Bird & Bird

One firm.
Your firm.

Tech & Comms Challenges, Opportunities and Predictions 2024

Introduction

In the ever-changing landscape of technology, generative AI is seamlessly integrating itself into daily applications, steering the digital revolution with unprecedented speed, while quantum computing adds a new dimension to computational possibilities and drives new innovations in cybersecurity.

Recognizing the importance of environmental, social, and governance (ESG) values, companies are embracing their commitment to sustainability, resulting in a surge of investments and innovative initiatives aimed at achieving net-zero commitments. Beyond profit margins, companies now prioritize responsible business practices that contribute positively to the planet and society.

The business landscape globally is becoming increasingly challenging in terms of cybersecurity. We are witnessing a trend of increasing regulation in this area, with EU legislators having completed their work on the NIS2 and CER Directives - two key cybersecurity related legislation that came into force in 2023.

With the rise of technological advancements, legislators worldwide are considering whether to modify existing frameworks or establish new ones to govern the development and use of these technologies. While significant initial measures were initiated in 2023, we expect an increase in regulation and its implementation in 2024.

Across the globe, our clients consistently identify nine areas that significantly impact their business: Artificial Intelligence; Cybersecurity; Data; Cloud, IoT & Edge Computing; Quantum Computing; ESG; 5G & 6G; Web3, Metaverse; and NFTs, Tokens & Blockchain.

This 2024 report gathers predictions and observations from our global Tech & Comms lawyers. It looks at these nine specific areas and discusses the expected developments in the coming year.

Click here to access our Technology and Communications webpage

Ronald Hendrikx, *Partner*
+44 (0)20 7415 6000
ronald.hendrikx@twobirds.com

Marjolein Geus, *Partner*
+31 (0)70 353 8800
marjolein.geus@twobirds.com

Fabian Niemann, *Partner*
+49 (0)211 2005 6000
fabian.niemann@twobirds.com

Ted Chwu, *Partner*
+852 2248 6000
ted.chwu@twobirds.com

Cloud & IoT

READ MORE →

Cybersecurity

READ MORE →

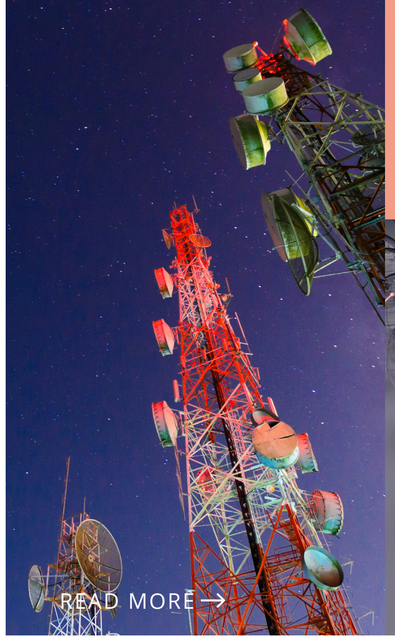
Metaverse

READ MORE →

Data

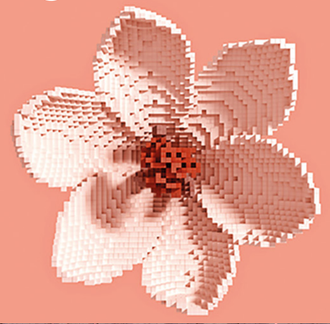
READ MORE →

5G/6G



READ MORE →

Artificial Intelligence

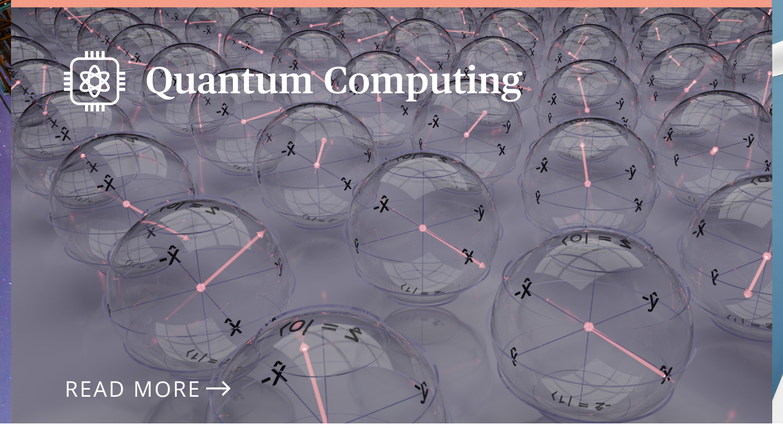


READ MORE →

ESG

READ MORE →

Quantum Computing

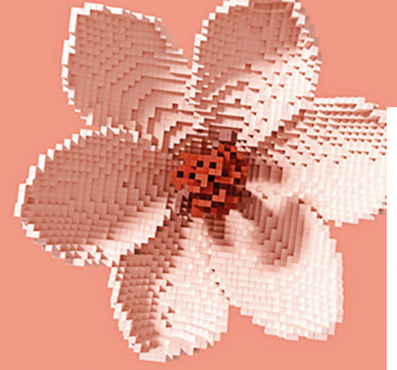


READ MORE →

NFTs, Tokens & Blockchain

READ MORE →

Artificial Intelligence

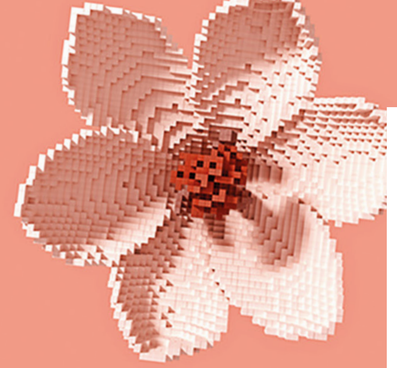


Copyright implications of generative AI

In 2016, the Next Rembrandt project focussed our attention on the possibility of creativity without a (human) creator. While IP lawyers have been debating whether copyright can subsist in works generated using AI ever since, until very recently the question was more academic than commercially important for most of us. This is changing as we move into 2024. If your software developers can double their productivity using generative AI, it seems like a no-brainier to use it. But what if there's a risk that the software you develop will no longer be protected by copyright? This risk isn't limited to software and is going to flow through supply chains, e.g. should I let my marketing agency create campaigns using generative AI? Whichever industry you operate in, 2024 is likely to be the year you start looking at how this (once academic) issue plays out in your polices and contracts.

Toby Bond
Partner
UK

Artificial Intelligence

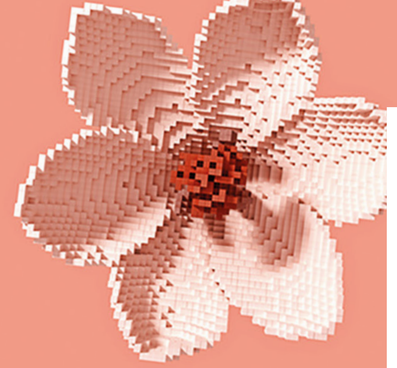


Can generative AI created works be protected?

AI will no doubt be a hot IP topic in Denmark in 2024, not least in connection with generative AI in creative processes. One main IP-related AI issue arising is that copyright protection requires that the work is a human creation, leaving it uncertain whether, and to what extent a work created through generative AI can be legally protected. Another main issue is that the training of AI through text and data mining of existing works might violate copyrights in such works, if the training of the AI is carried out without permission from the owners of the copyright. Finally, as a third IP-related AI main issue, it should be mentioned that contents created through AI might violate copyright and other IP rights in existing content. Thus, legal disputes are likely to emerge in 2024 and onwards related to such issues. In 2023, Denmark saw the belated implementation of the DSM Directive into the Danish Copyright Act. Legal disputes are likely to emerge in 2024 and onwards, concerning the interpretation of the various new provisions of the Copyright Act inserted as implementation measures, not least the provisions permitting text and data mining under certain circumstances.

Mogens Dyhr Vestergaard
Senior Counsel
Denmark

Artificial Intelligence

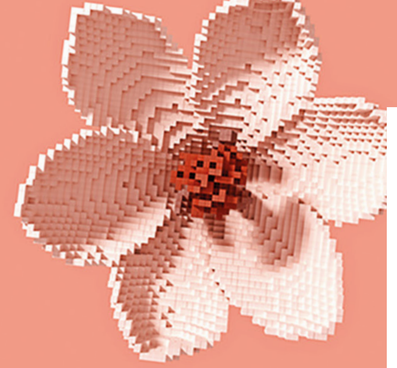


AI and extra-territorial reach

AI developers, distributors and downstream deployers will need to start their compliance planning in earnest for the incoming EU Artificial Intelligence Act. As the first “hard law” attempt to regulate the use of AI systems, in particular foundation models, the AI Act is likely to trigger the “Brussels effect”. This is a form of regulatory globalisation whereby the EU externalises its laws outside its own borders. Apart from the impact on regulators in other jurisdictions, companies operating globally are likely to feel obliged to apply the new rules in the AI Act across all their markets, or face accusations that they offer less protection to consumers and businesses outside the EU.

Francine Cunningham
Regulatory And Public Affairs Director
Belgium and Ireland

Artificial Intelligence



AI liability

2023 was the year that AI was introduced to the public on a large scale. In 2024, AI systems will extend further into the consumer and business space, directly impacting more individuals. This also heightens questions around what should happen when something goes wrong.

Attention will shift towards the European Union's liability framework for AI, which has so far (understandably) been overshadowed by the AI Act. Many are not aware that the EU is working on a proposal for a revision of the Directive on liability for defective products ("Product Liability Directive") and a proposal for a Directive on adapting non-contractual civil liability rules to AI ("AI Liability Directive"). These legislative pieces will likely bring significant changes for product and non-contractual liability, for companies which include manufacturing, importing, distributing, selling, operating, integrating or modifying AI systems and AI-enabled goods. Envisage the introduction of frameworks for claiming disclosure of evidence from defendants and lightening the burden of proof for claimants with presumptions of defectiveness/fault/causality.

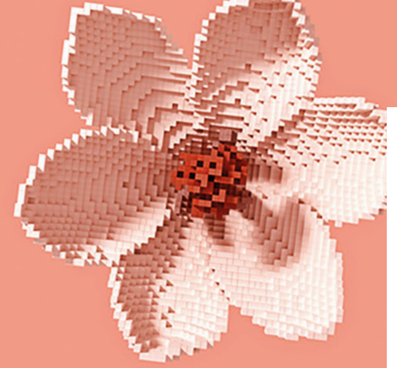
Much of the discussion around AI liability will be the expectations placed on companies, a currently challenging question. Part of the answer will be fought out in (what is expected to be) the wrapping up the details for the AI Act. The AI Act will provide an extensive set of norms for both system manufacturers and deployers. Failure to meet these norms may lead not only to regulatory consequences but also civil liability within the AI value chain and/or towards affected individuals. In 2024, there will be an emergence of AI standards - technical, organizational and ethical – in addition to implementation of said standards and (we expect) serious contract negotiations efforts.

Shima Abbady

Associate

Netherlands

Artificial Intelligence

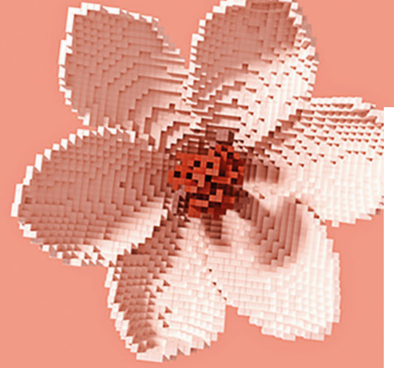


Contracting for AI

With recent advances in AI, 2023 saw businesses seeking to embrace the technology, putting the guardrails in place for their internal testing and hackathons, working out how they can best deploy it. Following these efforts, we expect in the next 12 months to see more and more business move from the “evaluate and test” phase to full deployment. This inevitably will require contracts to be entered into with the suppliers of the AI systems, and for those contracting parties to consider the particular issues that arise when contracting for AI systems. Parties will have to grapple with issues such as whether they need to limit how a system can be used, in order to comply with emerging legislation, how to approach acceptance testing in order to minimise the risk of hallucinations or remove bias, and how to legislate for ownership in the outputs of a system when there may be questions of whether the outputs may contain intellectual property rights eligible for ownership.

Will Bryson
Senior Associate
UK

Artificial Intelligence



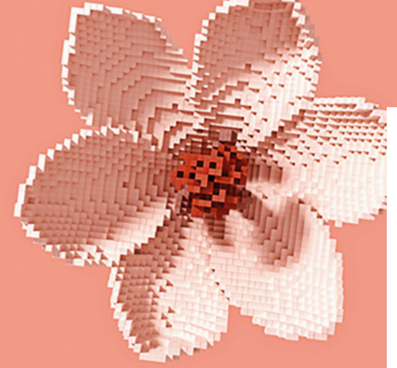
Human centric AI

The EU Artificial Intelligence Act is taking shape alongside several new initiatives around the globe. The EU has continued with its human centric approach to AI, focusing on human intervention, human review and human oversight. In particular, we see a continued push for the 'right to explanation' with specific texts taking shape in the discussions within the EU institutions. However, as great as the right to explanation is, the black box problem persists and we are likely to see a development of explanation models straying away from the current approximations of explanations of AI to an increased use of counterfactuals in order to meet the obligations under a potential right to explanation while facing the reality of AI. One thing is for certain, AI is top-of-mind and managing the right to explanation is one of several issues facing businesses.

Mattias Lindberg
Partner
Sweden

Hans Kalderén
Associate
Sweden

Artificial Intelligence

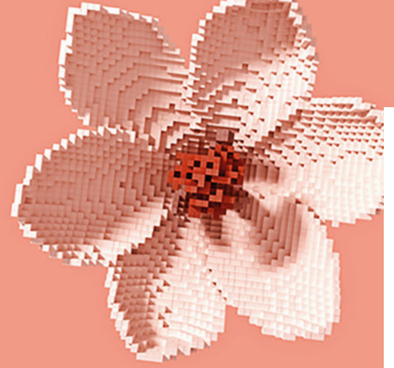


AI in employment

Perhaps unsurprisingly, AI will continue to dominate the discourse in an employment context during 2024 as companies (particularly within the tech sector, which was an early adopter of these tools) not only use AI-powered applications to make decisions regarding their workforce, for example with respect to recruitment and performance management, but also where employees are increasingly using generative AI in the performance of their duties. The UK currently sits behind the EU in terms of the regulation of AI, however with a draft 'AI and Employment' Bill which seeks to address workers' rights in the context of AI set to be published in 2024, in addition to a prospective change in government which could herald a shift towards a more protectionist attitude, we expect that 2024 will be the year of increased regulation in this area.

Furat Ashraf
Partner
UK

Artificial Intelligence



AI & life sciences

We can already see some surgeons operating with virtual reality headsets that display X-rays of patients in their field of vision to help them during an operation. The number of innovations in this field is only set to multiply. Now that the AI Act has reached political agreement at the end of 2023, it is clear that the growing power of AI and its increasing penetration of the world of healthcare is undoubtedly a challenge for the future and one that will have to be met over several years. This interpenetration between AI and the healthcare sector means that any project developer in this field will have to take into account a wide range of regulations, in particular health regulatory, health law and personal data protection law. In the healthcare sector, AI systems are now classified as high-risk systems, which means that specific requirements will have to be applied, particularly with regard to the data sets used and the transparency and information provided to users.

The life science sector will also see an increase in fund-raising, which will be essential to support project leaders and enable them to transform their business and comply with current and future legal requirements.

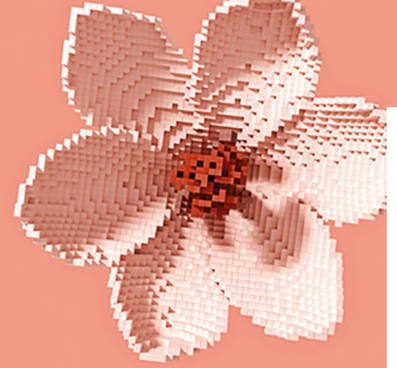
The world of life science is in the midst of the AI revolution, and new standards are being introduced in this area.

Emmanuelle Porte
Partner
France

Caroline Arrighi-Savoie
Associate
France

Oriane Zubcevic
Associate
France

Artificial Intelligence



AI & drug development

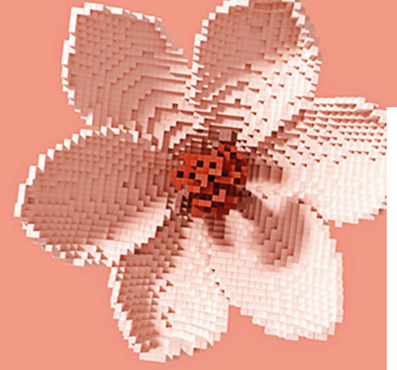
AI has been making significant impact in the area of drug development and will continue to do so. Successful examples of the use of AI in various stages of drug development are identification and validation of potential drug targets, the prediction of efficacy and safety and as a tool used for clinical trial design and patient selection. Last year, the regulators have stepped in too, as both the EMA and FDA have started to take position with regard to the use of AI in the development of new medications. The WHO has also published their point of view on the use of AI for health.

Furthermore, the European Commission has published their proposal for the reform of the EU pharmaceutical legislation, which also largely focusing on fostering (technological) innovation, also referring to the use of AI. Due to the many groundbreaking ways of using AI in drug development and the fact that the regulatory landscape is beginning to take shape, the role of AI in healthcare will only become more and more important and we will see a lot of developments in this area in the next year.

Hester Borgers
Associate
Netherlands

Christian Lindenthal
Partner
Germany

Artificial Intelligence

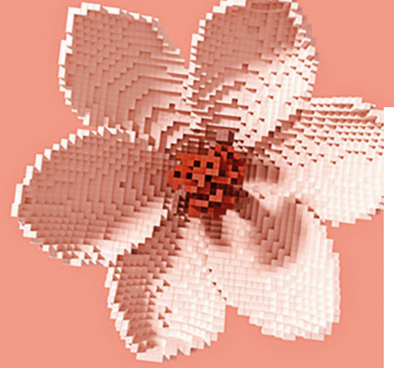


Shaping AI regulation

In 2024 more countries will continue to shape the regulation of AI. While most agree that legal guardrails around AI are necessary to contain the technology's limitations, regulation must also not compromise AI's potential economic value. However, this is proving difficult in practice, for example in disputes over the definition of AI; the riskiness of different AI systems; and the appropriateness of specific obligations. The key players (US, China, EU and UK) are taking different approaches, with the US relying on voluntary commitments, the EU about to adopt the cross-sector AI Act, China having adopted most of the AI legislation so far, and the UK with its pro-innovation regulatory approach to AI. It will be exciting to see how this develops and which countries take the lead in the global AI innovation race.

Nils Lölfing
Counsel
Germany

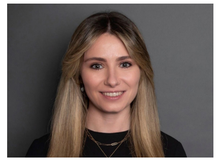
Artificial Intelligence



Generative AI and children

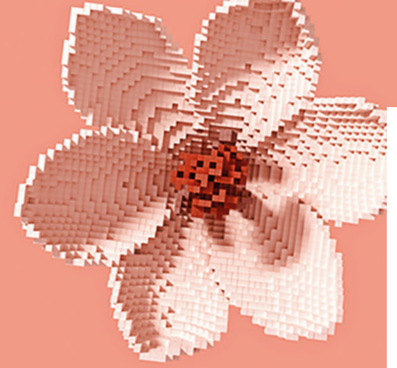
The meteoric rise of high-profile generative AI-based apps and services in 2023 has shown how this technology can make our lives easier by completing tedious tasks, offering novel use cases and making life more fun. This has been true for children as much as adults and preliminary research indicates that children may potentially be more prolific adopters of generative AI technologies than adults, using it for homework, to choose their outfits and for entertainment amongst many other uses. At the same time, 2023 saw data protection regulators raising concerns about the potential negative impacts of this technology for the privacy and safety of children, especially younger users, with pockets of enforcement action taken across Europe against different services. We expect that this focus will continue in 2024 and that age assurance and age verification will be a major aspect of this scrutiny with regulators examining whether providers of generative AI services with a minimum user age limit (usually 13 years) are taking effective measures to prevent underage users from accessing their tools.

Anna Morgan
Partner
Ireland



Shauna Joyce
Associate
Ireland

Artificial Intelligence

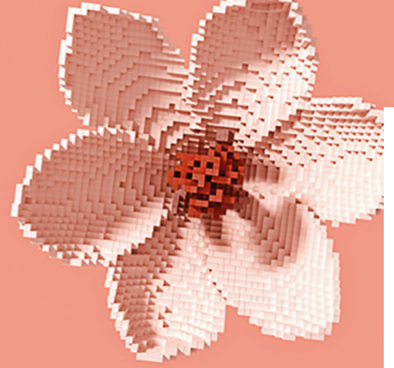


Adoption of generative AI

Generative AI is predicted to permeate everyday applications and processes, beginning with tasks such as drafting texts. This advancement in technology is expected to revolutionize customer service chats, making them more efficient and interactive. The impact will be high even on lower skilled workers who tend to profit most from generative AI support. As this tech continues to evolve, it is likely that we will witness its first impact on headcount, especially in sectors like customer service. It will be essential to prepare for the transition by training of staff and investing in technology.

Tobias Bräutigam
Partner
Finland

Artificial Intelligence



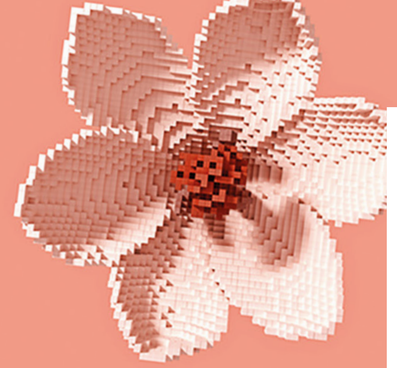
GCC governments harnessing AI

Gulf Cooperation Council (GCC) governments have ambitious plans to position themselves at the forefront of the digital revolution. They will harness AI to drive economic growth and enhance competitive advantages in both public and private sectors. For example, NEOM, the $500 billion smart megacity envisioned for northwest Saudi Arabia, has already planned for an unprecedented activation of AI and IoT technologies. GCC countries need to quickly start building the necessary foundations to ensure their governments can process, store and transfer large amounts of data. From a privacy perspective, we note a continued trend towards new data protection regulations and laws released in the region. For example, the recent publication of the Implementing Regulations to the Kingdom of Saudi Arabia's Personal Data Protection Law and the United Arab Emirates Executive Regulations to the federal data protection law that are expected next year. As a result of these efforts and provided the key foundations are put in place, GCC countries have a realistic opportunity to play a leading role in the 'global digital race'.

Nona Keyhani
Associate
UAE

Simon Shooter
Partner
UK

Artificial Intelligence

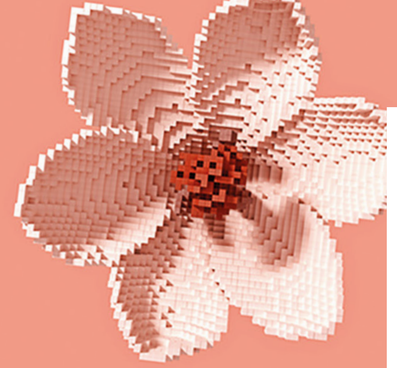


New UK legal framework for self-driving vehicles

It has long been recognised that a new legal framework is required in the UK to regulate the use of automated vehicles. Automated vehicles are those that are capable of driving themselves without control or monitoring by a human individual for at least part of a journey, i.e. control by autonomous self-driving systems or technologies. Their use has significant legal consequences, not least in that a human driver should no longer be the main focus of accountability for safety and liability. In that context, following an approximate four-year review process by the Law Commission, the UK Government has published an Automated Vehicles Bill which will be making its way through the UK Parliament during 2024. In its current form, the Bill: (a) includes a safety threshold for driverless vehicles, so that standards can be enforced according to technical assessment; and (b) specifies that automated vehicles will be subjected to an authorisation system, under which the organization responsible and liable for the autonomous/self-driving system will be identified. The Bill is expected to unleash the potential growth of the self-driving technology sector (in the region of circa £42 billion by 2035).

Russell Williamson
Senior Associate
UK

Artificial Intelligence

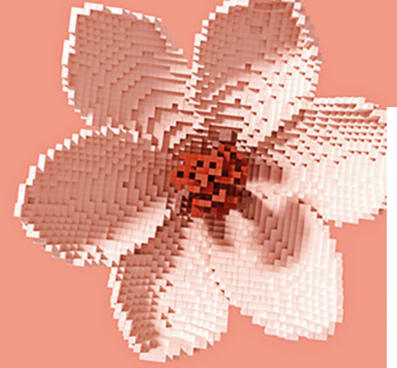


Liability damages caused by AI systems

It can be expected that, once the AI Act is passed (possibly by beginning of the year), the legislative process for the legislative process for regulating AI will continue. This aims to introduce new rules regarding liability for damages caused by AI systems. The new rules are likely to be covered by two new Directives (as proposed by the European Commission) aimed at adapting the existing legislation to the particular features of AI, by (i) introducing harmonization of certain aspects of national fault-based liability rules, and (ii) amend the existing harmonized legislation on defective products.

Pablo Berenguer
Partner
Spain

Artificial Intelligence



Security risks using AI

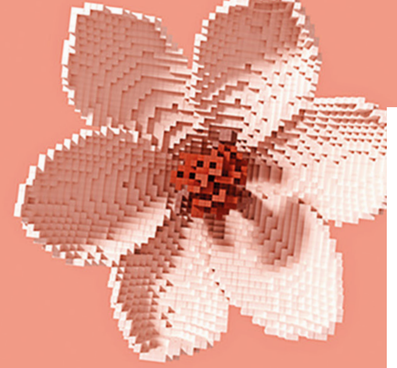
In 2023, generative AI emerged as one of the most rapidly adopted technologies in history. It is the most significant technological advancement in decades and is, and will continue to, transform industries, jobs and productivity.

With this explosive growth of generative AI over the past year, security risks have begun to emerge: hackers can make generative AI tools behave in unintended ways through indirect prompt injection attacks; and data poisoning of the data sets that train large language models can cause serious damage to AI models that ingest that data.

In 2024, there is likely to be a focus on, and proliferation of, security protection mechanisms for generative AI tools. Whilst AI itself is still developing rapidly, tech companies will be working hard to mitigate these security risks. From a commercial law perspective, we are also addressing any such security risks through contractual mechanisms in contracts involving AI.

Kate Deniston
Professional Support Lawyer
UK

Artificial Intelligence



Generative AI in legal services

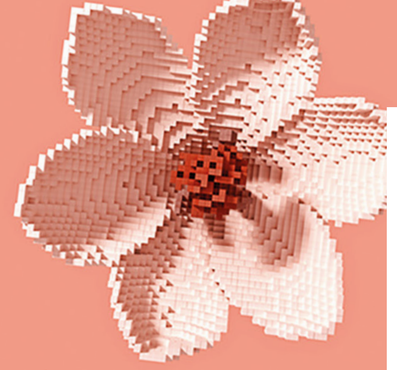
Generative AI systems will have a significant impact on legal services. It will not replace lawyers or even significantly reduce their time spent on core legal tasks, but it will inspire new ways of working for lawyers.

Generative AI will be useful for creating and perfecting many legal deliverables, such as templates and other knowledge-based resources, and also for retrieving data from past advice so that lawyers can rely not only on their memory and experience.

Generative AI will also transform the mass review of legal documents, allowing lawyers to focus on the key points rather than the text itself, especially by access to quick summaries of lengthy texts.

Tomasz Zalewski
Partner
Poland

Artificial Intelligence

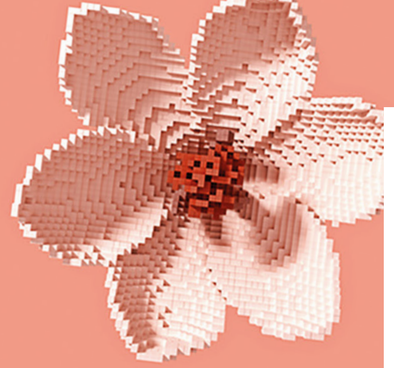


Tools in software code development

Polish companies provide significant amounts of software development services to foreign tech companies (body-leasing, nearshoring and BOTT setups). The question of the IPR / copyrights status of a source code developed with the assistance of generative AI tools may be one of the most discussed and important legal issues in the upcoming year.

Kuba Ruiz
Senior Counsel
Poland

Artificial Intelligence



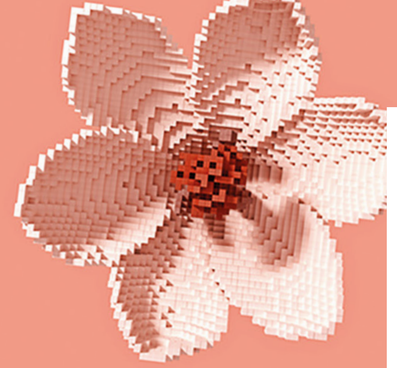
AI liability and consumer protection

In 2024, AI and the product liability rules will be a hot topic due to the EU's evolving regulatory stance on AI. The EU's proposed changes, aimed at modernising current products liability rules and introducing an AI-specific Liability Directive, will drastically change the landscape of consumer protection and business exposure. This will balance consumer safety with innovation, but could also increase legal claims against tech companies. The new rules are intended to harmonise national liability laws for AI and products incorporating AI systems, making compensation easier for AI-related damages. As AI systems become more prevalent, these changes will impact a wide range of sectors, sparking widespread discussion and debate.

Pawel Lipski
Partner
Poland

Monika Hughes
Counsel
Poland

Artificial Intelligence

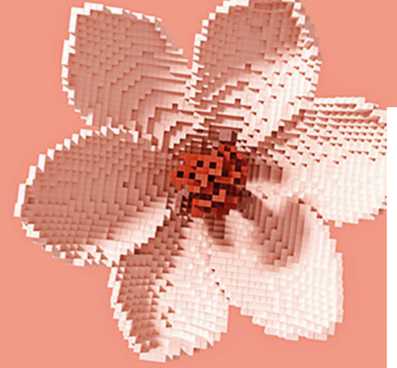


EU AI regulation

The EU AI Regulation is expected to be adopted in late 2023 or early 2024. Its approval will be a milestone both for providers and users in EU member states and for providers and users in third states. The regulation will apply not only to providers placing AI on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country, but also to providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union. The regulation will be applicable two years after it has entered into force, without doubt, its content will be taken into account from the moment of its approval, including its interrelation with data protection and intellectual property regulations, since it will set the rules of the game for the development of AI systems.

Celia Bouzas
Senior Associate
Spain

Artificial Intelligence

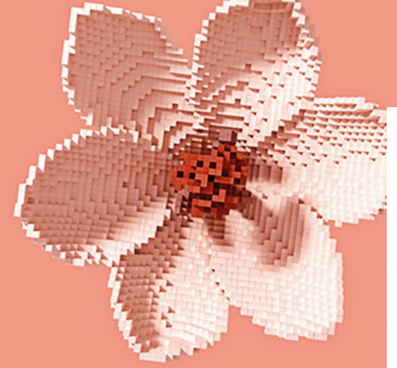


Spanish AI regulation

The use of AI in the European Union will be regulated by new regulations (at the moment, they are mere proposals). Spain has adopted certain laws on AI and, specifically, has approved the establishment of the first Supervisory Agency for Artificial Intelligence in the European Union. All of this clearly shows that Spain understands that AI will be one of the fields that generates great commercial activity. The establishment of the Spanish Supervisory Agency for Artificial Intelligence marks one of the initial key components of Spain's AI regulations. In this context, the current situation will probably lead to new interesting legal developments in 2024.

David Fuentes
Associate
Spain

Artificial Intelligence

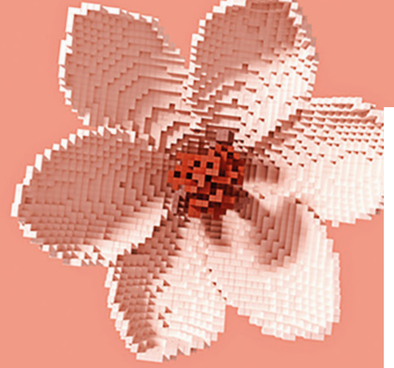


AI regulations across the globe

With the EU AI Act in the making, 2024 will be the year where guiding principles and new rules for AI will be introduced in the USA and the UK. However, we expect the 'Brussels effect' to be limited, since the USA and UK are likely to follow their own course in terms of regulating high-risk systems, foundation models and general purpose AI. We expect new foundation models to hit the market with competitive features. Artificial General Intelligence (AGI) may be expected, but not sooner than 2028.

Feyo Sickinghe
Of Counsel
Netherlands

Artificial Intelligence

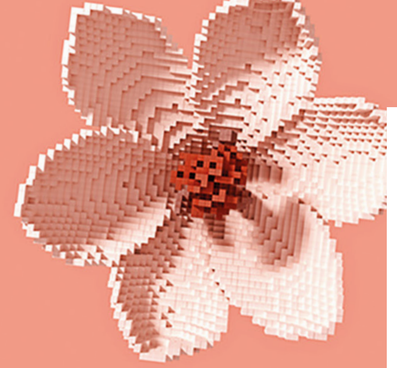


AI and the energy value chain

There are a vast number of AI use cases across the entire energy value chain – time series forecasting, market analysis, optimized bid selection, anomaly detection, failure prevention, consumption pattern recognitions, and more. Ofgem has estimated that there are 110 AI use cases in the system operator alone. It is now accepted that AI will be a key technological enabler for energy companies, and so, with generative AI at its peak hype, and with the European Parliament aiming to reach an agreement on the proposed EU AI Act by the end of 2023, energy companies have already been making great investments into the adoption of AI solutions. A 2023 Global Data report predicts that AI in the energy sector will be worth $909 billion in 2030.

Kathryn Parker
Associate
UK

Artificial Intelligence



AI and security

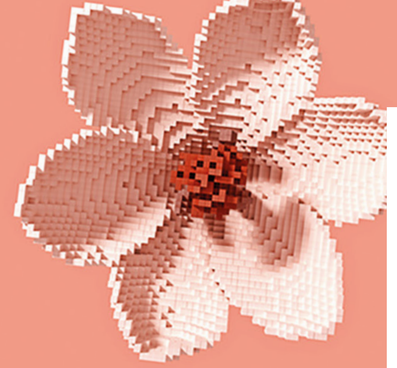
Although there is no AI-specific legislation, China's AI-specific administrative regulations have almost been going hand in hand with the emerging of AI technologies. In 2023, China has published Deep Synthesis Regulation, Generative AI Measures and Measures for Review of Scientific and Technological Ethics (for Trial Implementation). The key areas in China's AI governance are more about the algorithm and ethics principles.

In 2024, we are likely to see more national standards with detailed requirements from technical perspective and possibly more sector-specific regulations on AI technologies.

Tanya Luo
Associate
China

James Gong
Partner
China

Artificial Intelligence



AI and antitrust

2024 is shaping up to be a big year for antitrust enforcement in the technology sector and we expect that competition regulators will be keeping a particularly close watch on AI service providers.

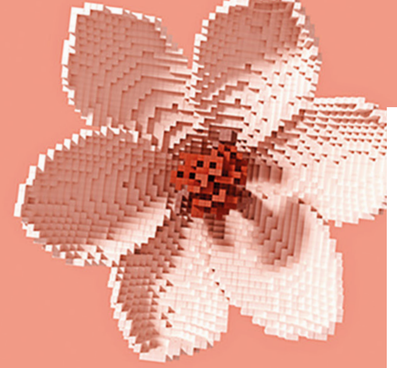
While the breakneck speed of recent developments in AI is a great example of the type of technological innovation that may increase productivity and economic growth, its likely that competition regulators will increasingly scrutinize whether the data advantages held by some AI systems are distorting competition.

There is also some risk that the continued proliferation of AI usage may increase antitrust risks in other sectors. Competition regulators, including the Australian Competition and Consumer Commission, are increasingly highlighting that AI algorithms, and in particular pricing algorithms, may facilitate types of collusion that are prohibited under competition laws.

Patrick Cordwell
Associate
Australia

Thomas Jones
Partner
Australia

Artificial Intelligence



Regulating AI in Australia

While the Australian government considers how best to tackle regulating AI in general, presently the regulation remains left largely to existing (and at times, arguably outdated) legislation, such as in privacy, intellectual property, or consumer protection laws e.g., the Privacy Act 1988 (Cth), Copyright Act 1968 (Cth), and the Competition and Consumer Act 2010 (Cth).

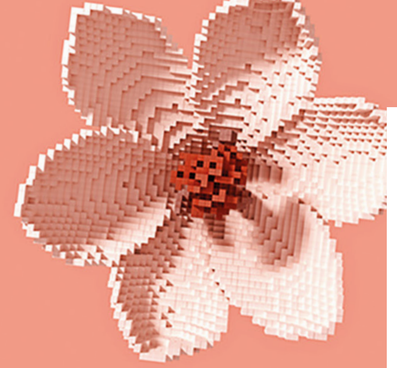
While it remains to be seen whether and how these laws will change to account for generative AI technologies, the government has agreed to the Privacy Act Review Report recommendations on the following changes to the Privacy Act in relation to automated decision making (so anticipate legislation to give effect to these recommendations):

- Privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights;
- High level indicators of the types of decisions with a legal or similarly significant effect on an individual's rights should be included in the Privacy Act and this should be supplemented by OAIC guidance; and
- A right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made should be introduced and entities should be required to include information in privacy policies about the use of personal information to make substantially automated decisions with legal or similarly significant effect.

Alex Gulli
Senior Associate
Australia

Hamish Fraser
Partner
Australia

Artificial Intelligence



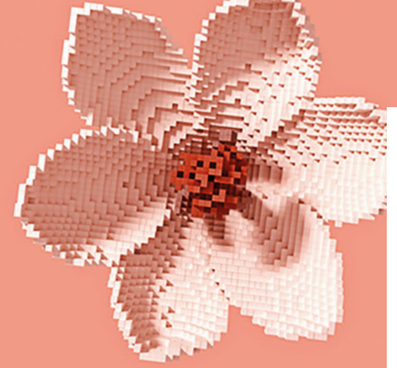
Australia's approach to responsible AI

The Department of Industry, Science and Resources has been consulting on safe and responsible AI in Australia and a discussion paper on this topic was published in June 2023. Before canvassing a broad spectrum of possible responses to the governance of AI, the discussion paper proposed that the governance measures adopted by Australia be guided by the need to ensure there are appropriate safeguards and to provide greater certainty for businesses. The discussion paper welcomed feedback on how the Australian Government could mitigate any potential risks of AI and support safe and responsible AI practices and, in August 2023, public consultation was closed. We expect to see further steps taken by the Australian Government, in 2024, as it looks to consider appropriate regulatory and policy responses.

James Hoy
Senior Counsel
Australia

Hamish Fraser
Partner
Australia

Artificial Intelligence



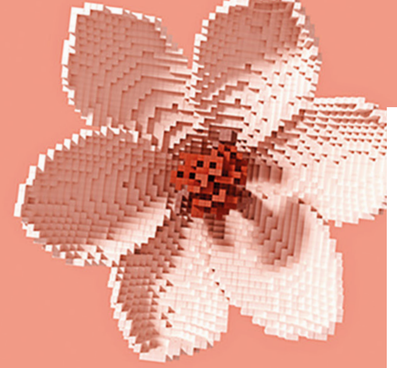
Emerging technologies

Emerging technologies, such as AI, machine learning, blockchain, natural language processing, and chatbots will continue to pose new legal questions and risks, such as the regarding the creation and infringement of intellectual property rights, the breach of data protection and privacy rights, consumer protection infringements, and contravention of product liability laws. In the EU it will be easier for individuals to seek to assert their rights and interests in these areas through the courts and judicial frameworks, rather than relying on the regulators, who may lack the resources, expertise, or authority to deal with these complex and novel issues, including as they effect each other.

Deirdre Kilroy
Partner
Ireland

Kelly Mackey
Associate
Ireland

Artificial Intelligence



Copyright implications of generative AI →

Can generative AI created works be protected? →

AI and extra-territorial reach →

AI liability →

Contracting for AI →

Human centric AI →

AI in employment →

AI & life sciences →

AI & drug development →

Shaping AI regulation →

Generative AI and children →

Adoption of generative AI →

GCC governments harnessing AI →

New UK legal framework for self-driving vehicles →

Liability damages caused by AI systems →

Security risks using AI →

Generative AI in legal services →

Tools in software code development →

AI liability and consumer protection →

EU AI regulation →

Spanish AI regulation →

AI regulations across the globe →

AI and the energy value chain →

AI and security →

AI and antitrust →

Regulating AI in Australia →

Australia's approach to responsible AI →

Emerging technologies →

More governments will enact AI regulations seeking higher technical and ethical standards

GlobalData

Without proper guardrails around TuringBot-generated code, Forrester predicts that in 2024 at least three data breaches will be publicly blamed on insecure AI-generated code – either due to security flaws in the generated code itself or vulnerabilities in AI-suggested dependencies

Forbes - Predictions 2024

Generative AI has a cold shower in 2024 as the reality of cost, risk and complexity replaces the hype of 2023

CCS Insight's predictions for 2024

By 2030, AI enables 50% of companies in a European country to trial a four-day working week

CCS Insight's predictions for 2024

Cybersecurity

EU cybersecurity requirements in 2024

We are witnessing a trend of increasing regulation in the area of cybersecurity, with EU legislators having completed their work on the NIS2 and CER Directives, as well as the Regulation on Digital Operational Resilience for the Financial Sector (DORA) - three key pieces of cybersecurity-related legislation that came into force in mid-January 2023. The proposed legislation on cybersecurity requirements for products with digital elements (Cyber Resilience Act (CRA)) will complement the existing EU cybersecurity framework, once formally adopted by the co-legislators in the next time.

From a practical standpoint, it is crucial for companies, as a first step, to understand whether these legislative acts (in relation to NIS2/CER: in conjunction with the local implementation of these acts) apply to them directly and/or indirectly (i.e., through customers) and to prepare a compliance plan. As a second step, after conducting a gap analysis, entities covered by the legislation should focus on implementing the necessary measures to comply with the new EU cybersecurity laws and address any gaps. Simultaneously, it will be important to monitor updates to further specifications and additional cybersecurity requirements that will emerge at both EU and national level in the context of some of the aforementioned cybersecurity laws.

Natallia Karniyevich
Senior Associate
Germany

Cybersecurity

DORA: challenges and opportunities

An issue expected for 2024, is the financial sector having to align its preparation for DORA. DORA is no longer a novelty or something to be pushed until later; the content of the Act itself and the Regulatory Technical Standards (RTS) underway sets out details of the new requirements for the financial sector overall. However, the RTS's have been subject to heavy criticism from the sector during hearings for lacking proportionality and ensuring adequate allowance for a risk-based approach. What changes this criticism leads to is yet to be seen, but there is no doubt sharing of knowledge and of best practices of driving compliance implementation is going to be key.

The anticipated complexity and cost implications of aligning with DORA and RTS could particularly challenge smaller institutions, which may struggle with resource allocation for compliance. This underscores the need for both the sector and advisors to drive or assist compliance via nuanced, scalable solutions within the regulatory framework to accommodate diverse operational scales and risk profiles across the sector.

The evolving nature of the cyber threats and the technology necessitates continued dynamic, adaptable strategies and a buy-in from the organization. Effective implementation of DORA – but especially the intentions behind DORA - will not only hinge on compliance but also on the sector's ability to foster innovation and create a positive narrative within the regulatory boundaries, ensuring resilience becomes a matter of pride in a rapidly changing digital landscape.

Mathias Mølsted Andersen
Senior Associate
Denmark

Cybersecurity

New encryption algorithms

Some commonly used encryption protocols, such as RSA encryption, rely on integer factoring or similar mathematical problems which cannot be solved by classical computers. However, they could be solved by full-scale quantum computers. So, if such quantum computers were ever built, they would be capable of decoding the respective data meant to be protected. It is not excluded that third parties intercepting and storing encrypted data today will be able to decrypt it in the future by using a quantum computer. To counter this threat, organizations like the US National Institute of Standards and Technology (NIST) are standardizing cryptographic algorithms that are safe against attacks from full-scale quantum computers. In 2023, the NIST has announced three algorithms whose standardization will be completed in 2024. Further algorithms will follow. Companies should keep an eye on this development to ensure they are implementing the newly standardized algorithms in due time.

Juliana Kliesch
Senior Associate
Germany

Cybersecurity

Security for connected products

One important aspect of cybersecurity that is likely to have increased prevalence relates to connected products, i.e. those products that have physical and digital aspects and connect with other devices and/or platforms/ networks. In order to tackle the challenge of connected products having inadequate security protections (including where a customer's personal security is threatened by cyber-attacks or third party hackers), various legislative initiatives have been implemented. At the EU level, the European Commission has adopted the proposal for a Cyber Resilience Act to create common cybersecurity standards for manufacturers and sellers of both tangible and intangible digital products. In the UK, certain requirements under the Product Security and Telecommunications Infrastructure Act 2022 will apply from 29 April 2024, including in relation to: (i) ensuring unqiue passwords (to prevent the use of default passwords); (ii) the provision of information on how product security issues can be reported; and (iii) the information to be provided on the minimum period after which products will no longer receive security updates. Compliance with such requirements will be high on the agenda given that the sanctions provided for under the legislation include fines up to the greater of £10 million or 4% of an operator's revenue.

Russell Williamson
Senior Associate
UK

Cybersecurity

Cyber identity and e-delivery

While awaiting the eIDAS 2.0 Regulation, Poland has already proposed a cyber identity solution: mObywatel. Now all players in the Polish market will adjust their systems,in order to effectively identify their clients using mObywatel credentials. This will be linked with another significant development – obligatory e-delivery (G2B and B2B), which will effectively apply from December 2023, but we expect the implementation process to take place in Q1 of 2024.

Kuba Ruiz
Senior Counsel
Poland

Cybersecurity

AI and cybersecurity

Cyber teams will need to collaborate more with other stakeholders, such as business units, regulators, customers, and partners, to explain and align their security strategies. Regulatory changes will facilitate benchmarking and cyber will increase in significance in the procurement process, as certain entities will have increased regulatory obligations which will flow down to vendors, and their cyber teams. There will be increased spending on cybersecurity capabilities, performance, and risk identification and management.

Machine learning will introduce vulnerabilities and improve those launching cyber-attacks, and we will see activity in areas such as adversarial attacks, data poisoning, ransomware, phishing, zero-day attacks and model stealing. AI and machine learning will also play a key role in advancing cybersecurity, heling cyber teams analyse large volumes of data, identify threat patterns and anomalies, and will speed up the learning from feedback.

Deirdre Kilroy
Partner
Ireland

Cybersecurity

The impact of NIS2

In October 2024, the new Network and Information Security Directive (NIS2) will compel organizations to prioritize cybersecurity due to its expanded scope and stringent risk management requirements. This directive, building on the existing NIS directive, widens its impact across various sectors, prompting a re-evaluation of cybersecurity measures. Further, NIS2 emphasizes supply chain security, extending its influence on suppliers. As a result, cybersecurity demands will extend across industries, becoming both a legal obligation and a competitive differentiator as well as a ‘license to play’ in technology-heavy industries.

While awaiting further clarification on certain aspects of NIS2, including any certification schemes, organizations are expected to adopt existing security frameworks such as ISO 27001, NIST, and CIS18 to achieve and demonstrate compliance with the directive's security requirements. Consequently, an increase in adoption and certification under these frameworks is anticipated in the coming year.

Another expected trend in 2024, driven by NIS2, is the shift towards a more integrated cybersecurity approach. This entails moving beyond the IT department's realm, embedding cybersecurity in management, and making it a company-wide priority. NIS2 requires cybersecurity efforts to be anchored within management, with the potential of holding management personally liable for non-compliance. It also mandates training for both management and employees. This is expected to drive organizational restructuring and the implementation of processes, procedures, and training to ensure effective integration of cybersecurity, especially as a management priority.

Anna Hjortlund
Associate
Denmark

Cybersecurity

The impact of NIS2 on data centres

During 2024, data centres will have to comply with the cybersecurity risk management and incident reporting requirements of NIS2, a new EU directive that aims to improve the cybersecurity of essential and important entities. Data centres will have to take specific actions to comply with NIS2, such as taking measures to prevent and mitigate the impact of cyber-attacks on their operations, assets, and data, and ensuring the security of their supply chains and service providers. Those availing of the services of data centres are likely to take the quality of the NIS2 efforts into account which purchasing data centre services.

Deirdre Kilroy
Partner
Ireland

Georgina Parkinson
Associate
Ireland

Cybersecurity

Impact of NIS2 on the life sciences sector

NIS2 is a new EU directive that aims to improve the cybersecurity of essential and important entities, including many pharmaceutical and biotech companies and which will take effect in 2024. Pharma companies that are involved in key research and development activities of medicinal products, or that manufacture certain medical devices and basic pharmaceutical products, will have to comply with the cybersecurity risk management and incident reporting requirements of NIS2, as they are considered important entities under NIS2. Entities that are subject to NIS2 will have to update their cybersecurity policies and practices, take steps to ensure the security of their supply chains and service providers, and take measures to prevent and mitigate the impact of cyberattacks on their operations, assets, and data.

Deirdre Kilroy
Partner
Ireland

Kelly Mackey
Associate
Ireland

Cybersecurity

Power to grant injunctions against ‘newcomers’

In November 2023 the UK Supreme Court confirmed that the courts have power to grant injunctions against ‘newcomers’. This new form of injunction, granted without notice against persons who cannot be known at the time the order is made, and therefore can apply to anyone in the world, has wide significance especially in the online world where violations of private and public rights can occur behind a veil of anonymity. We see that the advent of this groundbreaking injunction could provide businesses who are victims of cyber crime and online frauds with an additional weapon against the hackers.

Jeremy Sharman
Partner
UK

Cybersecurity

Cybersecurity in Poland

Poland has a tendency to be slow in implementing EU law, and we can assume that the same will apply to the NIS2 Directive.

However, even before the Polish parliamentary elections which took place in October 2023, Poland prepared an amendment to the Polish Cybersecurity System Act that, if adopted, would significantly affect cybersecurity service providers operating on the Polish market.

Financial institutions will also start implementing DORA, which will indirectly affect ICT third party service providers (mostly tech companies providing services to the financial sector). The Polish Financial Supervision Authority may also add some additional requirements specific to Poland, so it is worth monitoring legislative work in this area.

Kuba Ruiz
Senior Counsel
Poland

Cybersecurity

Cyber-attacks will be a challenge for the insurance sector

According to the latest 2024 Risk in Focus Report issued by the European Confederation of Institutes of Internal Auditing, *"84% of respondents cited cybersecurity and data security as a top five risk compared to 82% last year"*. Insurance companies are not alien to this technological predicament due to the sensitive nature of its business model.

Here are some trends that may explain the evolution of the sector (i) higher frequency and severity of the attacks due to the digitalization of the economy and the use of AI (ii) risk-delocalization and an increasing number of catastrophic-in-nature claims due to the ubiquitous nature of the internet; and (iii) increase of "wiper attacks" (aimed at deleting and destroying data), specially linked to state-sponsored actor. For instance, Sweden has reported an increase in cyber-attacks since they announced it intention to join NATO.

These realities may entail more legal uncertainty due to the untested nature of the new insurance forms before the Courts, a tightening of the insurance forms and a strong focus on cyber hygiene (i.e., the implementation of best practices in the use of cyber assets) as a prerequisite of the coverage.

Ignacio Belmar
Associate
Spain

Cybersecurity

Cross-boundary data flow within the Guangdong-Hong Kong-Macao Greater Bay Area

2023 has seen a clear impetus on fostering an integrated regulatory framework for the flow of personal data from Mainland China to Hong Kong. In June 2023, the Hong Kong Government and the Cyberspace Administration of China signed a memorandum of understanding for facilitating cross-border data flow within the Guangdong-Hong Kong-Macao Greater Bay Area (GBA). This was followed by a consultation draft of the GBA Cross Border Personal Information Protection Requirements published by China's national information security standards committee in November 2023. On this basis, the Hong Kong government has been working with the Guangdong Province regulatory authorities to formulate a pilot scheme for streamlining the cross-border data transfer compliance efforts for finance, credit-checking and the healthcare sectors. These developments are clear and gradual steps towards a certified channel for cross-border data transfer between GBA and Hong Kong-based organizations.

We remain watchful on the kind of permitted data categories that will benefit from this relaxation.

On that backdrop, Hong Kong's data protection and cybersecurity regulatory landscape is braced for changes. The Government indicated that the cybersecurity bill will be introduced in the 2024 legislative process. We expect the cybersecurity and data protection legislative changes to evolve and materialise in the context of the continuous relaxation of the GBA cross-border data transfer rules, and in conjunction they will significantly shape how organizations structure their operational and compliance arrangements in the Greater China region.

Wilfred Ng
Partner
Hong Kong

Cybersecurity

Heightened risk of regulatory investigation and action in Australia

In 2022-23, several Australian regulators not traditionally known for privacy related enforcement (including the Australian Securities and Investments Commission (ASIC) and Australian Competition and Consumer Commission (ACCC)) have succeeded in bringing enforcement action against companies for cybersecurity failures (for example for breach of Australian Financial Services Licence duties in respect of a data breach and misleading statements in a privacy policy) and (in the case of ASIC) have indicated that directors who do not ensure their company has "adequate" cybersecurity and the ability to recover from an attack could face action by ASIC. In addition, Australia's privacy regulator, the Office of the Australian Information Commissioner (OAIC) has received additional funding for enforcement activities. We therefore expect to see heightened enforcement action risk in 2024 with further investigations and/or actions commenced by Australian regulators, particularly if the OAIC's enforcement powers are further expanded (as is currently proposed in the ongoing review of Australia's Privacy laws).

Emma Croft
Senior Associate
Australia

Julie Cheeseman
Partner
Australia

Jonathon Ellis
Partner
Australia

Cybersecurity

According to the EU Agency for Cybersecurity (ENISA), the ransomware business model has grown exponentially in the last decade and is projected to cost more than $10 trillion by 2025, up from $3 trillion in 2015

GlobalData

71% of respondents believe cybersecurity is either already disrupting their industry or will do so in the next 12 months

GlobalData

Research suggests that one in two businesses has been the victim of a successful cyberattack in the past three years, and the cost of these attacks to industry is expected to grow to over $10 trillion by the end of 2024

Forbes - The Top 5 Tech Trends in 2024

Data

Access to industrial data by default

Connected device and cloud processing ecosystems will both be heavily impacted by the incoming EU Data Act, which aims to unlock access to hordes of valuable industrial data. The Data Act is expected to come into force in early 2024, with most provisions applying from Q3 - Q4 2025. Now is the time for providers of connected products and related services to prepare for a future in which access to product data and related service data is made available by default. Others will begin to look for new opportunities and business models presented by the access to industrial data unlocked by the Data Act.

Click here to access our Digital Rights & Assets European Digital Strategy Developments guide

Francine Cunningham
Regulatory And Public Affairs Director
Belgium and Ireland

Data

The Data Act introduces new rules for data processing services

In addition to regulating connected products, the Data Act will also introduce new rules for providers of data processing services. These are digital services that enable ubiquitous and on-demand network access to shared computing resources. The Data Act will bring standard term control for terms impacting the switching between these cloud service providers. For companies that means reviewing existing terms, in particular in terms of fees that would make switching between competing data processing services harder.

Tobias Bräutigam
Partner
Finland

Data

The European Health Data Space

The importance of health data has clearly been demonstrated during the pandemic, while it has also become clear that there are barriers to accessing and sharing health data across EU borders. To overcome these barriers and to unleash the full potential of health data, the European Commission has proposed a regulation to create a European Health Data Space (EHDS) which covers health data exchange between patients and health professionals as well as the secondary use of such data.

The proposal is expected to move into the final negotiations in the fall of 2023 lasting into the spring of 2024. As the regulation is adopted and enters into force, it will strengthen the EU's role within global health and deepen the cooperation between the EU Member States. Its introduction is expected to increase, and change, the usage of health data in the EU.

Mattias Lindberg
Partner
Sweden

Data

Impact of the EU Data Act on the energy sector

The European Union is implementing another milestone in its European data strategy - the EU Data Act. Formal adoption by the European Parliament and the Council is scheduled for the end of 2023, aiming to increase transparency and make data more usable. A vast amount of data is already generated during generation, transmission, deployment and use of energy. The new EU Data Act therefore opens up new potential for the use of data in the energy sector, and a further push in energy digitisation, leading to great implications for the sector going forward.

Kathryn Parker
Associate
UK

Data

Data switching and interoperability

Amongst many obligations like data sharing for data holders, the EU Data Act creates a framework for switching between data processing services and interoperability.

We expect companies will start making preparations for new streams of business based on data sharing and creating new business opportunities.

Feyo Sickinghe
Of Counsel
Netherlands

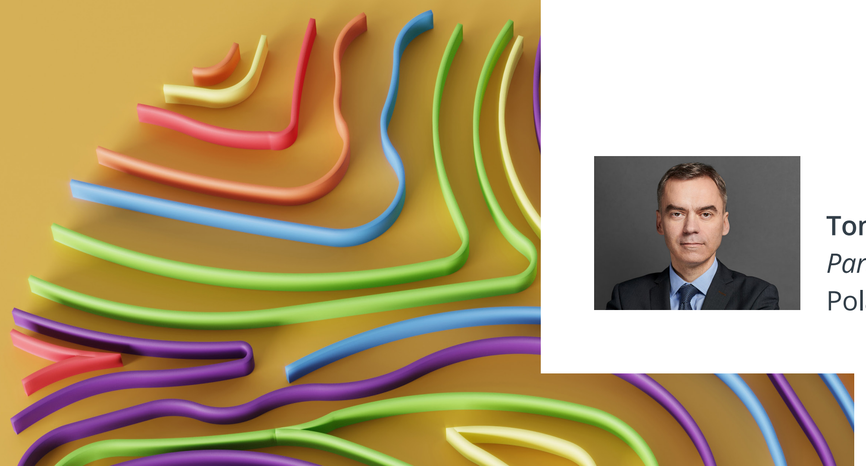
Data

UK roadmap for energy digitalisation

The UK Energy Digitalisation Strategy developed by the UK Government and the UK energy regulator, Ofgem, also seeks to make the energy system more visible and system data more shareable. With regards to building a framework for the sharing of energy related data, Ofgem has suggested that there will be a call for input in April 2024, with a consultation and workshops to follow, estimating a 12-18 month process of building a digital roadmap and data sharing infrastructure. In March this year, the Department for Energy Security and Net Zero published details regarding a 6 month feasibility study to assess the feasibility of a 'digital spine' concept for the UK energy system, as proposed by the Energy Digitalisation Taskforce in 2022.

Kathryn Parker
Associate
UK

Data



Digitalisation regulations

EU digital regulations are starting to become complex and complicated. In 2024, the market will be shaped by many pieces of legislation that have already been adopted or are at the end of the legislative process, such as the DMA, DSA, Data Act, AI Act, DGA, eIDAS 2 and NIS2. These regulations are the outcome of many concurrent legislative processes and, as a result, there may be many areas where these regulations overlap or are inconsistent with each other. This may lead to increased compliance costs for all companies and legal uncertainty, which would be detrimental to business development.

Tomasz Zalewski
Partner
Poland

Data

User’s data conservation and access

In the last couple of years, the French legal framework surrounding the conservation of and access to the users' data collected by online intermediaries has undergone tremendous changes to accommodate for the principles set out by European case law. Since the new provisions that rule data conservation and access, vary greatly depending on the category of data at play and the gravity of the criminal offence being investigated, the implementation of this complex new regime has impacted both criminal and civil cases, as civil plaintiffs can no longer request the communication of a user's data for the sole purpose of a civil proceeding.

Consequently, national courts are now in the process of clarifying the practical ramifications of this reform, a task even more crucial in light of the probable rise in legal disputes that should occur following the aftermath of the DSA, and, at a national level, of several French laws on cyberspace. Regrettably, however, aside from the lingering legal uncertainty that surrounds the conservation of and access to data collected before and after this new legislation, the compliance of the French framework with European law still remains uncertain.

Djazia Tiourtite
Partner
France

Anne-Sophie Lampe
Partner
France

Data

Digital Services Act (DSA) & copyright

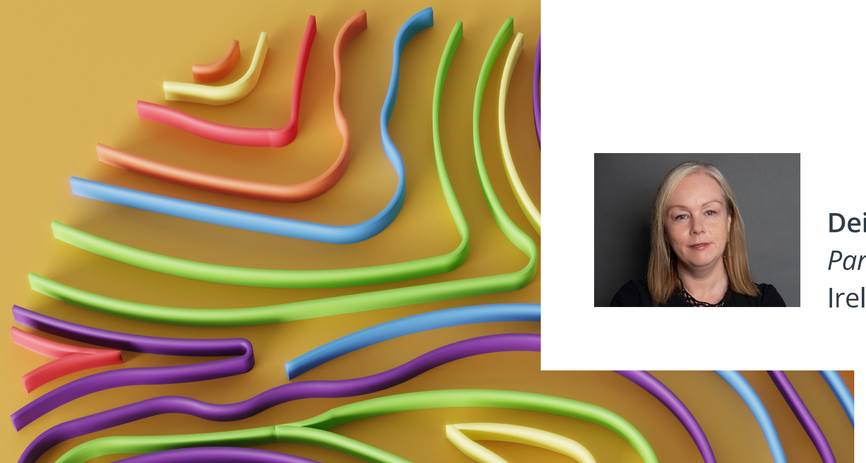
The DSA implementation in 2024, will participate in catalysing a shift towards curbing online misinformation, protecting user rights, and regulating digital platforms. This legislative overhaul may spark an uptick in legal disputes between plaintiffs, such as copyright owners, and intermediary service providers that were not expressly targeted by the existing legal framework (i.e., catching service providers and mere conduit service providers).

Copyright owners, empowered by the DSA's provisions, will likely be more assertive in holding these technical service providers accountable for their capacities in intervening on network infrastructures to prevent copyright infringements. Simultaneously, these service providers, will be faced with stricter regulations, navigating a complex area of compliance measures and due diligence that may not be implemented in their current operational processes.

Djazia Tiourtite
Partner
France

Anne-Sophie Lampe
Partner
France

Data



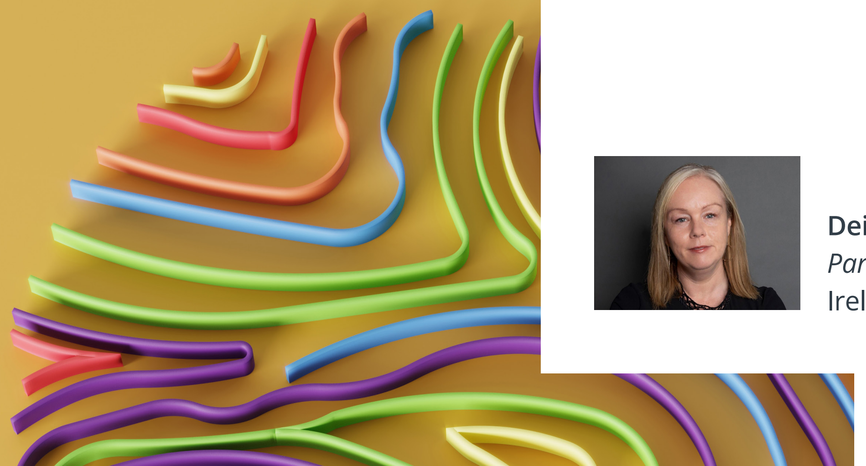
Consequences of the DSA

The force of the DSA will be felt after February 2024, as regulators are appointed, trusted flaggers approved, and the legislative instrument will apply beyond the very large entities. The DSA aims to harmonise, strengthen and clarify the legal framework for digital intermediary services in the EU. As the DSA interacts with other areas and sources of law, such as data protection, consumer protection, competition law, intellectual property law, and fundamental rights legal teams will need to update their thinking and advice, and intermediaries will need to adjust their products and services. Legal teams will need to keep abreast of the developments and changes in the relevant legal fields, and to deal with the potential conflicts and inconsistencies that will inevitably arise.

Legal teams working in online marketplaces and platforms will need to adjust and take account of the increased risk of litigation and dispute resolution issues which arise under the DSA. The DSA creates new avenues and mechanisms for legal redress and enforcement. The DSA grants users and other affected parties the right to seek judicial and regulatory remedies against online intermediaries and platforms for the infringement of their rights or interests.

Deirdre Kilroy
Partner
Ireland

Data



The DSA and its impact on retail

Online marketplaces will have to comply with new obligations under the DSA aimed at ensuring transparency and accountability for their users, business users, and public authorities. They will have to provide clear and accessible information about their terms and conditions, their content moderation policies and practices, their ranking and recommendation mechanisms, and their advertising and commercial communications. Online marketplaces will also have to deal with enhanced user rights and protections. For example, online marketplaces will have to provide effective, DSA compliant and user-friendly mechanisms for users to flag and report illegal content and goods, to challenge content moderation decisions, and to escalate complaints.

Deirdre Kilroy
Partner
Ireland

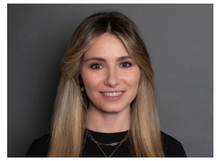
Megan Kearns
Associate
Ireland

Data

Parental consent and parental controls

There has been an increasing emphasis during 2023 by regulators and policy makers in relation to the risks posed to children online and the means by which higher level of protections can be ensured for children. Against this backdrop, parental consent and parental controls are emerging at the intersection of privacy and safety as a key means of providing heightened protection of children as users of digital services. During 2023 there has been an increasing industry focus on implementing more reliable technical solutions for verifying parental relationships and enabling effective parental involvement (e.g. through the provision of parental control settings). We anticipate that increasing regulatory attention in this area during 2024 will continue to fuel demand and growth in the market for products and technical solutions which facilitate the provision of parental consent and parental involvement while respecting data protection principles as well as the rights of the child.

Anna Morgan
Partner
Ireland



Shauna Joyce
Associate
Ireland

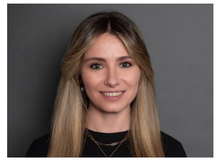
Data

Children's data protection and privacy

The regulatory spotlight on the processing of children's personal data will continue to grow more intense in 2024. As predicted in our 2023 report, 2023 saw much attention focused on this topic by EU/EEA data protection authorities with a further major cross-border processing decision as well as enforcement actions taken by the UK ICO, and individual EU data protection authorities during the year.

We anticipate growing momentum in this area of supervision and enforcement, not least due to the anticipated publication in 2024 of the EDPB Guidelines on processing children's data, as well as the wider work being conducted by the European Commission to establish an EU Code of Conduct on age appropriate design (covering privacy as well as safety and security) as part of its New European Strategy for a Better Internet for Kids (BIK+).

Anna Morgan
Partner
Ireland



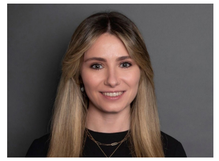
Shauna Joyce
Associate
Ireland

Data

Age verification / age assurance

As predicted in our 2023 report, emphasis on age verification and age assurance by regulators and policy makers in the UK and EU/EEA continued to gather pace in 2023 with various data protection enforcement actions focusing on the efficacy and circumventability of measures deployed by digital services to prevent children below stipulated user age limits from accessing their services. In 2023, the UK ICO continued to lead the way in its work towards standardising the measurement of age assurance solutions and this is set to continue in 2024, with the UK's Ofcom also undertaking work on age assurance guidance. Separately, during 2024 work at International Standards Organization (ISO) level on establishing an international standard for age assurance will also continue. Meanwhile the European Commission has indicated in its New European Strategy for a Better Internet for Kids (BIK+) that it will work towards a European standard on age assurance and age verification which will clarify what is expected from industry when age verification is required on any online services. We anticipate that the robustness and efficacy of age verification and age assurance measures deployed by digital services will be an ever-increasing focal point for data protection, content and online safety regulators during 2024. In parallel, we anticipate that technical innovation and the market for solutions will continue to grow as a result of industry demand caused by regulatory attention on this issue. Against this backdrop, some of the key questions for 2024 in this area will revolve around whether a harmonised regulatory approach will emerge at least across Europe, how data protection principles can be best respected by age assurance and verification products and whether widespread technical solution interoperability across the digital ecosystem is capable of being achieved in reality.

Anna Morgan
Partner
Ireland



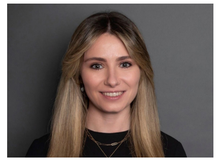
Shauna Joyce
Associate
Ireland

Data

Online safety/ content regulation in Ireland

Following the enactment in Ireland of the Online Safety and Media Regulation Act (OSMRA) at the end of 2022, 2023 saw the establishment of a new regulator, the Media Commission (in Irish Coimisiún na Meán), which will enforce, amongst others, the new laws established in the OSMRA around harmful online content. The Media Commission will also be Ireland's regulator for the purposes of the EU Digital Services Act and for the regulation of online terrorist content. We expect, based on the Media Commission's published work programme and a public consultation on a draft online safety code for video sharing platforms, that 2024 will see the Media Commission finalise this first Online Safety Code and potentially start to take substantive actions in supervising and enforcing against video sharing platforms under the code.

Anna Morgan
Partner
Ireland



Shauna Joyce
Associate
Ireland

Data

Access to industrial data by default →

The Data Act introduces new rules for data processing services →

The European Health Data Space →

Impact of the new EU Data Act on the energy sector →

Data switching and interoperability →

UK roadmap for energy digitalsation →

Digitalisation regulations →

User's data conservation and access →

Digital Services Act (DSA) & copyright →

Consequences of the DSA →

The DSA and its impact on retail →

Parental consent and parental controls →

Children's data protection and privacy →

Age verification / age assurance →

Online safety/ content regulation in Ireland →

Online Safety Act (OSA) in the UK →

Data breaches →

Privacy and Electronic Communications Regulations (PECR) fines →

Data classification, data asset and data market →

China's data export →

Australia's Privacy Act Review Report →

Trends in the gaming industry →

Online Safety Act (OSA) in the UK

Implementation of the OSA will start slowly but steadily gather pace with the first rounds of consultations already having opened with more to follows. OFCOM's stated approach is to implement a four phase regulatory strategy by establishing standards, driving industry improvements, assuring compliance and only then holding to account by way of enforcement. We predict that the OSA compliance will become an increasingly important part of organizations compliance with digital regulation as we move through those phases and the various consultations are codified into formal guidance.

Click here to access our Digital Rights & Assets UK Digital Strategy Developments guide

James Moss
Partner
UK

Data

Data breaches

In 2024, data breaches are likely to become more frequent, complex and expensive. This will most likely be caused by the increased use of artificial intelligence and machine learning by bad actors seeking to access people’s personal data. In 2023, the biggest cause of data breaches have been employee error – this will likely lead to a resurgence of more robust GDPR training for employees in 2024 and the increased adoption and use of automation processes to minimise human error in organizations.

James Moss
Partner
UK

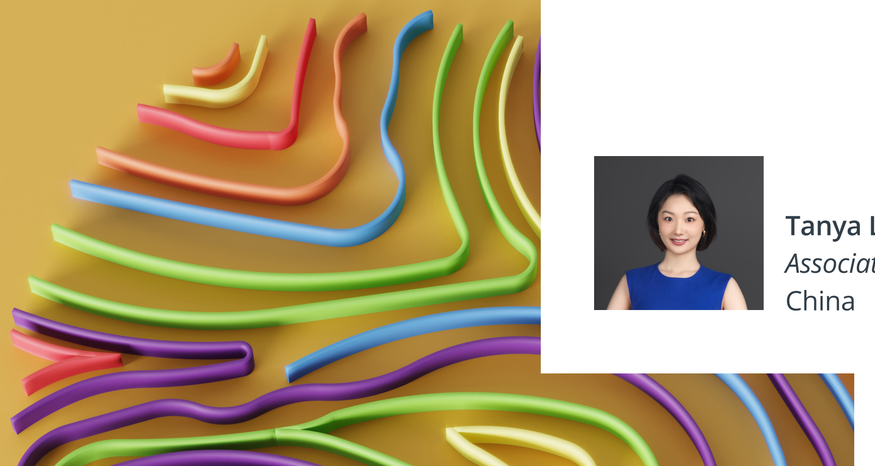
Data

Privacy and Electronic Communications Regulations (PECR) fines

In terms of PECR enforcement in 2024, the ICO is likely to continue its active and robust enforcement of the PECR, especially in relation to unsolicited electronic marketing communications, which are the main source of complaints and breaches of the PECR. Some factors that may influence the ICO's enforcement strategy includes a prioritisation of enforcement actions based on the volume and nature of complaints, focusing on the most serious, persistent, and widespread breaches that cause the most harm or distress to individuals, as well as changing legal and technological developments which will undoubtedly impact electronic communications and marketing, particularly with the existence of AI, blockchain and voice over internet protocol. The Data Protection and Digital Information (No. 2) Bill which is a piece of UK legislation that aims to update and simplify the data protection framework in the UK will also make significant changes to the PECR and simplify the rules on electronic communications and cookies. Most notably, the Bill increases potential fines for the PECR breaches in line with those under the UK GDPR, and introduces a new statutory code of practice for direct marketing.

James Moss
Partner
UK

Data



Data classification, data asset and data market

Chinese central and provincial level governments have established policies to encourage the development data market. One of the notable progress this year are regulations on data asset management. In 2023, China published Interim Provisions on the Relevant Accounting Treatment for Data Resources of Enterprises in which data resources are clearly classified into the scope of intangible assets. Following the regulation, China Appraisal Society issued Data Asset Assessment Guidance, giving specific instructions on the assessment of data asset.

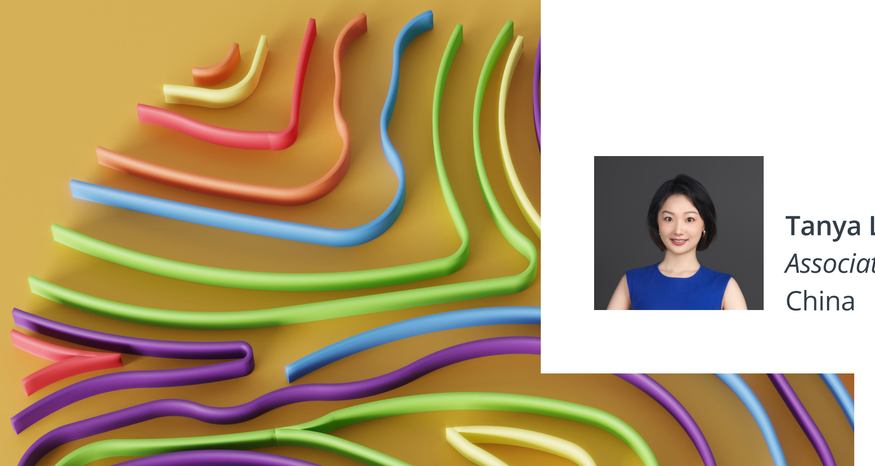
The Ministry of Finance in the last quarter issued an Interim Provisions on the Relevant Accounting Treatment for Data Resources of Enterprises to be effective as of 1 January 2024.

In 2024, we are likely to see more companies explore the opportunities in data market, including data rights registration, data asset assessment, data asset trading, etc. In the meantime, it is likely to see more regulations on data classification to be issued by sectoral authorities and provincial level governments so as to support the data market.

Tanya Luo
Associate
China

James Gong
Partner
China

Data



China's data export

China's data export framework has been completed with the release of China's Standard Contractual Clause in early 2023. A number of companies and organizations have been reported for successfully passing the security assessment or filing the China SCCs. However, in September 2023, China released the draft Regulation for Administering and Promoting Cross-border Data Flow ("Draft CBDT Regulation"), proposing to make substantial changes to the current data export regime while also exempting a wide range of data export activities from the current data export regime. If the Draft CBDT Regulation is implemented as it is, then many data exporters will be released from all or part of their obligations under the current data export regime.

In 2024, we are likely to see the if the Draft CBDT Regulation will be promulgated and whether multinational companies will bear less burdensome data export obligations. In addition, the certification regime under the existing data export regime may also be further revised and special treatment to China's Guangdong–Hong Kong–Macao Greater Bay Area is likely to be established.

Tanya Luo
Associate
China

James Gong
Partner
China

Data

Australia's Privacy Act Review Report

In February 2023, Australia's Attorney-General released the Privacy Act Review Report. The report followed an extensive review of Australia's outdated privacy laws and contained 116 proposals, including significant changes to the scope of data regulated by the Privacy Act and the rules that apply to the handling of such data, which were designed to better align Australia's laws with global standards of privacy protection and give individuals more control over their personal information. In September 2023, the Australian Government released its response to the report, with 38 proposals agreed to, 68 proposals "agreed in-principle" and 10 proposals "noted". We expect to see further steps taken by the Australian Government as part of this ongoing reform process, in 2024, including the release of exposure draft legislation.

Click here to access our Digital Rights & Assets APAC Digital Strategy Developments guide

Julie Cheeseman
Partner
Australia

James Hoy
Senior Counsel
Australia

Data

Trends in the gaming industry

As with many industries, the gaming industry will no doubt continue to be impacted by the recent developments in artificial intelligence, be it AI generated voice content, use of AI to design concept art or in content moderation. We also expect to see the industry continue to be disrupted by the focus on protection of children as a result of the ICO's Age Appropriate Design Code and the new Online Safety Act, with a particular focus on the use of age assurance technologies.

Matthew Buckwell
Senior Associate
UK

Data

Access to industrial data by default →

The Data Act introduces new rules for data processing services →

The European Health Data Space →

Impact of the new EU Data Act on the energy sector →

Data switching and interoperability →

UK roadmap for energy digitalsation →

Digitalisation regulations →

User's data conservation and access →

Digital Services Act (DSA) & copyright →

Consequences of the DSA →

The DSA and its impact on retail →

Parental consent and parental controls →

Children's data protection and privacy →

Age verification / age assurance →

Online safety/ content regulation in Ireland →

Online Safety Act (OSA) in the UK →

Data breaches →

Privacy and Electronic Communications Regulations (PECR) fines →

Data classification, data asset and data market →

China's data export →

Australia's Privacy Act Review Report →

Trends in the gaming industry →

Big data will increasingly be combined with AI technologies, especially machine learning, for prediction, real-time analytics, and augmented data management

GlobalData

Advertisers will increasingly seek a return to first-party data based on direct interaction with the consumer and reduce their dependence on third-party data

GlobalData

GlobalData estimates the total data analytics market will be worth $188.8 billion in 2027

GlobalData

ESG

ESG regulatory challenges for the telco industry

2024 is expected to be the year when the EU legislator will finalise the remainder of its ambitious Green Deal regulatory package, including most notably the Corporate Sustainability Due Diligence Directive (CSDDD). This means that the industry will be forced to move from proclaiming sustainability statements and ambitions to implementing the regulatory ESG requirements not only in their own business operations but also in their supply chains.

Moving from carbon-neutral – reducing and offsetting carbon emissions from a company's own operations (Scope 1 and 2 emissions) - to a net-zero target in which also emissions across the whole value chain (scope 3) are reduced to zero requires a rigorous and holistic approach with cannot always be reconciled with direct commercial interests. The EU CSDDD will stimulate this shift in attention from internal operations to contributions from the value chain required to realise progress towards net-zero.

The challenges for progression in this journey towards net-zero requires measuring and monitoring scope 3 emissions, 'greening' the supply chain and becoming a more circular economy. Transgressing from a linear 'make, take, dispose' economy where raw materials are wasted after use into a circular economy in which companies recycle, reuse, remanufacture and refurbish products requires not only innovation and willingness to invest. It also invokes a shift in mindset, and this will be enhanced by the acceptance of the Regulation on Ecodesign for Sustainable Products proposed by the European Commission.

Pauline Kuipers
Partner
Netherlands

Click here to access our ESG trending topics page

ESG

The German Energy Efficiency Act

Following the amendment to the EU Energy Efficiency Directive in September 2023 (EU 2023/1791), a new Energy Efficiency Act was implemented in Germany in November 2023.

The German Energy Efficiency Act obliges public authorities and bodies to energy savings of 2% per year and requires companies, quite generically, to minimize and reuse waste heat. The data centre industry is targeted above all.

The law places high demands on the operation of data centres in terms of energy efficiency.

- A power usage effectiveness (PUE) value of 1.2 is to be achieved for newly constructed data centres.
- For waste heat recovery, an Energy Recovery Facilities (ERF) of up to 20% is required, which shall be achieved by connecting the data centres to the district heating network.
- Data centres must also obtain all of their energy from renewables - physically/virtually from 2026.
- Data centre operators must publish energy consumption data annually in a public register.

The German government intended to bring the Energy Efficiency Act into force earlier this year, before the amendment to the Directive. Though this goal was not achieved, it is assumed that other EU member states regard the new German law as a model for their national implementation of the amended Energy Efficiency Directive.

Finja Schlingmann
Associate
Germany

Dirk Barcaba
Partner
Germany

ESG

Data centres and sustainability

The data centre industry will continue to grapple with the challenge of meeting sustainability requirements and the growing demand for services. In the UK commercial leases of data centres can only be granted where the property has achieved an energy performance ratings at certain levels and these required levels will become higher over the next few years. The impact of mandatory disclosure of sustainability data (such as the EU's Corporate Sustainability Reporting Directive and the International Financial Reporting Standards) means that there is a laser focus on how sustainable the data centres of the future will be as this data will be available to the public.

We expect data centres to be monitored by consumers and watchdogs alike on their emissions, energy efficiency, water efficiency and climate goals. Greentech and design innovations, such as on-site power generation, clever cooling methodologies, use of distributed sensors and floating data centres will certainly all come into play and be harnessed to reduce data centres' carbon footprint. We also expect more collaboration between the regulators and the data centre industry to pioneer state of the art technologies and best practices for sustainability, particularly in the areas of energy efficiency and decarbonisation and the Climate Neutral Data Centre Pact is a good example of this. Going forward, nations will most certainly be regulating and calibrating the growth of data centre capacity in a sustainable manner consistent with their climate change commitments.

Sophie Phillips
Senior Associate
UK

ESG

Employee activism and corporate sustainability

We anticipate that ESG issues will increasingly dominate not only the company's agenda, but also that of employees in 2024. The roll-out of the Corporate Sustainability Reporting Directive across 2024 and into 2025, mandating qualifying companies to report on corporate sustainability metrics, including treatment of employees, management and corporate board diversity and social responsibility, will increase employee awareness of these issues.

In turn, we expect to see a rise in employee activism and other collective action in this area as employees seek to hold their employers to account over ESG values, particularly within the technology sector where employees are highly skilled and perceived to have greater bargaining power. ESG activity and credentials therefore look set to become an increasingly important talent attraction and retention tool for tech companies in the coming year.

Furat Ashraf
Partner
UK

ESG

New standards for corporate sustainability reporting in the EU

After last year's introduction of the CSRD, the EU has now introduced the European Sustainability Reporting Standards (ESRS), which are connected standards that specify how companies shall report under the CSRD. This complementary legislation marks another step forward in the transition to a sustainable EU economy.

The ESRS covers a full range of environmental, social, and governance issues, including climate change, biodiversity, and human rights. It is worth highlighting that some of the ESRS have been adapted to provide companies more flexibility; a few reporting requirements have been complemented with phase-in provisions, and others have been made voluntary.

Going forward, companies in scope will have to be aware of the ESRS to meet the regulatory requirements under the CSRD. Companies will have to adapt to this set of new rules on sustainability reporting, starting from the 2024 financial year, depending on the size of the company in scope. The CSRD and the ESRS are expected to be a game-changer for corporate sustainability reporting in the EU.

Ariana Sohrabi
Senior Associate
Sweden

Magda Lundh Woldegiorgis
Associate
Sweden

ESG

Is AI ESG compliant?

At its core, ESG compliance involves conducting business in a way that considers environmental impact, social responsibility, and ethical governance. When applied to AI, these principles raise concerns and opportunities.

In terms of environmental impact, AI's energy consumption is a key consideration. Training complex AI models often requires significant computational power, contributing to a substantial carbon footprint. Companies utilising AI must address this issue by investing in energy-efficient technologies, exploring green computing, and incorporating sustainability into their AI strategies.

On the social front, questions arise about the potential impact of AI on employment, as automation can lead to job displacement. ESG-conscious organizations must balance AI adoption with strategies for reskilling and upskilling their workforce, ensuring a fair and inclusive transition to an AI-enabled future.

Ethical governance in AI involves transparency, accountability, and unbiased decision-making. ESG compliance requires organizations to address AI algorithm biases that might perpetuate social inequalities. Ethical AI frameworks, explainable AI methodologies, and continuous monitoring are essential to uphold ESG principles in AI applications.

Despite these challenges, AI also offers avenues for advancing ESG goals. Machine learning algorithms can enhance sustainability initiatives by optimising energy consumption, reducing waste, and improving resource allocation. AI-driven analytics can help companies make data-informed decisions, positively impacting their social and governance responsibilities.

Therefore, a question is being raised among all stakeholders: is AI really sustainable and if yes, how to promote it and avoid greenwashing?

Sandra Sekula-Baranska
Counsel
Poland

ESG

ESG factors are considered more in the IT sector

Ecology is a growing factor in recruiting new IT specialists. According to the magazine "Manager Plus", a study revealed a growing interest in ecology among IT professionals during the recruitment process.

According to the study, 60% of respondents prefer to apply to companies that have a long-term strategy to reduce their environmental impact. Importantly, 46% of professionals expect digital ecology approaches to increasingly influence their employment decisions.

The research shows that women, and those aged 25-34, are particularly interested in digital ecology. Notably, almost 60% of IT professionals believe that employers should be open about their approach to the environment. More than half of respondents (54%) emphasise that companies should also be transparent in the area of digital ecology. In addition, 50% of IT professionals believe that technology employers should tell candidates how they are reducing their negative impact on the environment.

The data also shows that 58% of IT professionals aged 25-34 consider a company's values and mission when choosing a job, indicating the growing importance of environmental and corporate social responsibility issues. These are key considerations for technology companies to include in their recruitment strategies. It is also worth noting that almost half of IT professionals believe that an effective climate change policy will become an increasingly important factor in a candidate's willingness to work for a particular company. Transparent communication about environmental efforts will therefore become a key element in attracting and retaining talent in the IT industry.

The above shows that ESG and sustainable development are becoming a growing factor in choosing the future workplace in IT.

Sandra Sekula-Baranska
Counsel
Poland

ESG

ESG in the space and satellite industry

In 2023, ESG has increasingly played a role in space and satellite regulation and activities, with jurisdictions taking active steps towards introducing ESG considerations into space and satellite regulation. Notably, the UK consulted on measures to reflect sustainability objectives in its national space regulation, the EU has consulted on a proposal to introduce common EU rules for the safety, resilience and sustainability of space activities, and the US is considering legislation to address the challenge of space debris.

We expect to see this trend continue and jurisdictions will need to grapple with the practicalities of how to reconcile the need to keep regulatory barriers to space low while appropriately addressing ESG concerns. Meanwhile there will continue to be increased focus on the development of innovative technologies aimed at addressing ESG concerns, including active debris removal technologies and terrestrial applications of space technologies like space-based solar power.

Hayley Blyth
Associate
UK

ESG

Intersection of technology and ESG

On the back of COP28, we are expecting to see the wider use of technology such as blockchain based carbon tradition platforms gain wider acceptance and also the growth of circular technology, like Singapore-founded company ecoSPIRITS that has developed a low carbon, low waste distribution technology platform.

Aurore Dacier de Biasi
Associate
Singapore

ESG

Singapore’s push towards cleaner vehicles

We anticipate an increase in opportunities in the Electric Vehicle (EV) space, as Singapore is pushing to drive EV adoption. Singapore has established a comprehensive EV Roadmap under the Singapore Green Plan 2030 which includes a strong collaboration between the National Electric Centre and the private sector to deploy 60,000 EV charging points in the city-state by 2030 and the development of new EV regulations and standards.

Jeremy Tan
Partner
Singapore

ESG

Greenwashing enforcement priority in Australia

Greenwashing remains a key enforcement priority for the ACCC in 2023/2024. Following the publication of its draft guidance for businesses making environmental and sustainability claims in 2023, and the subsequent public consultation in relation to this guidance, we expect that the ACCC will publish its final guidance in 2024. Although the guidance is not law, it clarifies the regulator's views on best practice for businesses that wish to make environmental and sustainability claims about their goods or services in Australia. We anticipate that in 2024, the ACCC will closely monitor the market and will take enforcement action against companies that continue to make false, misleading and deceptive sustainability claims.

Lynne Lewis
Partner
Australia

Katrina Dang
Senior Associate
Australia

ESG

Regulators are taking an increasing interest in monitoring Scope 3 emissions. Businesses to become accountable and to continue their commitment to net zero by 2050

GlobalData

Companies perceive macroeconomic themes as a greater imminent threat to their business than ESG or technology themes

GlobalData

Governments are drafting anti-greenwashing legislation and introducing enhanced ESG accountability and performance tracking regulations

GlobalData

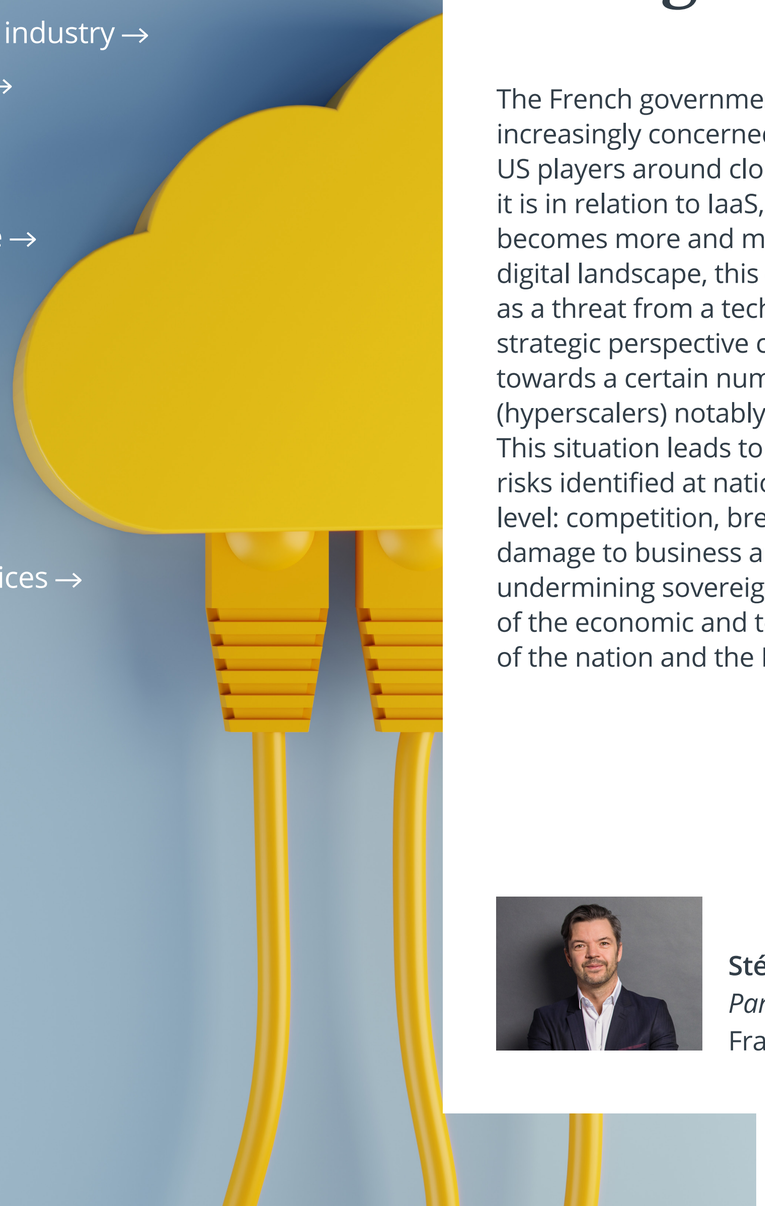
Cloud & IoT

Data Act – a game changer for the cloud industry

New technologies have during recent years seen a substantial rise in the regulation from EU. Among these regulations is the Data Act which was finally adopted on 27 November 2023. The Data Act aims to makie it easier and less costly for customers to switch cloud and other data processing providers. As a general rule, the supplier must be able to complete such a switch within 90 days and the supplier may – after an interim period of 3 years – not charge the customer separately for this assistance. Further, the switch must be done without loss of functionality (the principle of "functional equivalence"). The Data Act also introduces new requirements for the content of the contracts which must include the customers' rights under the Data Act in a clear language and be easily accessible prior to the entry of the contract. The contract must also contain an exhaustive specification of the categories of data and applications that can be exported upon switching. Although the Data Act does not take effect until July 2025, providers of cloud services are well advised to start adapting to these new regulations soon – especially by implementing technical measures to enable a fast migration to another provider, in addition to checking their terms and conditions.

Jesper Langemark
Partner
Denmark

Cloud & IoT

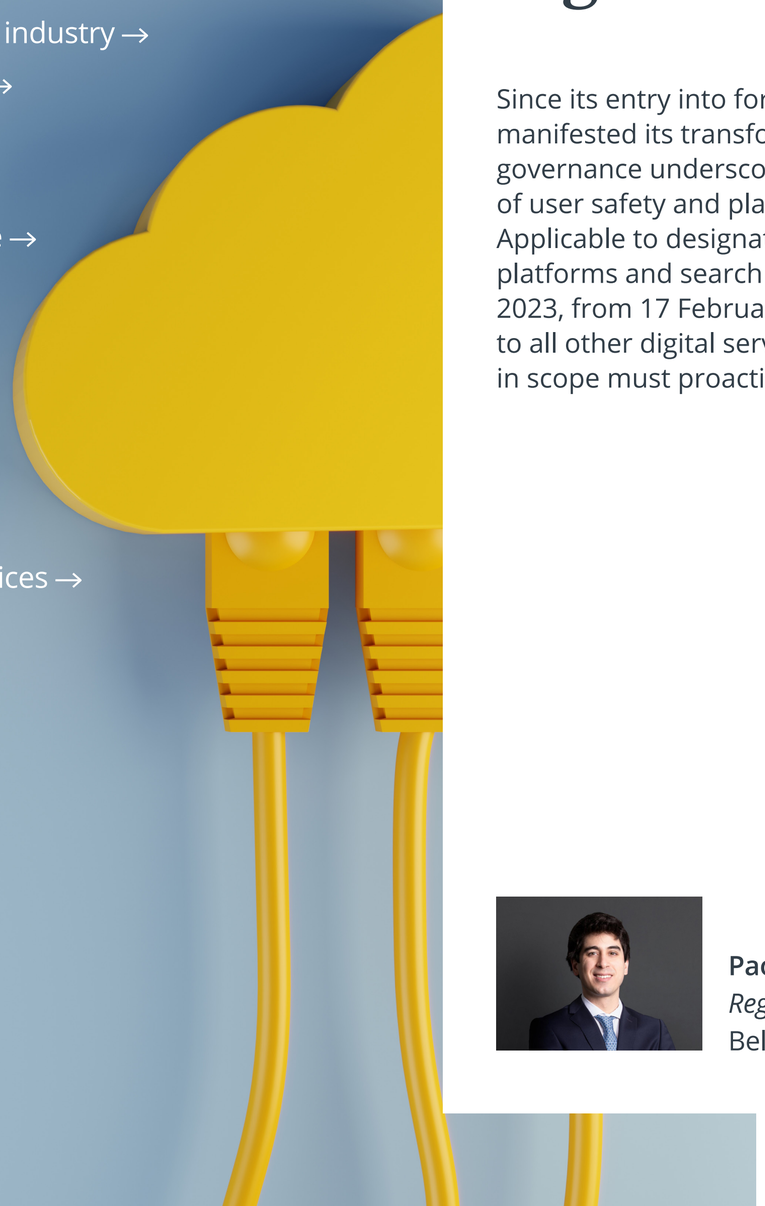


Emergence of specific cloud regulation

The French government and EU institutions are increasingly concerned by the supremacy of US players around cloud technologies whether it is in relation to IaaS, PaaS or SaaS. As cloud becomes more and more prevalent in the digital landscape, this domination is perceived as a threat from a technological, economic and strategic perspective created by dependency towards a certain number of Big Tech players (hyperscalers) notably in the IaaS domain. This situation leads to a certain number of risks identified at national and European level: competition, breach of personal data, damage to business and administration data, undermining sovereignty and the protection of the economic and technological interests of the nation and the EU based on laws with extraterritorial scope, risks of contractual abuse and abuse of technical dependence. As a result, legislators have decided to tackle those risks through policies based on notions such as cloud sovereignty or Trusted Cloud which will rely on both “hard” regulations such as the Data Act (Chapters VI through IX), addressing unfair contractual and commercial practices, switching of service providers, interoperability of services and protection against unlawful international access to data and on certification/ labellisation programs such as SecNumCloud in France or EUCS in the EU. This framework is shaping the premise of a sector specific regulatory environment applicable to the cloud business, which will be relevant for every digital law practitioner in a very near future.

Stéphane Leriche
Partner
France

Cloud & IoT

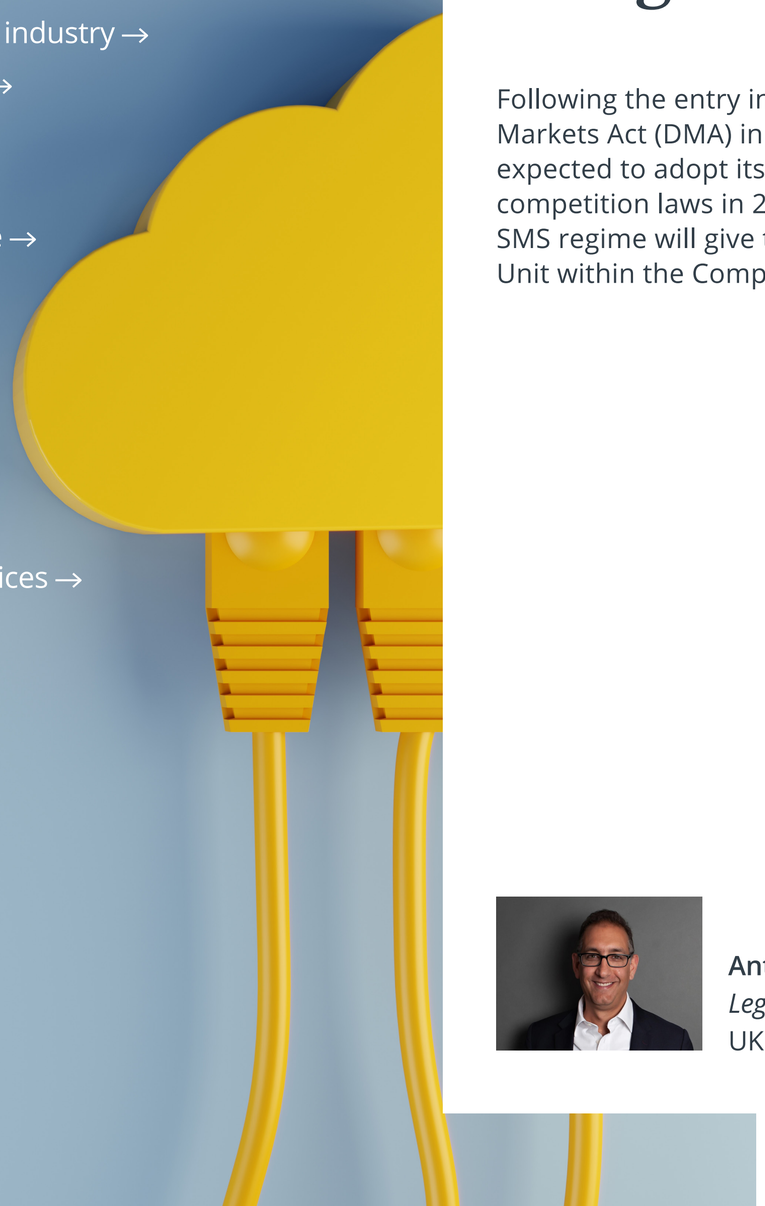


Digital services in the internal market

Since its entry into force, the DSA has already manifested its transformative force in digital governance underscoring the imperative of user safety and platform accountability. Applicable to designated very large online platforms and search engines since August 2023, from 17 February 2024 the DSA will apply to all other digital service providers. Companies in scope must proactively review current policies, products & strategies to assess what changes need to be made to align with DSA requirements. Service providers should also begin drafting a compliance plan to avoid potentially heavy fines. Dialogue with regulators at national level (so-called 'Digital Services Coordinators') is also encouraged after the designations of the DSCs from 17 February 2024.

Paolo Sasdelli
Regulatory And Public Affairs Advisor
Belgium

Cloud & IoT

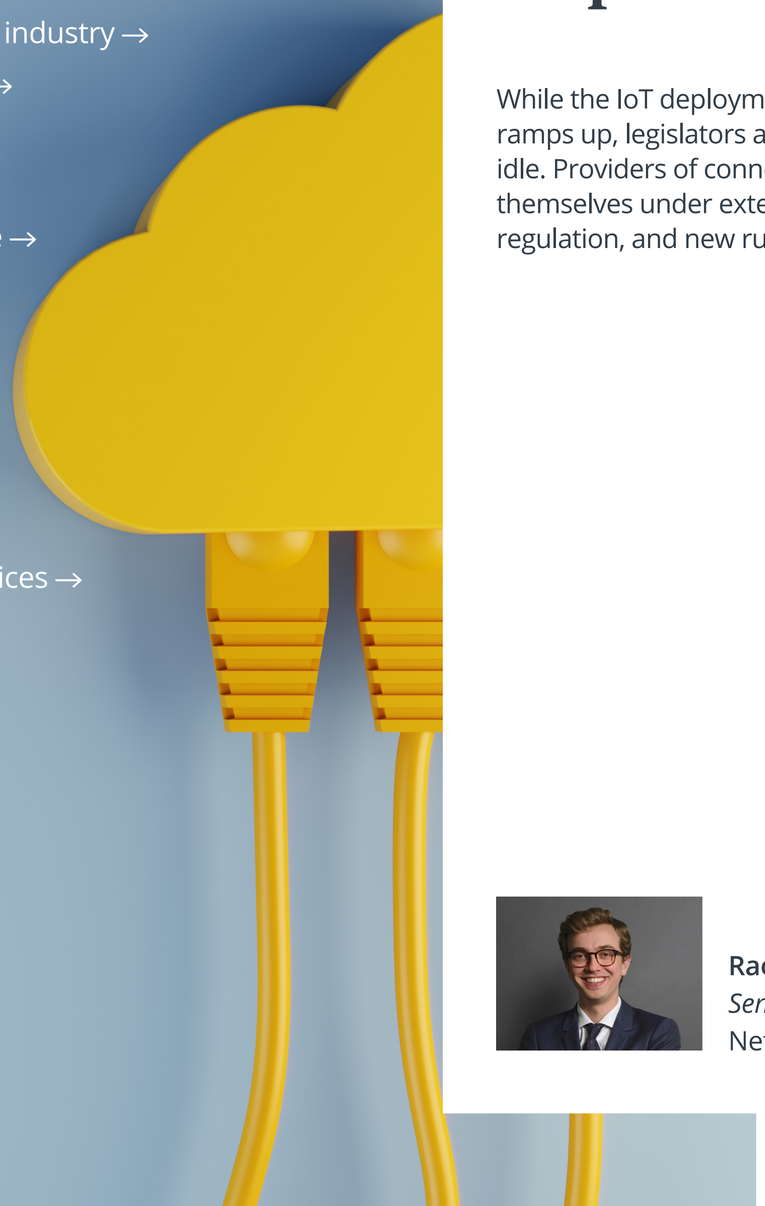


Will gatekeepers be tamed?

Following the entry into force of the Digital Markets Act (DMA) in Brussels, the UK is expected to adopt its new ex ante digital competition laws in 2024. The anticipated SMS regime will give the Digital Markets Unit within the Competition and Markets Authority new powers and the DMU will not hold back from using them. There are also ongoing market investigations into cloud hosting services and other investigations. 2024 promises to be a busy time.

Anthony Rosen
Legal Director
UK

Cloud & IoT

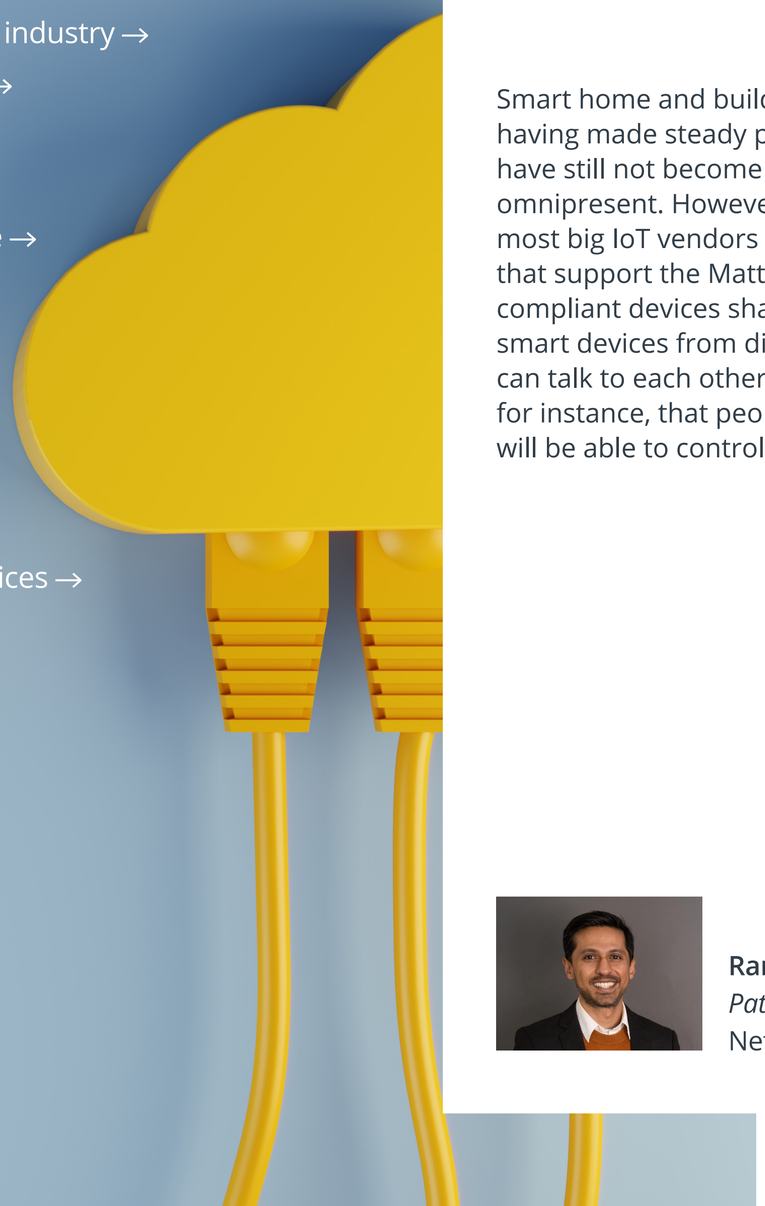


A speed bump for IoT deployment surge

While the IoT deployment continues and even ramps up, legislators and regulators will not sit idle. Providers of connectivity for IoT devices find themselves under extensive telecommunication regulation, and new rules are on the horizon for certain cross-border initiatives. For the IoT device transmitting data and permanently based in a foreign EU nation, known as permanent roaming, legislation and scrutiny are ramping up, ready to fill the regulatory void.

Raoul Grifoni Waterman
Senior Associate
Netherlands

Cloud & IoT

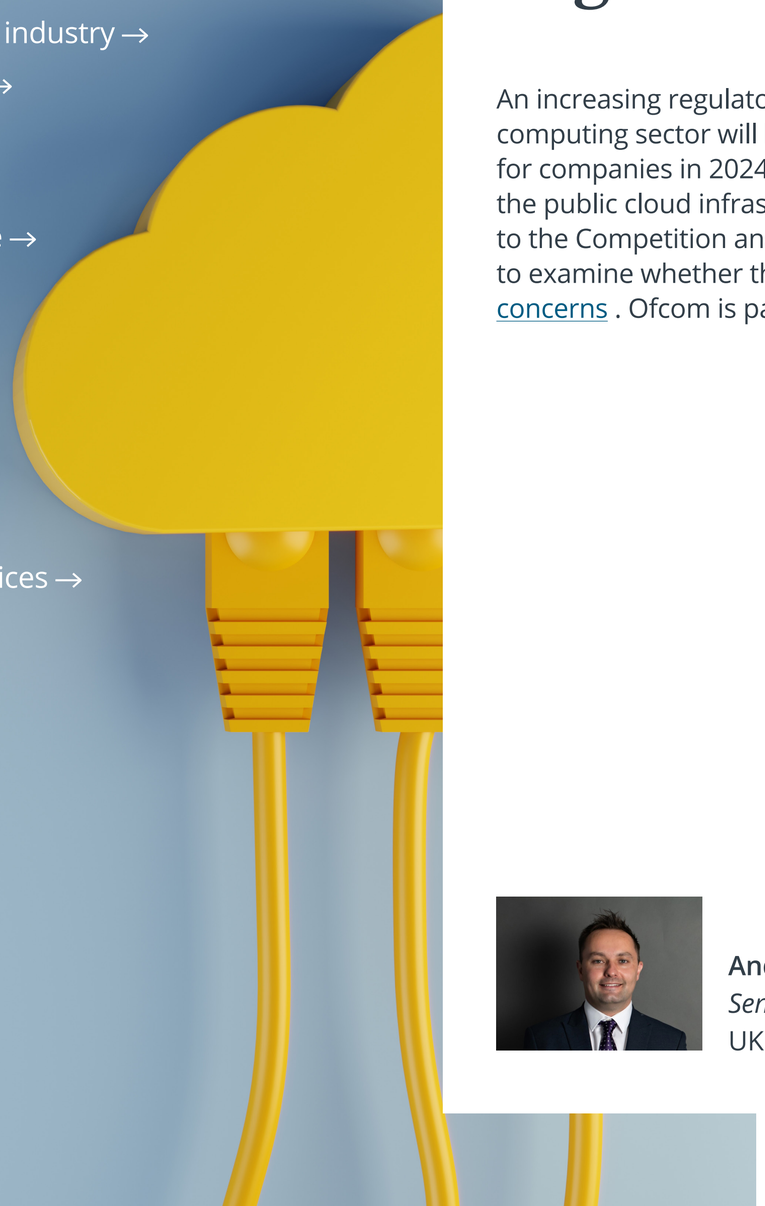


Generative and interoperable IoT

Smart home and building solutions, despite having made steady progress over the years, have still not become highly productive and omnipresent. However, in 2024 and beyond, most big IoT vendors will launch smart devices that support the Matter protocol. These Matter compliant devices shall allow people to deploy smart devices from different vendors which can talk to each other. This would mean, for instance, that people using Apple's Siri will be able to control Google and Amazon based devices. The other feature, apart from interoperability that will redefine smart IoT solutions is the use of generative AI. Currently, the level of automation and intelligence in smart devices is quite limited, often requiring somewhat sophisticated, manual rule creation by users. With the use of generative AI, smart devices will allow greater automation while also catering to non-technical users and shall thus signal the advent of a truly smart and disruptive paradigm.

Rameez Rahman
Patent Attorney
Netherlands

Cloud & IoT

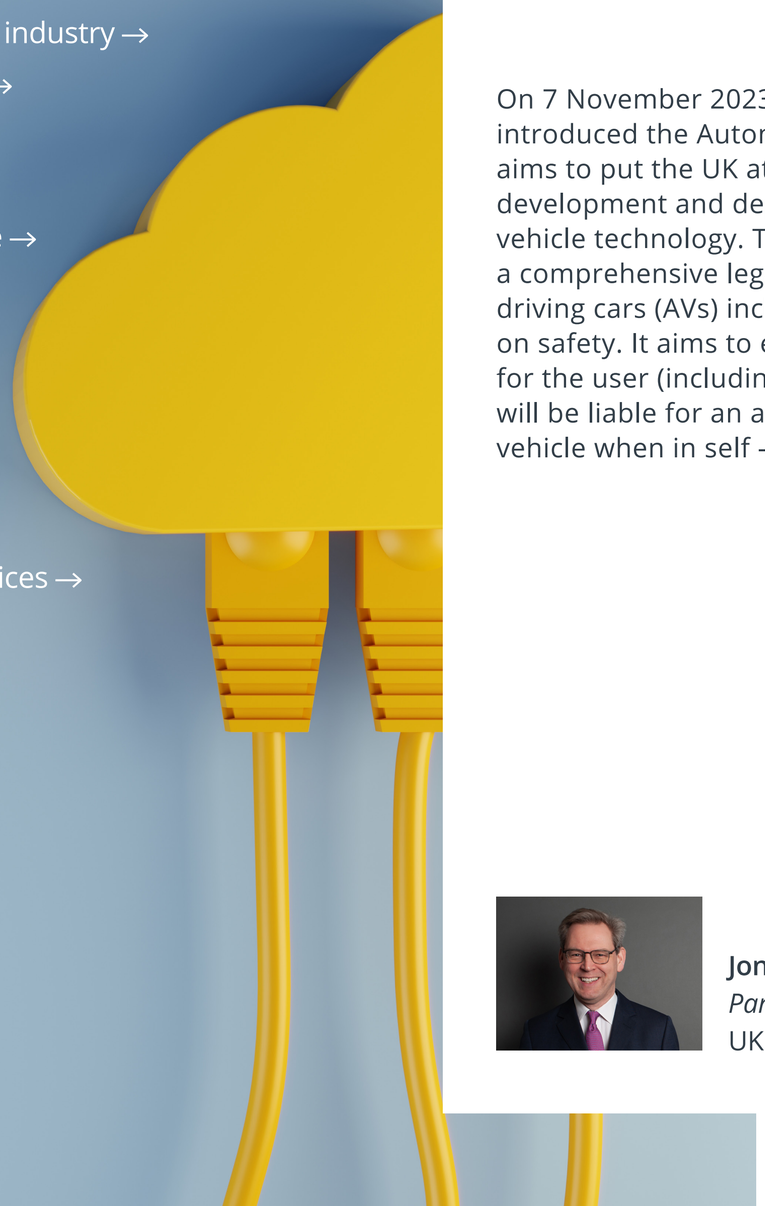


Regulation of cloud in the UK

An increasing regulatory focus around the cloud computing sector will have a significant impact for companies in 2024. Ofcom has referred the public cloud infrastructure services market to the Competition and Markets Authority to examine whether there are competition concerns . Ofcom is particularly concerned about financial and technical 'barriers' to customers switching cloud providers. This is something we encounter when negotiating contracts with cloud providers, where such barriers are often entrenched in their standard terms and conditions and negotiating away from this is difficult.

Andrew Vernon
Senior Associate
UK

Cloud & IoT

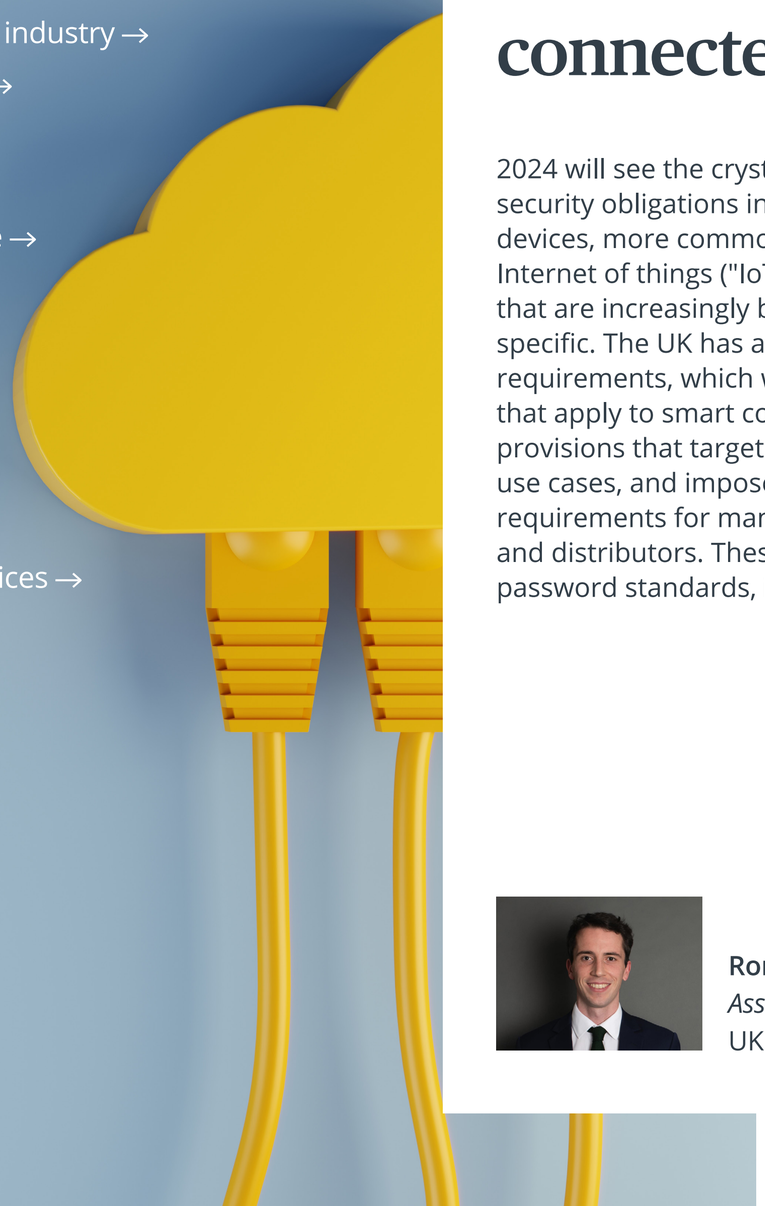


The Automated Vehicles Bill

On 7 November 2023, the UK government introduced the Automated Vehicles Bill which aims to put the UK at the forefront of the development and deployment of self-driving vehicle technology. The Bill is intended to be a comprehensive legal framework for self-driving cars (AVs) including a particular focus on safety. It aims to ensure clearer liability for the user (including that the manufacturer will be liable for an accident caused by the vehicle when in self -driving mode) and set the safety threshold for legal self-driving and establish an “in use” regulatory scheme to monitor the ongoing safety of the vehicles. In introducing the Bill, the government is aiming to promote the UK as a credible market for investment in AVs which it claims could be worth £41.7 billion by 2035. During 2024, expect to see increased investment in technology based on the clearer vision that the government has provided for how AVs will operate on the UK roads.

Jonathan Speed
Partner
UK

Cloud & IoT

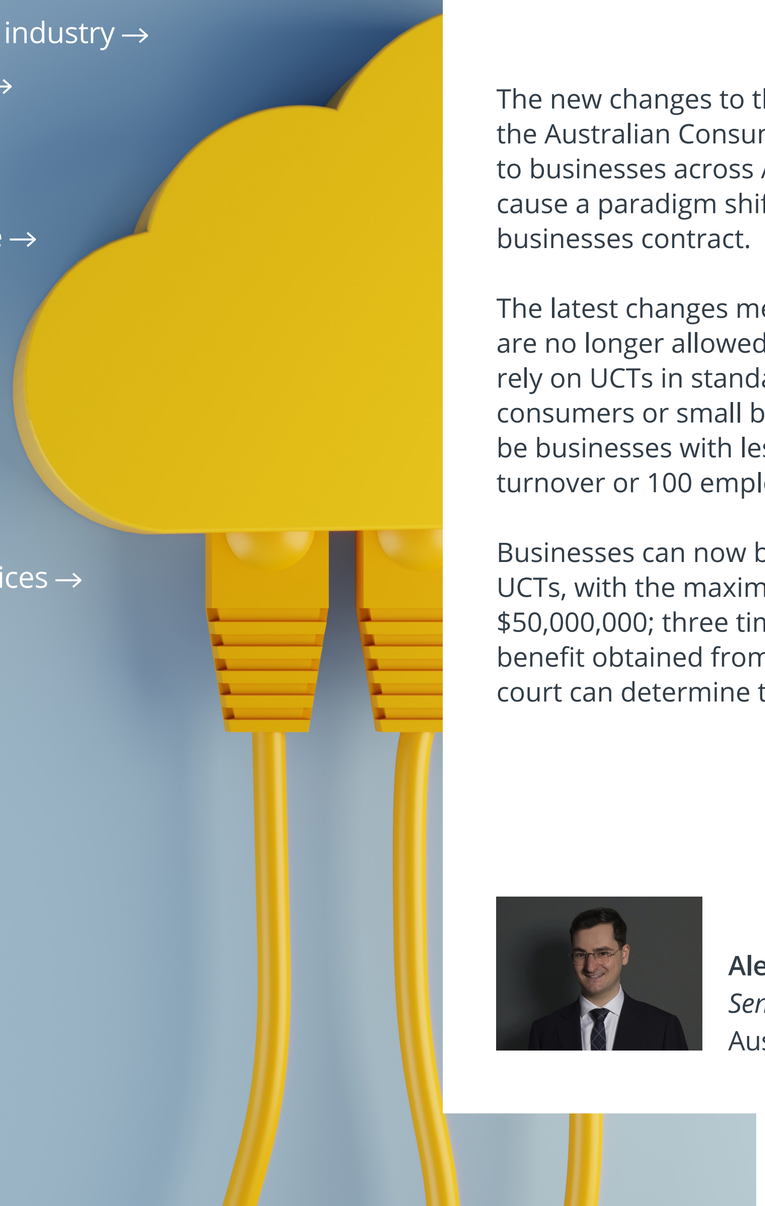


Product security requirements for IoT connected products

2024 will see the crystallisation of product security obligations in Europe for connected devices, more commonly known as the Internet of things ("IoT"), with requirements that are increasingly becoming technology specific. The UK has adopted new security requirements, which will apply from 2024, that apply to smart connected products with provisions that target or exempt specific use cases, and impose minimum security requirements for manufacturers, importers and distributors. These requirements include password standards, information on security updates, duties to respond to security flaws detected in products, and further scope for the government to adopt additional obligations. The EU's equivalent regime is due to be adopted by the start of 2024, which would establish parallel requirements that could diverge from the UK on key definitional points, relevant obligations, or the degree to which they rely on standards set by relevant bodies. 2024 could therefore be a time where the EU and the UK witness diverging regulatory compliance for connected products just as they are increasingly used by consumers.

Rory Coutts
Associate
UK

Cloud & IoT



Australia's unfair contract term (UCT)

The new changes to the UCT regime in the Australian Consumer Law now apply to businesses across Australia, and will cause a paradigm shift in the way tech businesses contract.

The latest changes mean that businesses are no longer allowed to propose, use, or rely on UCTs in standard form contracts with consumers or small businesses (which will now be businesses with less than $10 million annual turnover or 100 employees).

Businesses can now be penalised for using UCTs, with the maximum fine being up to $50,000,000; three times the value of the benefit obtained from the conduct (if the court can determine this); or if a court cannot determine the benefit, 30% of adjusted turnover during the breach period.

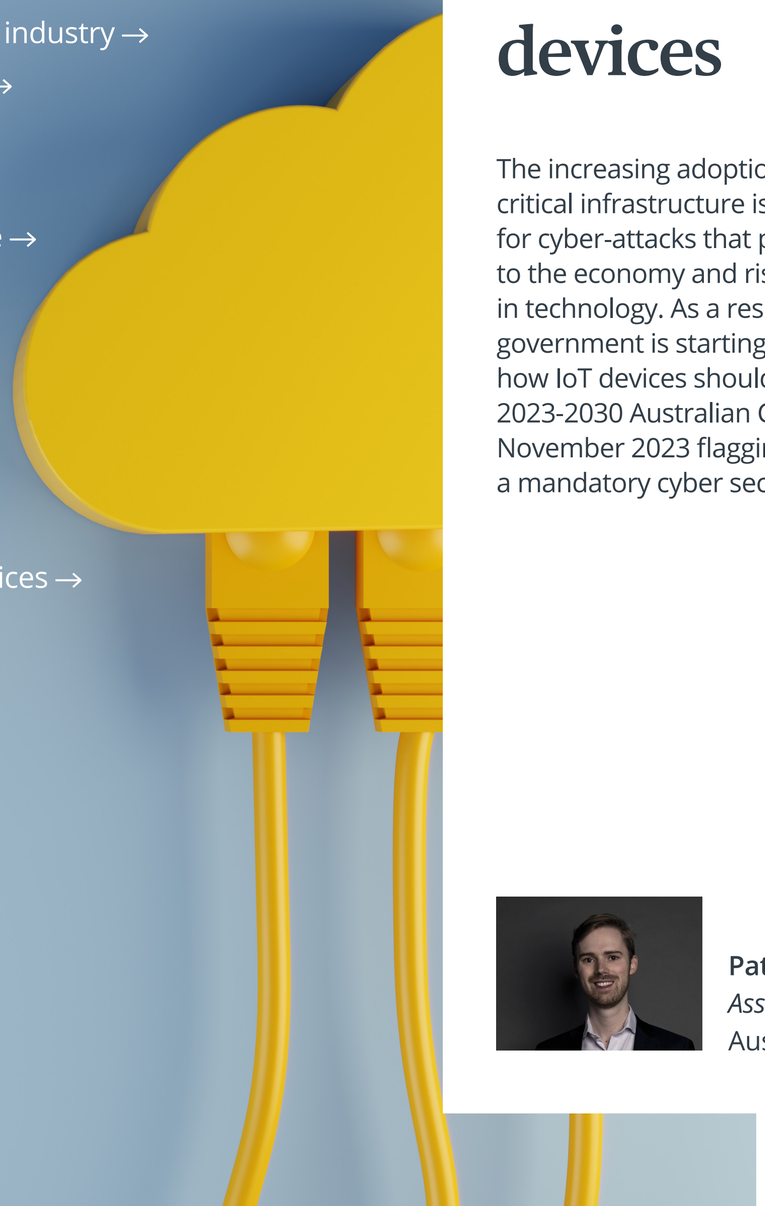
A term is unfair if it causes a “significant imbalance” between the parties that could cause “detriment” and is not in the “legitimate interests” of the party relying on the term. For example, broad, unilateral indemnities (e.g., for breach of privacy laws), automatic term renewals, unilateral termination rights, or charging for a service while the service is not being provided, without appropriate counterbalancing rights, could be unfair.

We expect many tech vendors to adjust their terms over the coming months to move away from extensive T&Cs towards simpler, balanced agreements.

Alex Gulli
Senior Associate
Australia

Hamish Fraser
Partner
Australia

Cloud & IoT



Increasing regulatory scrutiny of IoT devices

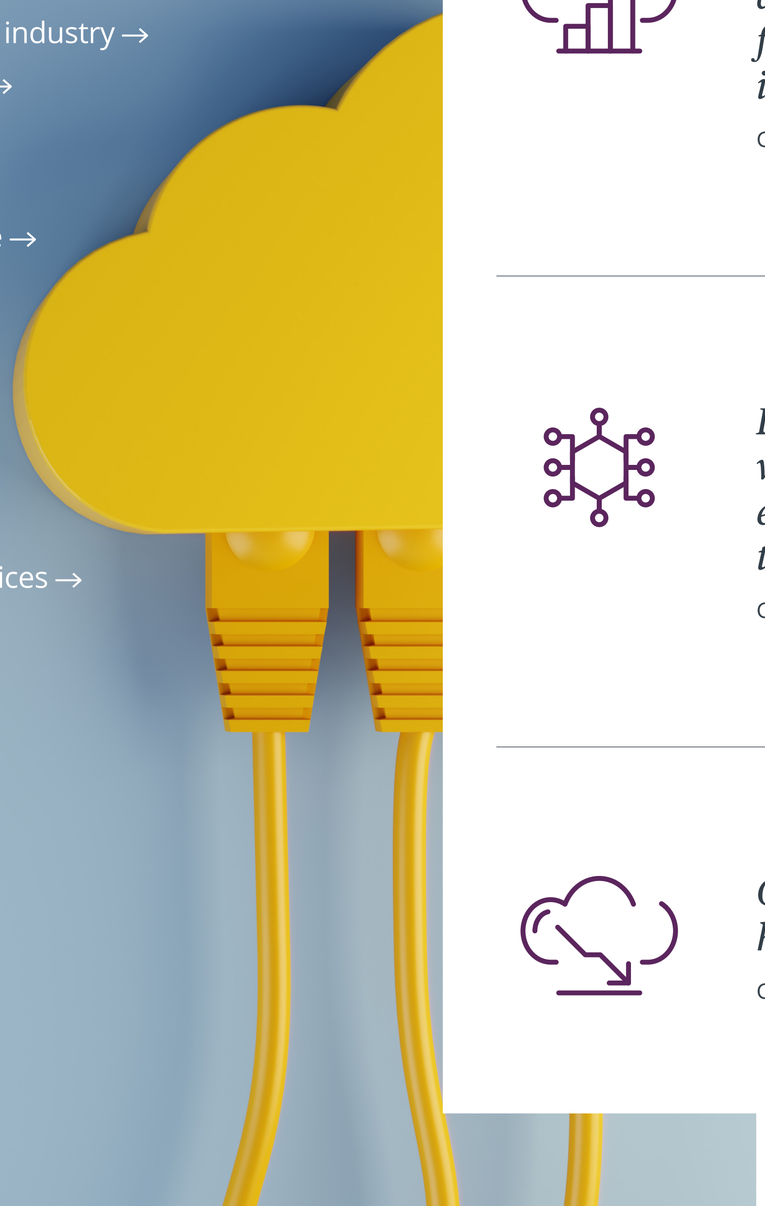
The increasing adoption of IoT technology in critical infrastructure is creating new vectors for cyber-attacks that pose systematic risks to the economy and risk undermining trust in technology. As a result, the Australian government is starting to look more closely at how IoT devices should be regulated, with the 2023-2030 Australian Cyber Strategy published in November 2023 flagging an intention to legislate a mandatory cyber security standard for IoT devices, consistent with the approach recently adopted in the UK.

At the same time, the Australian government is also consulting on how connected vehicles should be regulated, including in relation whether companies selling connected vehicles should be subject to carriage service provider obligations under the existing telecommunications regulatory framework.

Patrick Cordwell
Associate
Australia

Dylan McGirr
Associate
Australia

Cloud & IoT



Cloud computing revenues across all sectors are headed for strong growth, increasing from $552.3 billion in 2021 to $1.2 trillion in 2026

GlobalData

By 2025, data collection and processing will be done increasingly at the edge in embedded systems within IoT devices rather than by central computers

GlobalData

Cloud patent activity peaked in 2020 and has been steadily declining since

GlobalData

NFTs, Tokens and Blockchain

European Blockchain Sandbox bolsters blockchain credibility

Years after the initial blockchain-hype, the use cases where the technology is fit-for-purpose are emerging across a range of industry sectors. Pushed forward by the European Commission's initiative to launch the Blockchain Sandbox, regulators/authorities and innovators are brought together across all industry sectors, allowing regulators/authorities to enhance their knowledge of cutting edge blockchain technologies and allowing innovators to enhance their understanding of relevant laws and regulations. The second round of applications will start in Q1 2024 and will be announced on the project website here.

Raoul Grifoni Waterman
Senior Associate
Netherlands

Quirijn Mohr
Associate
Netherlands

NFTs, Tokens and Blockchain

Use of blockchain technology in ESG compliance (EU passports)

Blockchain technology is revolutionising the way companies approach ESG practices and product passports. With its inherent characteristics of transparency, security, and traceability, blockchain is playing a pivotal role in advancing sustainability and accountability.

Blockchain ensures a transparent and tamper-proof record of a company's ESG impact. Through decentralized ledgers, stakeholders can verify sustainable practices, ethical sourcing, and responsible production methods. This transparency not only fosters trust among consumers but also allows investors to make informed decisions based on authentic and traceable data.

Product passports, a digital representation of a product's life cycle, have also become a focal point for blockchain innovation. By utilizing blockchain, companies can create immutable records that detail a product's journey from raw materials to production and distribution. This ensures that consumers have access to accurate information about a product's environmental impact and ethical considerations.

Blockchain's ability to securely store and share data ensures that product passports are reliable and verifiable. Consumers can make environmentally conscious choices by accessing detailed information about a product's carbon footprint, sourcing practices, and adherence to ethical standards.

Blockchain contributes to supply chain sustainability by enabling real-time tracking and validation of every step in the production process. This not only aids in identifying inefficiencies but also ensures that products meet the highest standards of environmental responsibility.

Sandra Sekula-Baranska
Counsel
Poland

NFTs, Tokens and Blockchain

Singapore positioning itself as a cryptocurrency hub

In August 2023, the Monetary Authority of Singapore released a legal framework for stable coins in an effort to create a welcoming environment for cryptocurrency businesses. Following this development, we anticipate greater acceptance of tokenisation and crypto activities in Singapore and in the APAC region.

Chester Lim
Senior Associate
Singapore

NFTs, Tokens and Blockchain

European Blockchain Sandbox bolsters blockchain credibility →

Use of blockchain technology in ESG compliance (EU passports) →

Singapore positioning itself as a cryptocurrency hub →

More companies, not just crypto-mining firms, are slowly adding bitcoin to their treasuries

GlobalData

Gaming companies in the metaverse will invest in technologies such as AI, AR, VR, 5G, cloud computing, blockchain, and cybersecurity

GlobalData

Payments with blockchain will become more widely adopted, allowing for a higher degree of trust

GlobalData

Quantum Computing

Development of quantum computing

Despite some recent advances in building quantum computing hardware, the development of quantum computers is arguably still at the stage of foundational research. This will likely remain the case for the coming years (with some of the expected “near-term” applications coming from quantum chemistry and material science). At the same time, developments and research in the field of quantum computing, especially quantum algorithms, are providing new ideas for classical computing. This results in what is called quantum inspired computing. There are various practical applications for quantum inspired computing, such as for optimizing transport and logistics. Further inspirations from quantum computing for classical computing are to be expected.

Juliana Kliesch
Senior Associate
Germany

Quantum Computing

Legal risks with the final deployment of quantum technology

The ultimate development and deployment of quantum computing technology will mean an exponential advance in the processing power of systems, which will lead to the need to review the legal risks associated with information processing and real-time decision making. In addition, the popularisation of this technology will mean that current cryptographic encryption systems will need to be reconfigured, requiring a transition towards quantum encryption systems that guarantee the security of information protected by other types of less robust encryption.

Joaquín Muñoz
Partner
Spain

Quantum Computing

Advancements in research and development

Quantum computing is in the R&D stage of its technological life cycle, with further commercialisation anticipated in the coming years. In 2024, we expect to see an increased collaborative approach between academic institutions, research labs and quantum technology companies to enhance the technology. In the UK, additional private investment will help facilitate the R&D as well as UK government-led initiatives, such as the government's new "National Quantum Strategy" which commits to investing £2.5 billion into quantum technology over ten years from 2024 onwards. The UK government will also continue working with researchers and other key players to start preparing a regulatory framework for quantum technology so as to ensure its smooth integration into society.

One area that is impacted by quantum computing is cryptography, as quantum supremacy has the potential to decrypt some traditional encryption methods which are used to keep our personal data secure. Although it is unknown when this potential will be realised, standards organizations are developing and standardizing post-quantum cryptography as a pre-emptive countermeasure. Accordingly, we'll see governments and regulatory bodies begin planning new legal frameworks around cybersecurity and data protection.

Kate Deniston
Professional Support Lawyer
UK

Kaya Sapanoglu
Trainee
UK

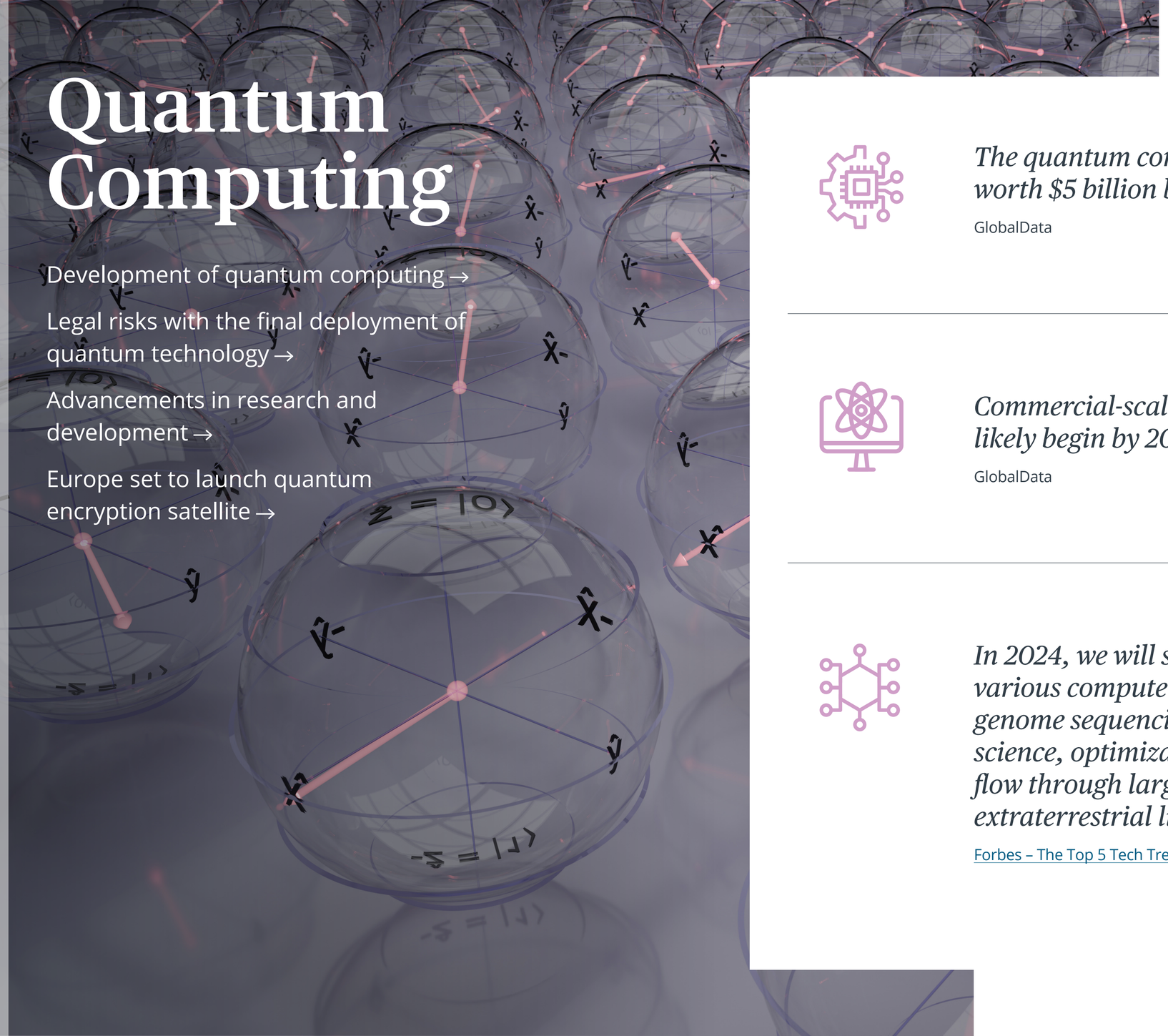
Quantum Computing

Europe set to launch quantum encryption satellite

The European Eagle-1 satellite – a cooperation between ESA, the EU, European national space agencies and European industry - is planned to launch in 2024, providing a European Quantum Key Distribution (QKD) system from space. With QKD it is possible for two parties at a distance to generate a secret key for use in encryption, while being able to detect whether a third party is eavesdropping in the production of the key: if the key generation is successful it is guaranteed that the key was not intercepted. As QKD relies on the quantum mechanical properties of the communication channel used in producing the key, it is not possible to use regular existing communication channels, instead one of the most promising channels is using the quantum physical properties of laser light in laser communication between ground stations via a low-earth orbit satellite. As with any such project the knowledge gained in developing the required technology is valuable in itself ("it's about the journey, not the destination"), so that we should see the benefits of the Eagle-1 project in 2024, even if the actual launch should be delayed.

Peter van Gemert
Partner
Netherlands

Quantum Computing



Development of quantum computing →

Legal risks with the final deployment of quantum technology →

Advancements in research and development →

Europe set to launch quantum encryption satellite →

The quantum computing market will be worth $5 billion by 2025

GlobalData

Commercial-scale quantum computing will likely begin by 2027

GlobalData

In 2024, we will start to see benefits as it's applied across various compute-heavy fields, including drug discovery, genome sequencing, cryptography, meteorology, material science, optimization of complex systems such as traffic flow through large cities, and even the search for extraterrestrial life

Forbes – The Top 5 Tech Trends in 2024

Web3 & the Metaverse

Digital payments in the metaverse

Some of the most interesting trends we are seeing lately are around digital payments and it will be fascinating to see how these developments can enhance user experience in the metaverse. Digital wallets have been mainstream for some time now, however we are seeing wallet providers seek to enhance their relationships with their existing user base by offering additional products and services, such as open banking-powered account information services, giving users a holistic view of their balances and transaction history, within their digital wallet. We expect to see more data-driven metaverse and payments related products over the next 12 months. These products may seek to capitalise on the developing regulation around digital identity and the UK's digital identity and attributes trust framework ("UK DIATF") as well as the rise in the use of contactless payments and digital till systems on the merchant end.

Christina Fleming
Senior Associate
UK

Web3 & the Metaverse

Risks relating to IP and image rights

NFTs are digital tools with wide-ranging possibilities and legal issues, which can be used in the metaverse and represent both physical and digital assets. As a general rule, obtaining a NFT does not entail the acquisition of proprietary rights over the tokenized asset. There is a potential issue of intellectual property and image rights infringement if the corresponding minter generates and offers NFTs involving those rights of another. In the European Union and, specifically, in Spain, the regulation on NFTs is not clear, but several interesting judgments have been delivered on metarverses and NFTs in Spain, and there are already some European and Spanish regulation proposals. In this context, the current situation will probably lead to interesting new legal developments and case-law in 2024.

David Fuentes
Associate
Spain

Web3 & the Metaverse

Australia's perspective on Web3

Web3, being a new iteration of the internet that is anticipated to be more autonomous, decentralised and reliant on crypto assets and blockchain technology, is still at its infancy. While there are presently no regulatory frameworks specifically for Web3 in Australia (other than IP Australia's guidance around trade marks filed in respect of elements of Web3 e.g. virtual goods and NFTs etc., discussed below), it is clear that significant changes will come about in the next few years, with increasing calls from industry for clarity. Australian regulators are becoming more active in relation to Web3, particularly in relation to consumer protection. For example, we have seen the Australian Competition and Consumer Commission impose significant penalties on platform operators (who will play an integral role in Web3) for misleading conduct in relation to the use of consumer data. We anticipate more involvement by consumer and other regulators in the near future.

Shariqa Mestroni
Special Counsel
Australia

Web3 & the Metaverse

Guidance on applications relating to virtual goods, the metaverse, NFTs, and blockchain

In 2023, as a result of the rapid increase in Australian trade mark applications claiming virtual goods (i.e. goods and services in the metaverse, NFTs and goods and services related to blockchain) the Australian Trade Marks Office released a guidance document on the classification of these technologies in Australian trade mark applications. The release of the Australian guidelines follows similar developments internationally, such as the European Union Intellectual Property Office's 2023 draft Guidelines and the Korean IP Office's 2022 examination guidelines for virtual goods. By way of summary, the exact nature of the virtual goods must be specified (e.g. downloadable virtual clothing and downloadable digital music files authenticated by NFTs. Whereas virtual services must take into account the impact of the services in the real world (e.g. a virtual restaurant won't provide real food therefore this is properly classified as an entertainment service).

Shehana Wijesena
Special Counsel
Australia

Web3 & the Metaverse

Digital payments in the metaverse →

Risks relating to IP and image rights →

Australia's perspective on Web3 →

Guidance on applications relating to virtual goods, the metaverse, NFTs, and blockchain →

Over the next five years, more enterprises and consumer brands will invest in video games to enter the metaverse

GlobalData

Augmented reality and virtual reality metaverses will drive consumer engagement and fuel brand loyalty

GlobalData

The metaverse will generate $627 billion in revenue in 2030

GlobalData

5G/6G

Scam calls and numbering

Telecoms regulators across the globe are increasing their focus on telephone numbering requirements in an effort to clamp down on fraudulent and scam calls and messages. We are seeing the tightening of number allocation requirements with increasing obligations on KYC procedures and even prohibtions on number allocation in certain countries. In a similar vein, there are strengthened requirements governing caller line identification requirements as well measues to limit scam calls and mesages. Unified communication providers need to familiarise themselves with the obligations as regulators have taken and are willing to take enforcement action to protect consumers.

Anthony Rosen
Legal Director
UK

5G/6G

SEPs and FRAND licensing: new regulation

SEPs (Standard-essential patents) and the corresponding FRAND (fair, reasonable, and non-discriminatory) licensing terms have been very relevant in relation 4G or 5G standards in recent years. The evolution of technologies has been characterised by the innovation and the improvement of the technological benefits for people. In this context, SEP-related disputes have reached several European and Spanish courts. In April 2023 the European Commission published a proposal of direct regulation in the FRAND domain. For this reason, it will be necessary to keep an eye on this potential new regulation on SEP-related matters in relation to the 5G and 6G standardisation process.

David Fuentes
Associate
Spain

5G/6G

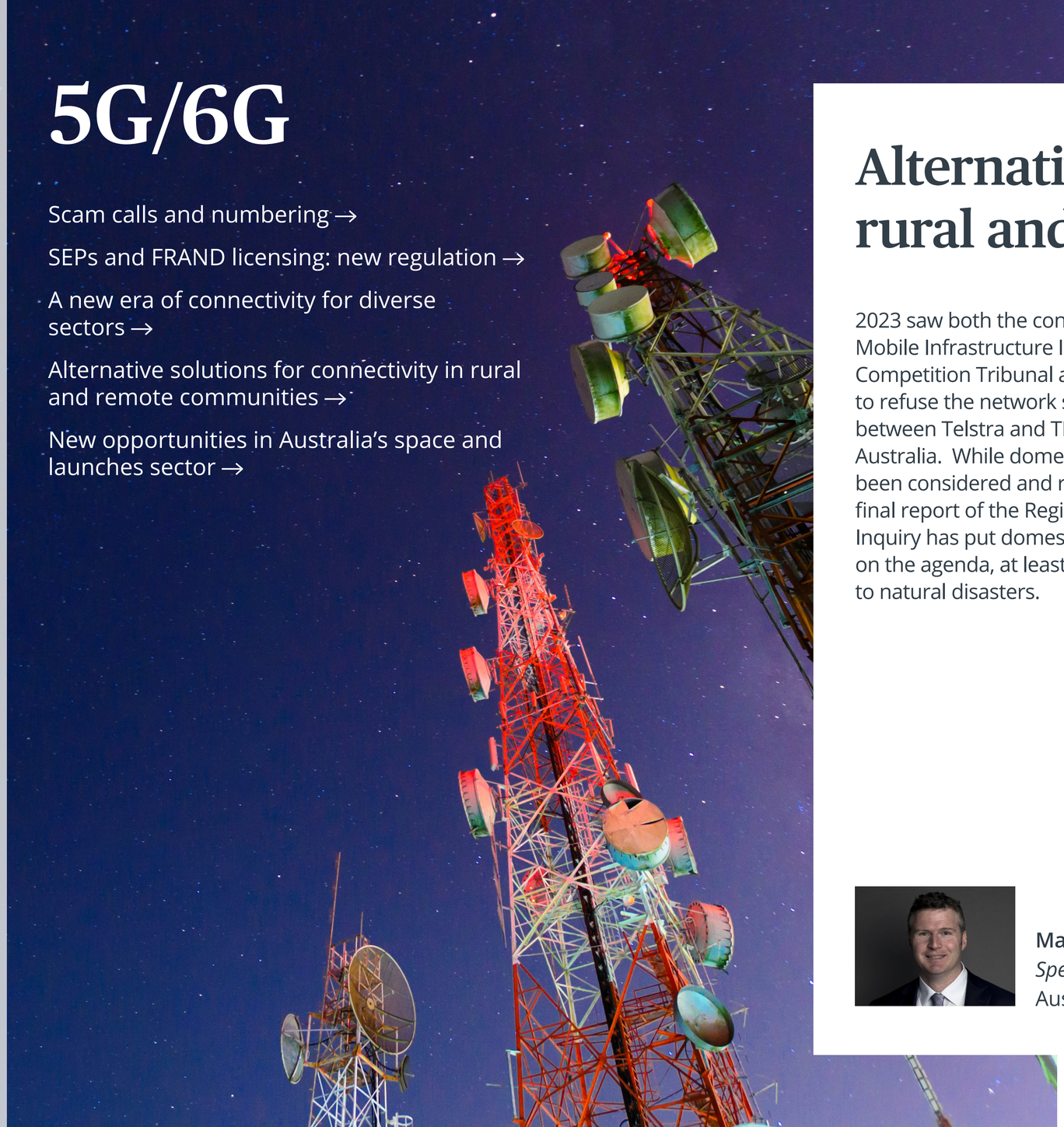
A new era of connectivity for diverse sectors

A major Swedish telecom company has demonstrated the potential of 5G beyond telecommunications by growing a '5G onion'. This innovation shows how 5G can revolutionize the food industry. Using the 5G network and new technology, food can be produced with less chemical treatment, yet have a longer shelf life. This is made possible by enabling complex heavy machines to operate in fields, such as a robot that identifies and removes weeds, reducing the need for herbicides. The entry of 5G into the food industry marks an exciting advancement in food tech. This is just one of many use cases for 5G, as its allowance for quicker and increased data flows combined with off-site processing capabilities can bring more tech to remote places like farms. We're just seeing the beginning of this transformation in the food industry and food tech and believe much more is to come.

Julia Jansson
Associate
Sweden

Hans Kalderén
Associate
Sweden

5G/6G



Alternative solutions for connectivity in rural and remote communities

2023 saw both the conclusion of the Regional Mobile Infrastructure Inquiry and the Australian Competition Tribunal affirm the ACCC's decision to refuse the network sharing arrangement between Telstra and TPG for remote and regional Australia. While domestic roaming has previously been considered and rejected by the ACCC, the final report of the Regional Mobile Infrastructure Inquiry has put domestic mobile roaming back on the agenda, at least as a temporary response to natural disasters.

In light of a recent significant mobile outage in Australia and a resulting Senate Inquiry, we expect to see calls for mobile roaming to go further and extend to regional and rural Australia more broadly.

Separately, the ACMA has launched a consultation on the regulatory environment for satellite direct-to-mobile services. It seems likely that the ACMA will embark on further reforms to enable this service for remote and rural users.

Matthew Bovaird
Special Counsel
Australia

Thomas Jones
Partner
Australia

5G/6G

New opportunities in Australia’s space and launches sector

There will likely be increased opportunities for collaboration and investment in Australia’s space and launch sectors following the signing of the Technology Safeguards Agreement (‘TSA’) between Australia and the United States on 26 October 2023. The TSA is designed to protect U.S space technology, while supporting the launch of space launch vehicles and satellites from Australia. The countries have also announced that a new Australia-based ground station will be set up to support NASA’s Artemis Program, and, separately, that the countries are prioritising integration and cooperation in space for defence and security. The TSA will likely provide Australian space companies with access to international markets and increased opportunities for collaboration and investment. However, one potential concern surrounds the impact of the TSA on Australia’s sovereign space capability if Australia develops a reliance on the United States for space technology and data.

Dylan McGirr
Associate
Australia

5G/6G

Scam calls and numbering →

SEPs and FRAND licensing: new regulation →

A new era of connectivity for diverse sectors →

Alternative solutions for connectivity in rural and remote communities →

New opportunities in Australia's space and launches sector →

By 2025, a connectivity performance rating is mandated as part of the sale of any property in a major European market

CCS Insight's predictions for 2024

15% of smartphone users have satellite-enabled devices by 2027

CCS Insight's predictions for 2024

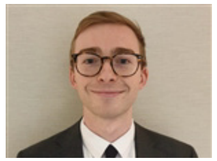
Over the next three years, China, the US, Europe, and Japan will aggressively build out their 5G infrastructures, with China already outpacing the rest.

GlobalData

Country contacts

Australia

Alex Gulli, *Senior Associate*
+61 2 9226 9888
alex.gulli@twobirds.com



Dylan McGirr, *Associate*
+61 2 9226 9888
dylan.mcgirr@twobirds.com

Emma Croft, *Senior Associate*
+61 2 9226 9888
emma.croft@twobirds.com

Hamish Fraser, *Partner*
+61 2 9226 9888
hamish.fraser@twobirds.com

James Hoy, *Senior Counsel*
+61 2 9226 9888
james.hoy@twobirds.com

Jonathon Ellis, *Partner*
+61 2 9226 9888
jonathon.ellis@twobirds.com

Julie Cheeseman, *Partner*
+61 2 9226 9888
julie.cheeseman@twobirds.com

Katrina Dang, *Senior Associate*
+61 2 9226 9888
katrina.dang@twobirds.com

Matthew Bovaird, *Special Counsel*
+61 2 9226 9888
matthew.bovaird@twobirds.com

Patrick Cordwell, *Associate*
+61 2 9226 9888
patrick.cordwell@twobirds.com

Shariqa Mestroni, *Special Counsel*
+61 2 9226 9888
shariqa.mestroni@twobirds.com

Shehana Wijesena, *Special Counsel*
+61 2 9226 9888
shehana.wijesena@twobirds.com

Thomas Jones, *Partner*
+61 2 9226 9888
thomas.jones@twobirds.com

Belgium

Francine Cunnigham, *Regulatory and Public Affairs Director*
+32 (0)2 282 6000
francine.cunningham@twobirds.com

Paolo Sasdelli, *Regulatory and Public Affairs Advisor*
+32 (0)2 282 6000
paolo.sasdelli@twobirds.com

China

James Gong, *Partner*
+86 10 5933 5688
james.gong@twobirds.com

Tanya Luo, *Associate*
+86 10 5933 5688
tanya.luo@twobirds.com

Wilfred Ng, *Partner*
+852 2248 6000
wilfred.ng@twobirds.com

Denmark

Anna Hjortlund, *Associate*
+45 2290 6052
anna.hjortlund@twobirds.com

Jesper Langemark, *Partner*
+45 22 26 20 02
jesper.langemark@twobirds.com

Mathias Mølsted Andersen, *Senior Associate*
+45 28 90 15 80
mathias.andersen@twobirds.com

Mogens Dyhr Vestergaard, *Senior Counsel*
+45 30 85 13 42
mogens.vestergaard@twobirds.com

Finland

Tobias Bräutigam, *Partner*
+358 (0)9 622 6670
tobias.brautigam@twobirds.com

France

Anne-Sophie Lampe, *Partner*
+33 (0)1 42 68 6000
anne-sophie.lampe@twobirds.com

Caroline Arrighi-Savoie, *Associate*
+33 (0)1 42 68 6000
caroline.arrighi-savoie@twobirds.com

Djazia Tiourtite, *Partner*
+33 (0)1 42 68 6000
djazia.tiourtite@twobirds.com

Emmanuelle Porte, *Partner*
+33 (0)1 42 68 6000
emmanuelle.porte@twobirds.com

Oriane Zubcevic, *Associate*
+33 (0)1 42 68 6000
oriane.zubcevic@twobirds.com

Stéphane Leriche, *Partner*
+33 (0)1 42 68 6000
stephane.leriche@twobirds.com

Germany

Christian Lindenthal, *Partner*
+49 (0)89 3581 6000
christian.lindenthal@twobirds.com

Dirk Barcaba, *Partner*
+49 (0)69 74222 6000
dirk.barcaba@twobirds.com

Finja Schlingmann, *Associate*
+49 (0)69 74222 6000
finja.schlingmann@twobirds.com

Juliana Kliesch, *Senior Associate*
+49 (0)69 74222 6000
juliana.kliesch@twobirds.com

Natallia Karniyevich, *Senior Associate*
+49 (0)69 74222 6000
natallia.karniyevich@twobirds.com

Nils Lölfing, *Counsel*
+49 (0)69 74222 6000
nils.loelfing@twobirds.com

Ireland

Anna Morgan, *Partner*
+353 1 (0)574 9850
anna.morgan@twobirds.com

Deirdre Kilroy, *Partner*
+353 1 (0)574 9850
deirdre.kilroy@twobirds.com

Georgina Parkinson, *Associate*
+353 1 (0) 574 9850
georgina.parkinson@twobirds.com

Kelly Mackey, *Associate*
+353 1 (0)574 9850
kelly.mackey@twobirds.com

Megan Kearns, *Associate*
+353 1 574 9850
megan.kearns@twobirds.com

Shauna Joyce, *Associate*
+353 1 (0)574 9850
shauna.joyce@twobirds.com

Netherlands

Feyo Sickinghe, *Of Counsel*
+31 (0)70 353 8800
feyo.sickinghe@twobirds.com

Hester Borgers, *Associate*
+31 (0)70 353 8800
hester.borgers@twobirds.com

Pauline Kuipers, *Partner*
+31 (0) 70 353 8810
pauline.kuipers@twobirds.com

Peter van Gemert, *Partner*
+31 (0)70 353 8800
peter.van.gemert@twobirds.com

Quirijn Mohr, *Associate*
+31 (0)70 353 8800
quirijn.mohr@twobirds.com

Rameez Rahman, *Patent Attorney*
+31 (0)70 353 8800
rameez.rahman@twobirds.com

Raoul Grifoni Waterman,
Senior Associate
+31 (0)70 353 8800
raoul.grifoniwaterman@twobirds.com

Shima Abbady, *Associate*
+31 (0)70 353 8800
shima.abbady@twobirds.com

Poland

Kuba Ruiz, *Senior Counsel*
+48 22 583 79 00
kuba.ruiz@twobirds.com

Monika Hughes, *Counsel*
+48 22 583 79 00
monika.hughes@twobirds.com

Pawel Lipski, *Partner*
+48 22 583 79 00
pawel.lipski@twobirds.com

Sandra Sekula-Baranska, *Counsel*
+48 22 583 79 00
sandra.sekula-baranska@twobirds.com

Tomasz Zalewski, *Partner*
+48 22 583 79 00
tomasz.zalewski@twobirds.com

Singapore

Aurore Dacier de Biasi, *Associate*
+65 6534 5266
aurore.dacier@twobirds.com

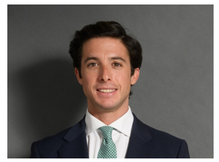
Chester Lim, *Senior Associate*
+65 6534 5266
chester.lim@twobirds.com

Jeremy Tan, *Partner*
+65 6534 5266
jeremy.tan@twobirds.com

Spain

Celia Bouzas, *Senior Associate*
+34 91 790 6000
celia.bouzas@twobirds.com

David Fuentes, *Associate*
+34 91 790 6000
david.fuentes@twobirds.com



Ignacio Belmar, *Associate*
+34 91 790 6000
ignacio.belmar@twobirds.com

Joaquin Muñoz, *Partner*
+34 91 790 6000
joaquin.munoz@twobirds.com

Pablo Berenguer, *Partner*
+34 91 790 6000
pablo.berenguer@twobirds.com

Sweden

Ariana Sohrabi, *Senior Associate*
+46 (0)8 506 320 00
ariana.sohrabi@twobirds.com

Hans Kaldéren, *Associate*
+46 (0)8 506 320 00
hans.kalderen@twobirds.com

Julia Jansson, *Associate*
+46 (0)8 506 320 00
julia.jansson@twobirds.com

Magda Lundh Woldegiorgis, *Associate*
+46 (0)8 506 320 00
magda.lundh@twobirds.com

Mattias Lindberg, *Partner*
+46 (0)8 506 320 00
mattias.lindberg@twobirds.com

UAE

Nona Keyhani, *Associate*
+971 4 309 3222
nootash.keyhani@twobirds.com

UK

Antony Rosen, *Legal Director*
+44 (0)20 7415 6000
antony.rosen@twobirds.com

Andrew Vernon, *Senior Associate*
+44 (0)20 7415 6000
andrew.vernon@twobirds.com

Christina Fleming, *Senior Associate*
+44 (0)20 7415 6000
christina.fleming@twobirds.com

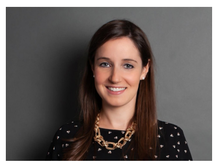
Furat Ashraf, *Partner*
+44 (0)20 7415 6000
furat.ashraf@twobirds.com

Hayley Blyth, *Associate*
+44 (0)20 7415 6000
hayley.blyth@twobirds.com

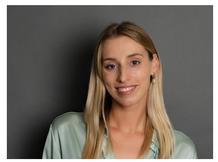
James Moss, *Partner*
+44 (0)20 7415 6000
james.moss@twobirds.com

Jeremy Sharman, *Partner*
+44 (0)20 7415 6000
jeremy.sharman@twobirds.com

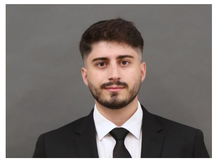
Jonathan Speed, *Partner*
+44 (0)20 7415 6000
jonathan.speed@twobirds.com



Kate Deniston, *Professional Support Lawyer*
+44 (0)20 7415 6000
kate.deniston@twobirds.com



Kathryn Parker, *Associate*
+44 (0)20 7415 6000
kathryn.parker@twobirds.com



Kaya Sapanoglu, *Trainee*
+44 (0)20 7415 6000
Kaya.Sapanoglu@twobirds.com

Matthew Buckwell, *Senior Associate*
+44 (0)20 7415 6000
matthew.buckwell@twobirds.com

Rory Coutts, *Associate*
+44 (0)20 7415 6000
rory.coutts@twobirds.com

Russell Williamson, *Senior Associate*
+44 (0)20 7415 6000
russell.williamson@twobirds.com

Simon Shooter, *Partner*
+44 (0)20 7415 6000
simon.shooter@twobirds.com

Sophie Phillips, *Senior Associate*
+44 (0)20 7415 6000
sophie.phillips@twobirds.com

Toby Bond, *Partner*
+44 (0)20 7415 6000
toby.bond@twobirds.com

Will Bryson, *Senior Associate*
+44 (0)20 7415 6000
will.bryson@twobirds.com

"Technology, media and communications form a core part of the firm's global offering, which incorporates market-leading teams across Europe, Asia-Pacific and the Middle East."

Chambers Global 2023 – Ranked band 1 for TMT

twobirds.com