technology, this foresight can give organisations greater confidence in their strategic investments.

For this reason, CMS has developed a digital regulation tracker tool,[21] providing insights and detail of recent and upcoming changes to regulation and law, to help clients navigate the changing landscape.

For Smousavi, digital regulation is one of many areas in which frequent and far-reaching rule changes are challenging companies' ability to keep pace. "The challenge that the clients face is the steady load of new regulation, not only digital regulation, but also ESG, reporting matters and more," she explains. "Maintaining a reliable monitoring and controlling system, given the mass of new regulation, has become more of a challenge for company leaders."

As a result, companies are now looking for help from external advisers to outsource their compliance monitoring. "Often, they recognise that they won't have the personal capacity to handle everything on their own given the increasing number of regulations to comply with."

What companies cannot outsource is the obligation to ensure they are ready for the oncoming wave of digital regulation, its opportunities, its threats and its legal implications. Some businesses have already engaged with this regulation in a concerted and sophisticated way. Others must start now if they want to grasp the advantage that lies in digital regulation.



Conclusion

Policymakers – and in particular those in the EU – are creating a new framework for the digital economy. The regulations should be understood as a comprehensive legal framework for an entire ecosystem, not as individual regulations.

The volume of recent and upcoming digital regulation in Europe may appear to be overwhelming, but there is no need for undue concern. Careful and strategic preparation will ensure that businesses can predict and mitigate compliance costs, minimise risks and, crucially, identify and capture the opportunities that this regulation presents.

This landscape will provide the foundations for new commercial opportunities, which businesses cannot afford to ignore. The new data-centric economy requires substantial thought and planning. Waiting to see the impact is not an option.

Every global business operating with connections in Europe will be affected by this new framework. It is essential that regulation becomes central to their digital strategy and decision-making for the future. If they succeed in this, and act on plans without delay, we will see businesses truly fit for the digital age.

Ready to take action?

Contact the team today on **Digihub@cmslegal.com**

Endnotes

To return to the footnote reference, click on a number.

1 https://digital-strategy.ec.europa.eu/en/news/data-act-businesses-and-citizens-favour-fair-data-economy

2 https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

3 https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

4 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

5 https://digital-markets-act.ec.europa.eu/index_en

6 https://bills.parliament.uk/bills/3453

7 https://www.gov.uk/guidance/national-data-strategy

8 https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en

9 https://www.gov.uk/government/news/prime-minister-launches-new-ai-safety-institute

10 https://www.commerce.gov/news/press-releases/2023/11/direction-president-biden-department-commerce-establish-us-artificial

11 https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328

12 https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops

13 https://bills.parliament.uk/bills/3453

14 https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

15 https://www.consilium.europa.eu/en/infographics/cyber-threats-eu/

16 https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

17 https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

18 https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/proposal-for-legislation-to-improve-the-uks-cyber-resilience

19 https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment

20 https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet

21 https://cms.law/en/int/publication/digihub

CMS Digital Regulation Hub

The **CMS Digital Regulation Hub** is home to our **Digital Regulation Tracker Tool**, providing an **overview of the key regulatory instruments for area of law, sectors and business activities** which are critical for decision makers as they adapt to the increasingly digital landscape.

In addition to this unique tool, **we explore the impact** this tsunami of regulation is having **for businesses across a variety of industries and how GCs can ride the waves to stay ahead of the curve**. Our latest report illustrates the key findings across Platforms, Content providers, Life Sciences & Healthcare, Energy & Infrastructure, Banking & Finance and Automotive industries.

To discuss how to cope with the challenges of Digital Regulations and to explore the opportunities for your business, **please contact one of our International experts**.

Ready to take action?

Contact the team today on **Digihub@cmslegal.com**

About us

Staff

> 9,000

59,8% female

Lawyers

> 5,800

51,5% female

62 new partners in 2022, taking the total to over 1,250

76 cities

45 countries

19 Practice and Sector Groups working across offices

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

---

cms.law

2311-0180644-5