Bird & Bird

One firm.
Your firm.

Tech & Comms Challenges, Opportunities and Predictions 2023

Introduction

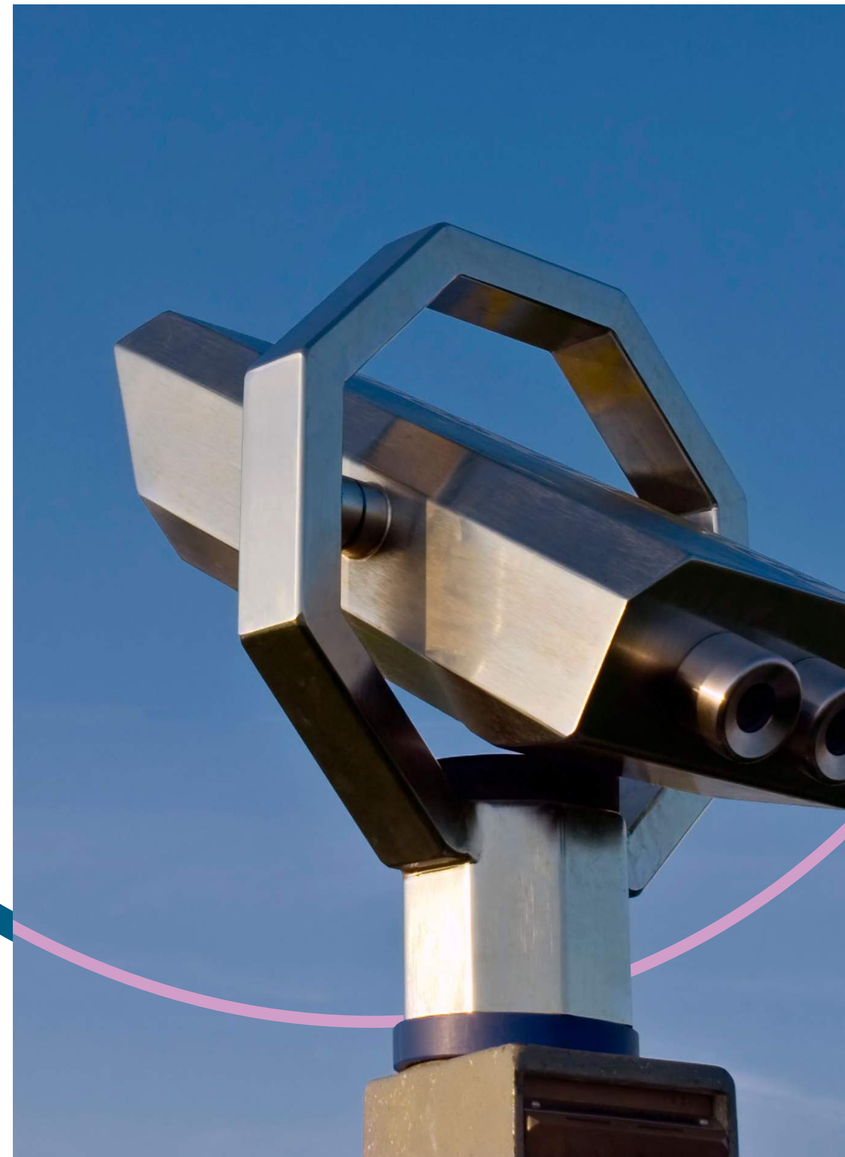
2022 saw an easing of lockdowns and restrictions imposed during the Covid pandemic, heralding a return to normality in many parts of the world. However, several global crises raised a new set of challenges: the Ukraine War, the climate crisis, escalating energy prices and the resulting impact on inflation, geopolitical instability as well as the threat of recession. Their impact is felt in different ways across the tech sector.

Against this backdrop we have seen our clients redefine the way they work, their focus and their ambitions, most notably in the area of Environmental, Social and Governance (ESG). Economic headwinds have caused companies to prioritise their innovation and change agendas. At the same time governments around the globe assess the need for new regulation, both for our climate and digital environment.

The easing of travel restrictions allowed our Tech lawyers to meet with their international colleagues and clients for the first time in two years. We used these opportunities to discuss and debate the issues that our clients across the globe have identified as being of significant importance to their business, for the way they innovate, operate and to become more resilient in the face of the challenges posed by the digital world and ESG considerations.

Nine areas featured heavily in our discussions, namely: Artificial Intelligence; Cloud & IoT; Cyber Security; Data; ESG itself; 5G & 6G; the Metaverse; NFTs, Tokens & Blockchains and, finally, Quantum Computing.

This 2023 report draws together a range of predictions and observations from our Tech & Comms lawyers, focusing on these nine areas and the developments we expect to see over the coming year.



Intellectual property

"A key IP issue will be whether the outputs of generative AI systems qualify for IP protection" *Read more →*

Employment

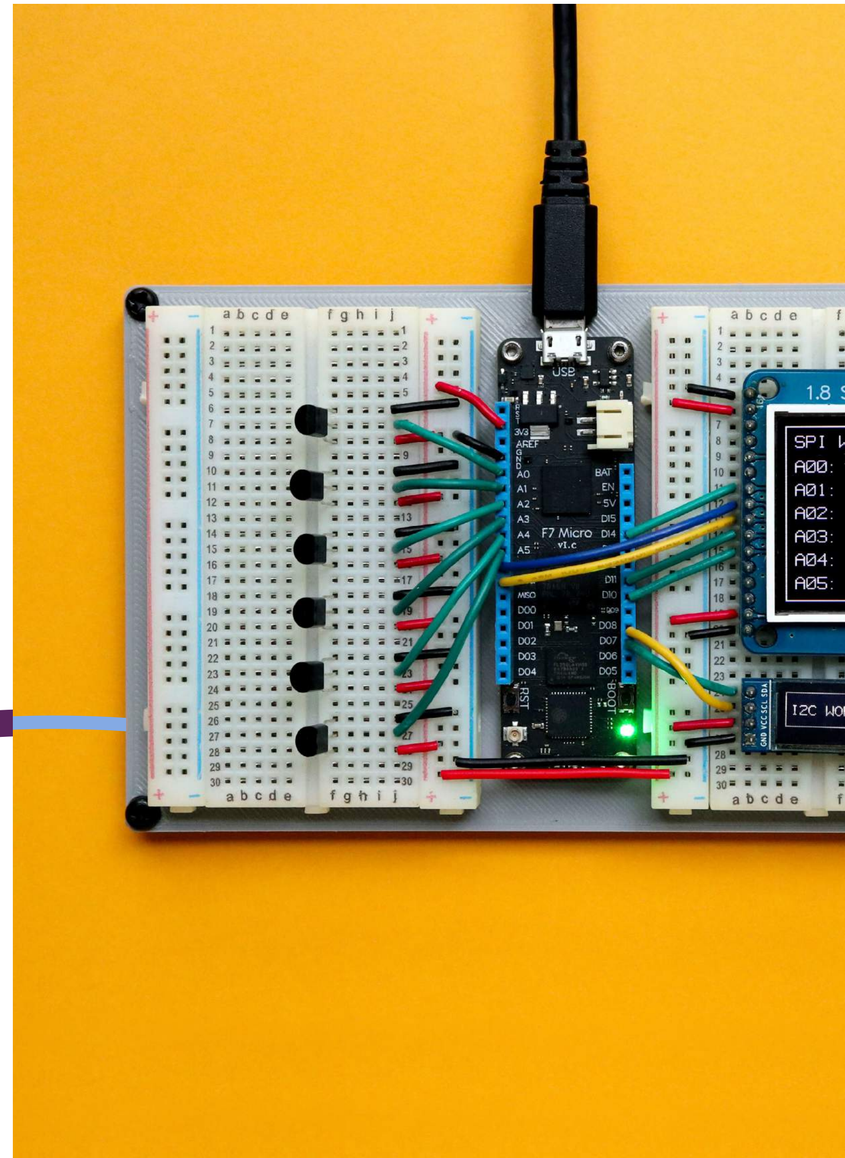
"2023 will see risk and compliance at the forefront of the people management agenda" *Read more →*

Corporate

"Investments will be driven by ESG and digital infrastructure"

Commercial

"International regulations will increasingly drive contracts in 2023"



Cloud & IoT

READ MORE →

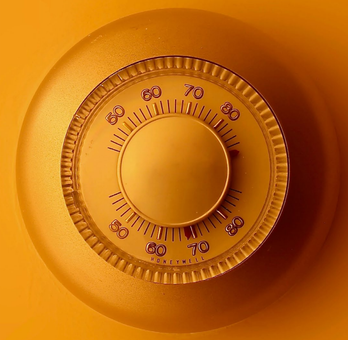
Cyber Security

READ MORE →

Metaverse

READ MORE →

Data

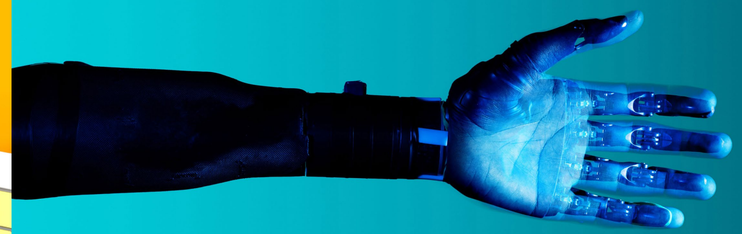


READ MORE →

5G/6G

READ MORE →

Artificial Intelligence

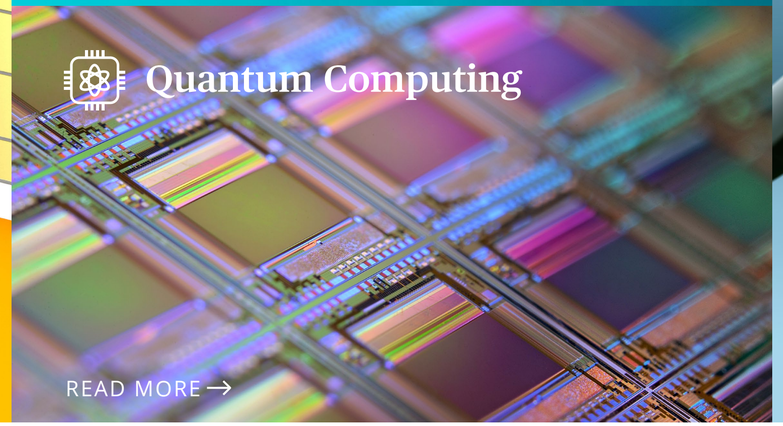


READ MORE →

ESG

READ MORE →

Quantum Computing

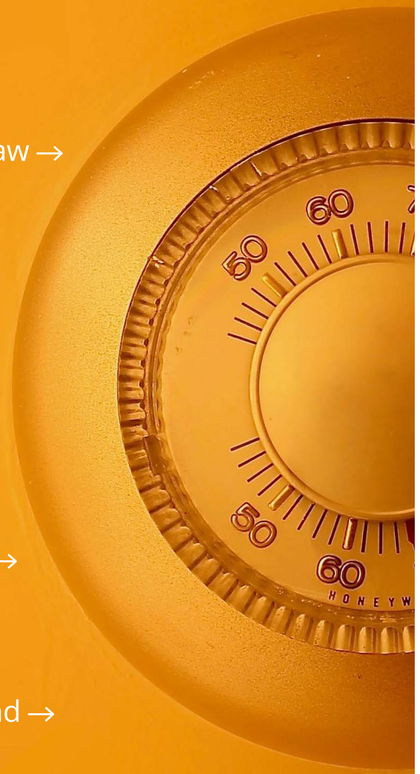


READ MORE →

NFTs, Tokens & Blockchains

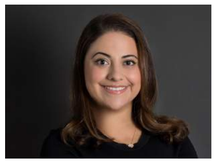
READ MORE →

Data



Data protection in the GCC countries

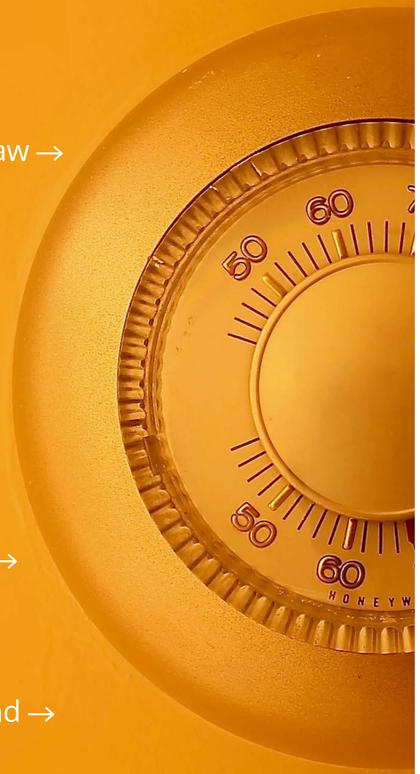
The GCC are increasingly focused on advanced digital technologies as a source of future growth. The deployment of innovative products and services involving AI, blockchain, IoT and AR relies heavily on data. In turn, GCC countries have identified the need for legal frameworks aligned with international standards to govern the growing focus on commercialising data. They have introduced a number of new privacy laws with Bahrain and Qatar taking the lead, followed more recently by the Kingdom of Saudi Arabia, Sultanate of Oman and United Arab Emirates. The move underlines the positional transformation from hydrocarbon to data-driven economies in the region and the related investment in large scale digital infrastructure and projects going forward.



Nona Keyhani
Associate
UAE

David Bintliff
Partner
UAE

Data



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 will force digital health providers to meet a series of new legal requirements applicable to the systems they use for processing health data. The regulation covers health data exchange between patients and health professionals as well as the secondary use of such data.

The initiative *MyHealth@EU* will be focused on health data exchange between patients and health professionals across member states. The aim is to give European citizens, travelling or living abroad, access to the same healthcare as they would have in their home country.

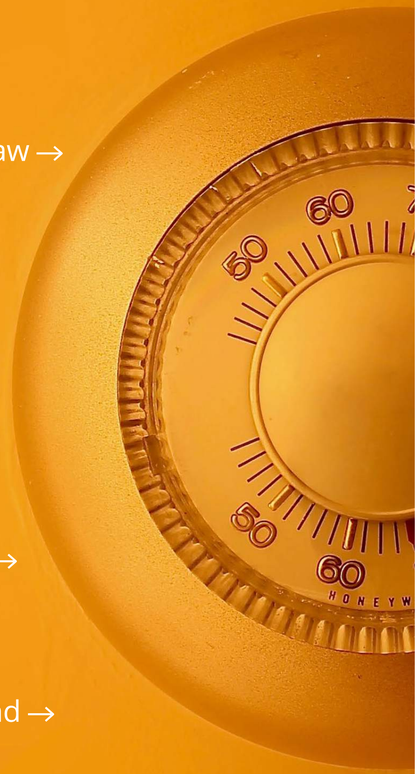
The initiative *HealthData@EU* will be focused on the secondary use of data. Researchers, policymakers and companies will be able to use and study patients' medical records if they receive a permit from a health data access body that will be set up in each member state.

The EHDS will put the EU at the forefront of big data and enable life sciences companies to access health data in a new way which will lead to further development and innovation, as well as reshape the way patients approach their health.

Ariana Sohrabi
Associate
Sweden

Mattias Lindberg
Partner
Sweden

Data



Approaching the demands of the digital decade

Europe's current "Digital Decade", with its onslaught of legislative enactments, comes during a time when compliance teams are under increasing pressure, due to diminishing resources in both capacity and budget. Although tempting to place additional compliance responsibilities on internal teams, doing so can create challenges in both talent retention and legislative compliance. Instead, we suggest that you do the following:

(i) Assess your current approach to compliance – what has worked well and how can this be used in future compliance work;

(ii) Implement tools slowly – consider the effectiveness of tolls and adapt accordingly;

(iii) Educate and support your compliance teams in any new roles or responsibilities they take on – do not leave them stranded; and

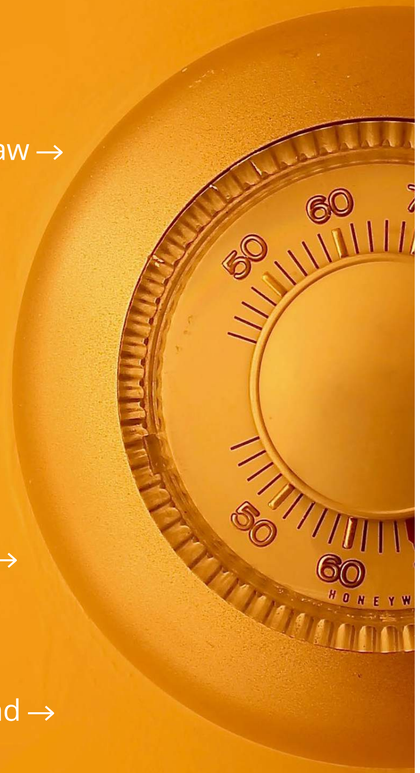
(iv) Avoid overloading your existing workforce – retaining your talent is key! Further information can be found in this article written by the Bird & Bird International HR Service and experts in Tech & Comms.

Ariana Sohrabi
Associate
Sweden

Beatrice Duke
Associate
Sweden

Hans Kaldéren
Trainee
Sweden

Data



Digital Services Act

The countdown has begun to the effective application of the new EU Digital Services Act (DSA), which introduces significant new obligations for providers of digital services, including online marketplaces, social media and search engines. Very large players will have to comply with the new rules by July 2023 and DSA requirements will kick in for all providers of digital services (except the very smallest) by February 2024. During the next year, Member States will have to decide on their competent authority and appoint Digital Services Coordinators. At the same time, the European Commission will have to staff up to prepare for enforcement. Expect the Commission to issue gradually guidelines, Implementing Acts and Delegated Acts which will help to define how the new rules will work in practice.

Francine Cunnigham
Regulatory and Public Affairs Director
Belgium

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

Data

Piracy of live online content

Under pressure from sports organisations and broadcasters, the European Commission is set to come forward with a Recommendation by June 2023 addressing the piracy of live online content. This non-legislative initiative falls short of the urgent regulation for immediate takedown of pirated live content that rights holders had called for. Nonetheless, the Recommendation may indicate legislative actions that the Commission will pursue in future, if the new Digital Services Act does not prove to be effective in counteracting the enormous damage done to the sports sector in particular by this illegal activity.

Francine Cunnigham
Regulatory and Public Affairs Director
Belgium

Paolo Sasdelli
Regulatory and Public Affairs Advisor
Belgium

Data

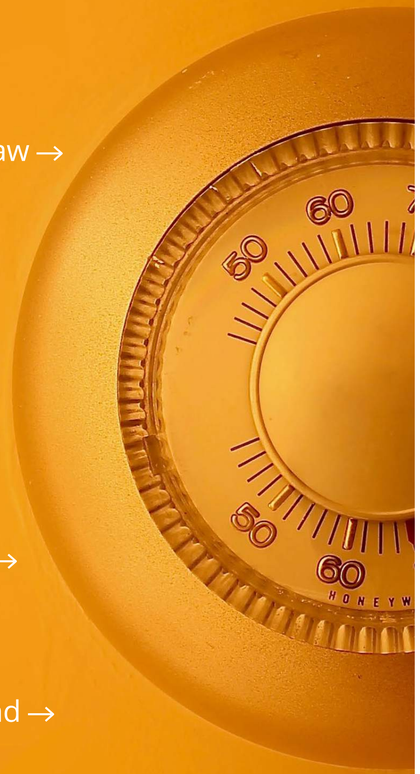
Access to in-vehicle data

By June 2023, the European Commission is expected to present a proposal on access to in-vehicle data, complementing the Data Act proposal which is currently going through the decision-making process in Brussels. This new, sector-specific proposal would lay down provisions on conditions of access to and use of data generated while connected cars and other vehicles are being driven. Key to this proposal will be the interplay between the right to access data, protection of privacy and cyber security rules. The Commission is also expected to present in 2023 a Communication on a European Mobility Data Space.

Francine Cunnigham
Regulatory and Public Affairs Director
Belgium

Paolo Sasdelli
Regulatory and Public Affairs Advisor
Belgium

Data



EUid

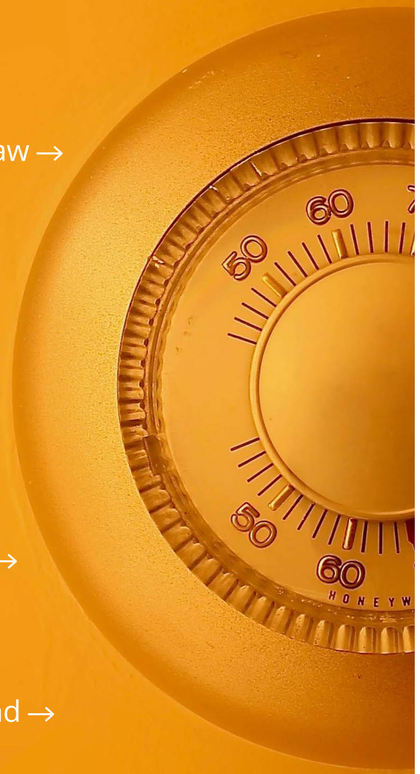
In June 2021, the European Commission published a proposal to amend the 2014 EU Regulation on electronic identification schemes and trust services for electronic transactions (known as the eIDAS Regulation).

Its primary objective is to establish a more harmonised approach to digital identification and to provide a future proof regulatory framework to support an EU-wide, simple, trusted and secure system to manage identities in the digital space, covering identification, authentication and the provision of attributes, credentials and attestations (European Digital Identity – EUid), and to create a universal pan-European single "European Digital Identity Wallet", which should be a product and service that allows users to store their identity data, credentials and attributes used for authentication, online and offline, and to create qualified electronic signatures in a single place.

Once adopted, this new regulation should significantly enhance and simplify offering and use of digital identification and trust services throughout the single market for all residents and businesses using electronic identification in connection with civil acts and commercial transactions or interacting with administrative bodies, and overcome the remaining obstacles related to issues of legal validity and mutual recognition of electronically executed documents.

Piotr Dynowski
Partner
Poland

Data



Waiting for eIDAS reform

In 2023, we will expect the announcement for a review of the Regulation (EU) No 910/2014 (Regulation eIDAS) with the aim of extending its benefits to the private sector and promoting trusted digital identities for all European citizens.

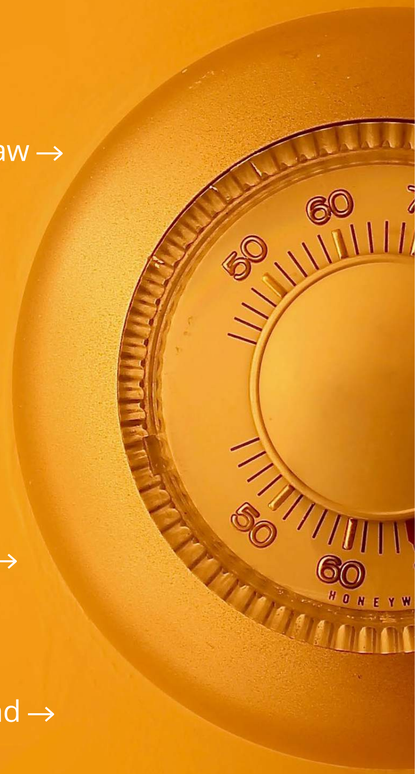
Among the new provisions, the reform will include, among other innovations: the introduction of the European Digital Identity Wallet, electronic identification schemes, unique identification, qualified preservation service for qualified electronic signatures, qualified electronic archiving service for electronic documents, electronic attestation of attributes and newly qualified trust services.

Niccolò Anselmi
Associate
Italy

Gian Marco Rinaldi
Counsel
Italy

Marta Breschi
Associate
Italy

Data



Widespread reform to Australian privacy law

On 21 May 2022, Australia elected a new Federal Government for the first time in 9 years with a mandate to, among other things, modernise Australia's privacy framework (which it can do without opposition given its significant majority in the lower house of Parliament). The Federal Government has already introduced a bill in Parliament (which seems likely to pass before the year ends) which, among other things, will significantly increase the maximum penalties for breaches of privacy laws to up to the higher of $50 million, three times the value of the benefit obtained by the privacy breach, or (if the benefit cannot be ascertained) 30% of the breaching entities' Australian turnover during a breach period.

The Attorney-General signalled the need to clarify to consumers how personal information is handled, in order to empower consumers to have greater control over their personal information.

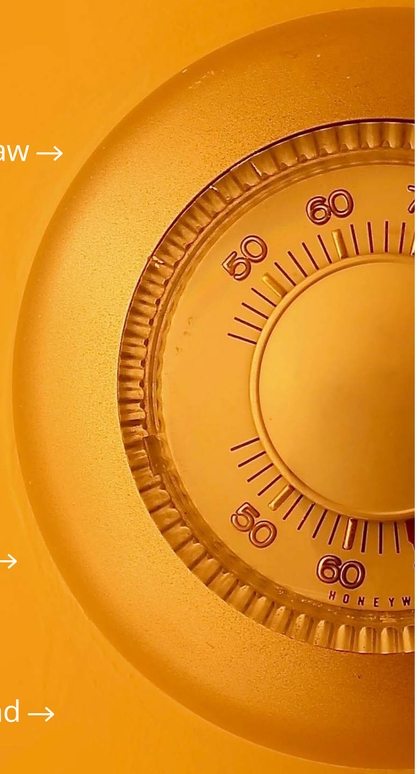
The Attorney-General expects to deliver a report on a review of Australia's privacy laws by the end of 2022 (furthering the aim to pass privacy changes as law in 2023) and indicated that the aim of reviewing privacy laws in Australia is to enhance protections for individuals and provide businesses with clarity on data privacy laws and expectations.

Hamish Fraser
Partner
Australia

Alex Gulli
Associate
Australia

Alex Dimovski
Graduate
Australia

Data

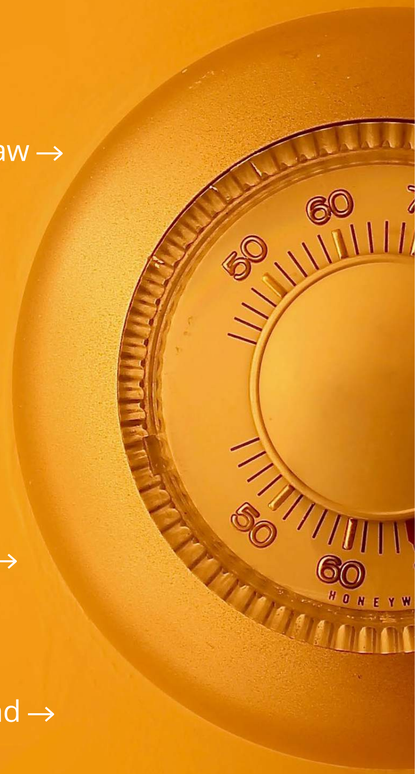


Continued focus on digital platforms

At the EU level the Digital Markets Act has been adopted which will give the Commission a new tool kit to tackle the challenges posed by digital markets. The first stage will involve the designation of so-called "gatekeepers" in the first half of 2023. This will represent the first opportunity to test the new regime. Actual compliance with the DMA's obligations will begin later from early 2024. In the UK, the Government has confirmed that we can expect legislation to enshrine its new digital competition "strategic market status" regime during the first half of 2023. Alongside this, both the European Commission and the Competition Markets Authority in the UK continue with their digital competition investigations.

Antony Rosen
Legal Director
UK

Data



Data and tax

An increasing number of individuals and businesses are using digital platforms to sell goods or provide services. Concerns that profits obtained by such vendors on digital platforms may not be properly reported for tax purposes, particularly where platforms operate in several countries.

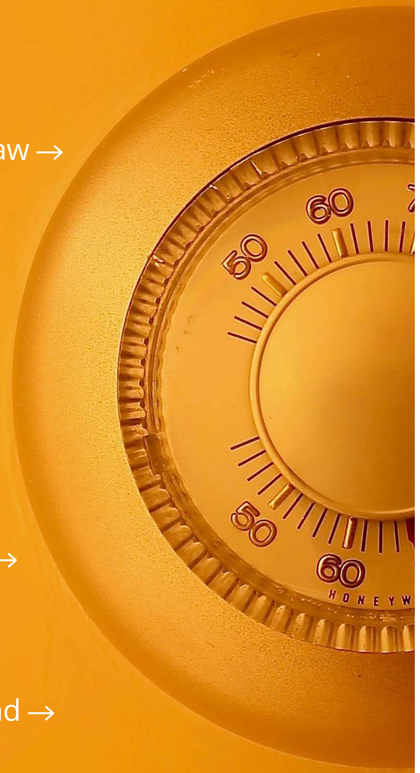
In 2023, DAC 7 (EU Directive 2021/514/UE) will come into effect, involving specific obligations for all EU online platform operators. DAC 7 transfers the operators' reporting obligations to digital platforms to help Member States fight tax evasion. These reporting of activities would cover a wide range and type of earnings from personal services, sale of goods to rentals of real estate and transport.

Platforms located outside the EU will have to report to the authorities of their home country, which will be responsible for exchanging information with EU Member States. Member States will be required to automatically exchange data received from the platforms with another country.

Annarita De Carne
Counsel
Italy

Giuliana Polacco
Senior Counsel
Italy

Data



Data export regime in China

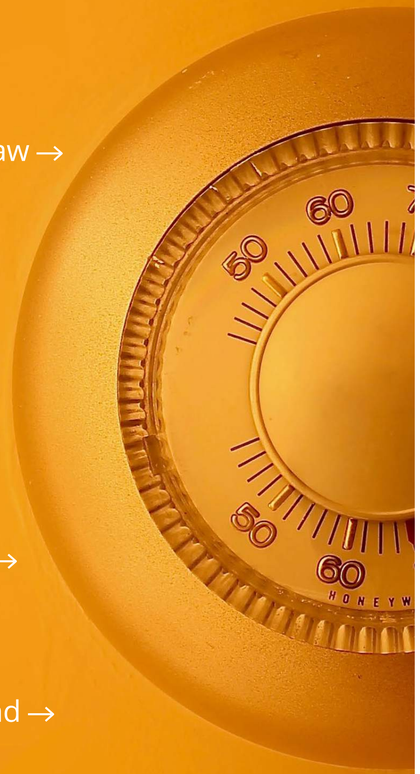
In 2022, China has proposed a series of important regulations and guidelines to supplement the three data export routes prescribed by the Personal Information Protection Law, most notably the Measures of Security Assessment for Data Export (Measures), the *draft* Standard Contract for Cross-border Transfer of Personal Information (Standard Contract), and the draft Technical Specification for Certification of Personal Information Cross-border Processing (Certification Specification).

Entities that are affected by the Measures should take immediate actions to ensure compliance, bearing in mind that the Measures only provide for a six-month grace period after the Measures take effect on 1 September 2022. Entities that are not affected by the Measures at this stage should also keep monitoring whether the processing activities are likely to meet any of the scenarios stipulated in Article 4 of the Measures and be prepared to sign the Standard Contract once the finalised version is in place.

James Gong
Partner
China

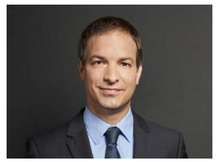
Jacqueline Che
Associate
China

Data



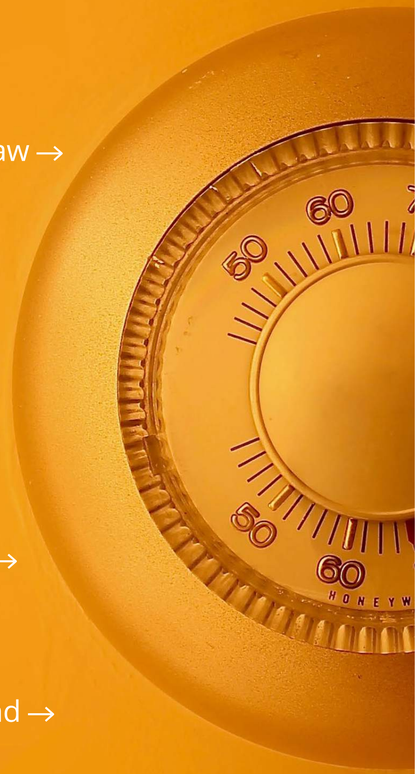
Digital Operational Resilience Act

As the Council of the European Union adopted the Digital Operational Resilience Act at the end of 2022, we expect various financial sector players and major ICT services providers to initiate early regulatory due diligence and implementation projects in 2023. However, we would recommend not carrying out any in-depth and ultimate implementation activities until regulatory technical standards (RTS) are published, which are to be prepared by the European Supervision Authorities over the next 18 months.



Kuba Ruiz
Senior Counsel
Poland

Data



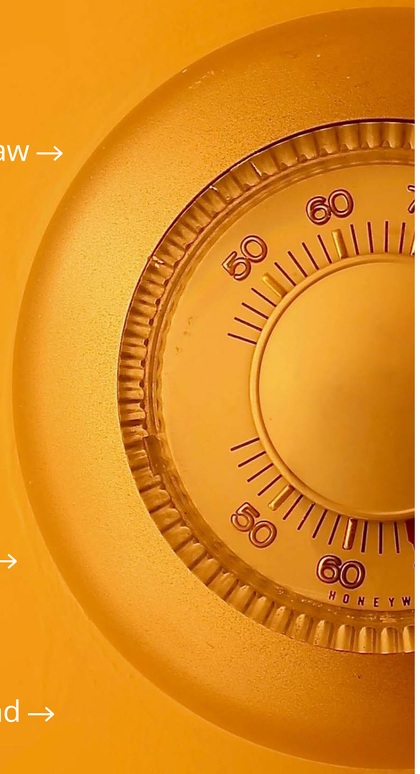
Consumer protection

Consumers and consumer protection organisations will increasingly exercise the new consumer rights, product liability laws, digital services rights, and other laws implemented in the EU. The catalysts for such consumer protection actions will not be new laws alone, but these actions will also be prompted by increased online activism and new consumer rights organisations with legal standing to take collective or representative legal actions.

Deirdre Kilroy
Partner
Ireland

Click here to access our International Business-to-Consumer website →

Data

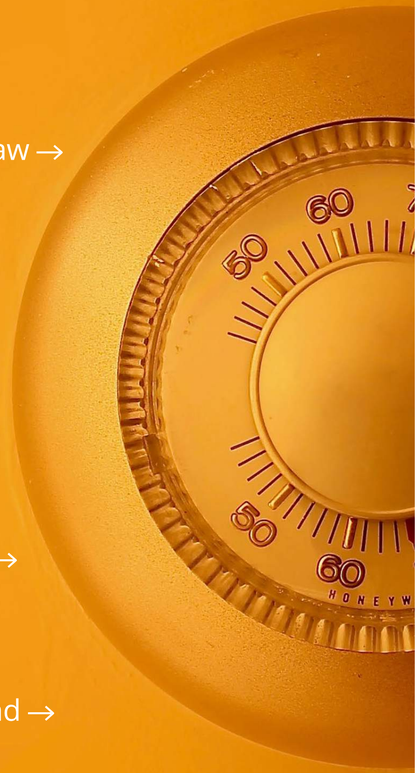


Loyalty customers

Whether it is only offering savings to loyalty card members for online supermarkets, offering discounts to those who facilitate access to personal data, or developing medical data based drug delivery options, consumer data-reliant products and services will be increasingly personalised. This will prompt a focus by regulators on dynamic pricing, complex profiling practices, transparency and the sources of data and adtech.

Deirdre Kilroy
Partner
Ireland

Data

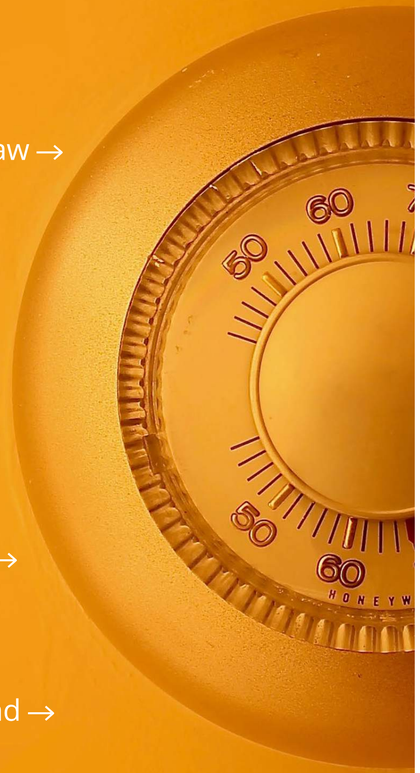


Electronic identity

Electronic identification services are becoming increasingly important in a digitised economy. Entities that have implemented identification systems for their customers are now reaping the benefits of providing electronic identification means to others. This trend will be reinforced when the planned regulation comes into force, which will introduce a 'European Digital Identity Wallet' (a universal pan-European single digital ID) which will extend benefits of eIDAS to the private sector.

Tomasz Zalewski
Partner
Poland

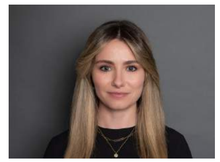
Data



Protection of children in the digital World

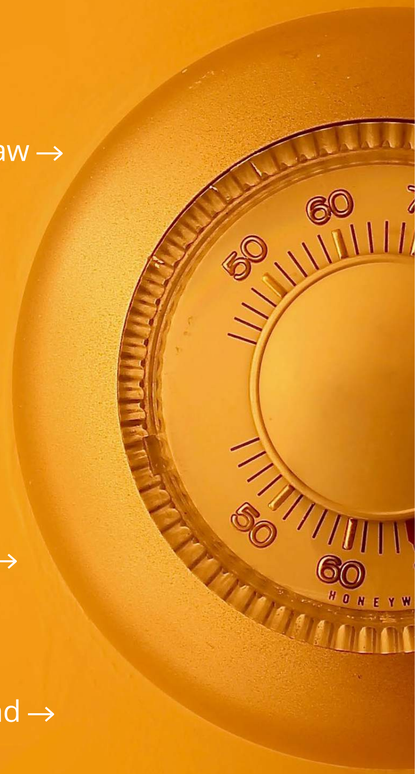
2022 saw the first cross-border processing decision under the GDPR on the processing of children's data (issued by the Irish Data Protection Commission, involving the Instagram platform) which involved all of the EU/EEA data protection authorities in the co-decision making process. With a further such cross-border processing decision pending (involving the processing of children's data by Tiktok) and separately, guidance on children's data protection issues awaited from the European Data Protection Board, it seems that children's privacy and protection of children's data will continue to attract increasing scrutiny from regulators in 2023. In addition, there continues to be a broader digital regulation focus at EU level on prioritising the protection and empowerment of children in the digital world. The Digital Services Act (DSA), once it enters into application, will require specific, proactive measures to be taken by platforms to protect children online (e.g. those set out in Article 28), amongst other general risk assessment and risk mitigation/ prevention measures. This will by no means be the last such initiative aimed at reduction of the risks to children posed by digital services - the European Commission released its New European Strategy for a Better Internet for Kids (BIK+) in May 2022 which includes a range of forthcoming measures to promote the protection and empowerment of children online. Notably this includes a commitment to the production of a comprehensive EU-wide age appropriate design code by 2024, and work towards standardising age assurance solutions, along with the promotion of media and digital literacy activities for children, teachers and parents. All of this points to an ever increasing policy making, and regulatory focus in the EU on the protection and empowerment of children in the digital world.

Anna Morgan
Partner
Ireland



Shauna Joyce
Associate
Ireland

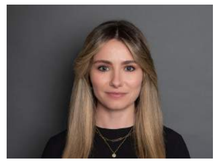
Data



Age verification / Age assurance

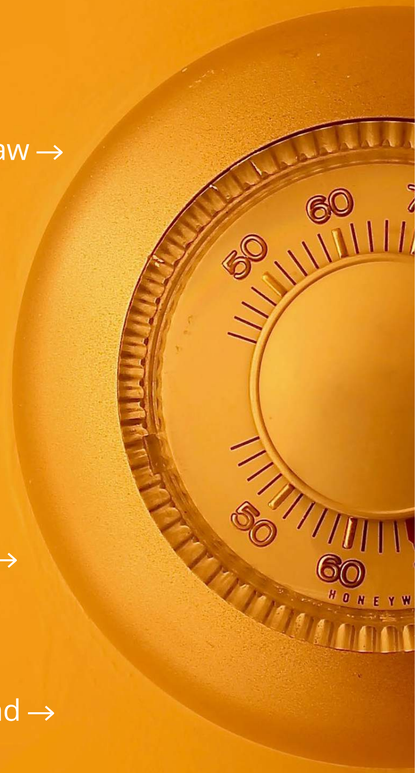
There has been an increasing emphasis during 2022 by regulators and policy makers in the UK and EU on the importance of age assurance (the term frequently used to collectively describe age estimation and age verification methods) as a means to ensure a higher level of protection for children in relation to risks posed by digital services. Age assurance will continue to be a burgeoning issue in 2023 across the UK and the EU. In particular the UK Information Commissioner's Office (ICO) will continue its work towards standardising the measurement of age assurance solutions while 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 verification which will clarify what is expected from industry when age verification is required on any online services. In this regard, the European Commission has stated that it will issue a standardisation request for a European standard on age assurance/age verification, compatible with the proposal for a European Digital Identity Regulation (eID proposal) by 2024. At an international level, an ISO working draft standard on age assurance systems has been produced with a view to establishing an ISO standard. It also seems likely that in 2023 data protection regulators will focus on age assurance in the context of the processing of children's data, with at least one cross-border processing decision pending from EU regulators involving age verification issues. In addition, with the advent of the higher standards of protection required for children/minors under the Digital Services Act and various national online safety laws, the ways in which digital service providers prevent access by children to higher risk services (and the efficacy of such methods) are likely to fall under scrutiny from online safety regulators as new laws in this area come into application.

Anna Morgan
Partner
Ireland



Shauna Joyce
Associate
Ireland

Data



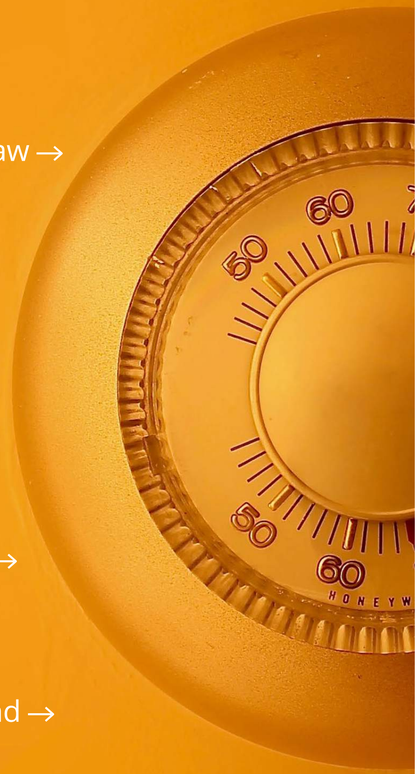
Online Safety Bill

Online content – the UK is continuing its scrutiny of the Online Safety Bill which will regulate illegal content, content harmful to children and content harmful to adults on user-to-user services and search engines. Following a change in Government, amendments have been tabled in Parliament which would alter the scope of content caught by the regime. Services will still have to assess and mitigate against the effects of illegal content and content harmful to children. However, duties that would have required certain services to mitigate 'legal but harmful' content have been removed. Instead, there will be an obligation on services to define which legal but harmful content they do not want to appear on their platforms in their terms of service, and enforce those terms. The Bill is expected to pass the UK Parliament and pass into law in Q3 2023, at which point further secondary legislation, and guidance and codes of conduct from Ofcom (the regulator) will be needed to implement the Bill. We expect organisations will have to comply with measures in the Bill in mid-2024 at the earliest.

Bryony Hurst
Partner
UK

Rory Coutts
Trainee
UK

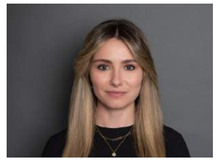
Data



Online safety / Content regulation in Ireland

The Online Safety and Media Regulation Act (OSMRA) was signed into law in Ireland on 10 December 2022 and it is expected that this legislation (which substantially amends and revises the Broadcasting Act 2009) will be commenced in the early part of 2023. The OSMRA establishes a new regulatory body, the Media Commission which will replace the current Broadcasting Authority of Ireland and also be responsible for regulating content, particularly harmful online content, available on online services. It applies to all video-sharing platforms or information society services that are under the jurisdiction of the Irish state and on which user-generated content is made available either directly or indirectly. Core obligations will be set out in a system of online safety codes which are to be established by the Media Commission; these will address “harmful online content” amongst other content related issues, while “age-inappropriate online content” will be the subject matter of guidance materials and advisory notes developed by the Media Commission. There will be very significant penalties for organisations which are found to have infringed online safety codes - administrative financial sanctions of up to €20 million or 10% of turnover for the preceding financial year as well as the possibility of various enforcement orders being made by the Media Commission or the Court (e.g. content limitation notices and access blocking orders).The Media Commission will also be the digital services co-ordinator for the purposes of the EU Digital Services Act (DSA) and it seems likely that implementing legislation giving effect to the DSA at a national level in Ireland will be introduced in 2023 which will sit alongside the OMSRA.

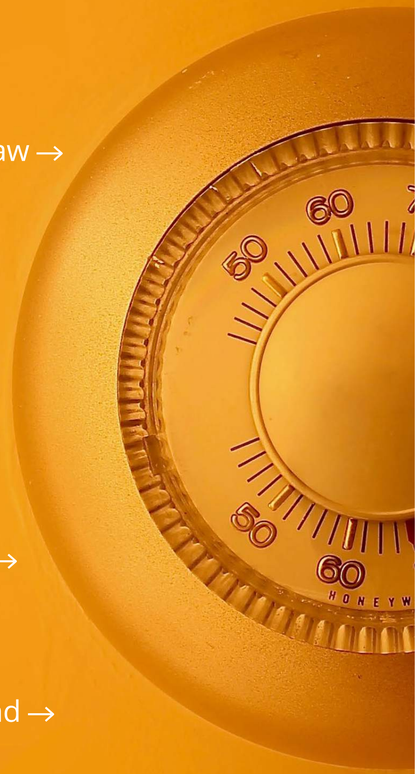
Anna Morgan
Partner
Ireland



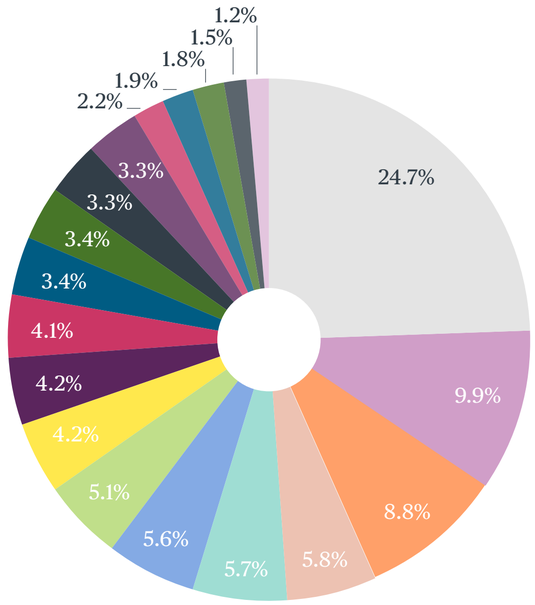
Shauna Joyce
Associate
Ireland

Data

- Data protection in the GCC countries →
- European health data space →
- Approaching the demands of the digital decade →
- Digital Services Act →
- Piracy of live online content →
- Access to in-vehicle data →
- EUid →
- Waiting for eIDAS reform →
- Widespread reform to Australian privacy law →
- Continued focus on digital platforms →
- Data and tax →
- Electronic identity →
- Data export regime in China →
- Digital Operational Resilience Act →
- Consumer protection →
- Loyalty customers →
- Protection of children in the digital World →
- Age verification / Age assurance →
- Online Safety Bill →
- Online safety / Content regulation in Ireland →

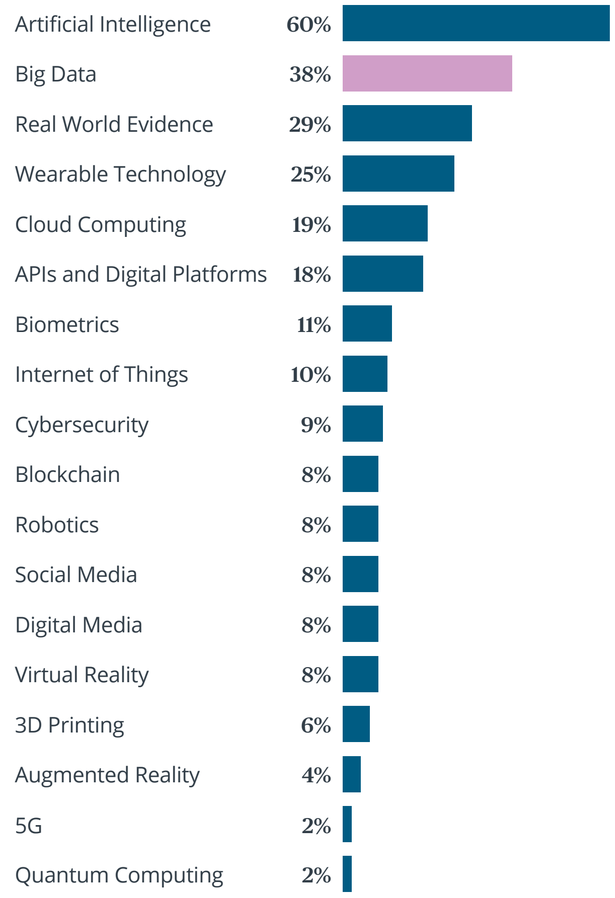


Total global data and analytics market in 2025



- Other*
- Manufacturing
- Information Technology
- Retail Banking
- Insurance
- Retail
- Energy
- Government
- Transport and Logistics
- Construction
- Consumer Goods
- Utilities
- Financial Markets
- Healthcare
- Education
- Media
- Communication
- Pharmaceuticals
- Mining

The Most disruptive technologies in the upcoming two years



Note: 'Others' includes agriculture, arts, entertainment, recreation, wholesale, business and professional, real estate, rental, leasing, construction and engineering, information and communications technology-related services, food services, travel and leisure, medical devices, and miscellaneous
Source: GlobalData

5G/6G

Spain – 5G regulation

Spain is seeing a sharp increase in the regulation of 5G technology. Last March 2022, the Royal Decree-Law 7/2022, of 29 March, on requirements to guarantee the security of 5G electronic communications networks and services was published in the Official State Gazette. It establishes security requirements for the installation, deployment and operation of electronic communications networks and for the provision of electronic and wireless communications services based on 5G technology. As part of this piece of regulation, Spain is expected to adopt a National Security Scheme for 5G networks and services, which is aimed at carrying out a comprehensive and global treatment of the security of 5G networks and services. Likewise, this new National Security Scheme will carry out a national risk analysis on the security of 5G networks and services and will address measures at national level to mitigate and manage the analysed risks. These measures may require prior certification for the use of equipment, software or services by a 5G operator, provider or corporate user; diversification targets in 5G networks and services supply chain; and measures to mitigate or manage the risks arising from terminal equipment and connected devices.

Alejandro Sola
Associate
Spain

5G/6G

Another spectrum auction in Germany?

In Germany, valuable mobile spectrum in the bands 800, 1800 and 2600 MHz is up for renewal by end of 2025. BNetzA has started the process to determine whether it will extend the current spectrum rights of the three mobile network operators or hold another competitive spectrum tender in the form of an auction or beauty contest. In order to complete the procedure in time before the current spectrum rights expire while allowing the operators to adjust their networks to the new spectrum allocation, a decision on the procedure will have been reached in 2023.

Valerian Jenny
Senior Counsel
Germany

5G/6G

Neutral host networks

With the upfront costs and complexity of deploying 5G networks, there is likely to be an increased focus on the use of neutral host networks. These networks involve the use of network infrastructure that is rented or leased to network operators by a neutral third party. The neutral host network model can provide a commercially viable option for network operators, particularly in regional areas, since operators are not required to bear the costs of building, maintaining and (largely) operating the infrastructure.

The increased focus on neutral host networks and active sharing is being supported in Australia by government. Both Federal and State governments have launched a series of initiatives to promote neutral hosting and active sharing models with a particular focus on addressing mobile blackspots in regional and remote Australia. These may serve as models for similar approaches elsewhere in other countries with similar geographic challenges.

The accelerating growth of 5G infrastructure in Australia will also provide opportunities for the development of smart cities. For example, Swinburne University recently announced a new government funded project that will use GPS sensors and high-resolution cameras on waste trucks to identify assets that need maintenance, such as road signs or damaged roads.

Matthew Bovaird
Associate
Australia

Dylan McGirr
Associate
Australia

5G/6G

5G network sharing

As the rollout of 5G networks continues to gather pace, mobile network operators are increasingly looking for ways to mitigate the significant costs associated with deployment. This has led to renewed interest in both passive and active forms of network sharing. By reducing the number of sites required and, in some cases, the amount of RAN equipment that an operator needs to deploy, substantial capital expenditure savings may be attained.

Two of Australia's three largest operators, Telstra and TPG, announced an active network sharing deal during 2022. The deal would see TPG gain access to Telstra's active mobile network infrastructure in regional parts of the country, which they contend will provide better connectivity and service quality to end users.

However, network sharing proposals also continue to be subject to close scrutiny from competition regulators. The Telstra/TPG deal is the subject of ongoing attention by the Australian Competition and Consumer Commission, which has flagged concerns that the proposal may dampen competition at infrastructure and service layers.

It is likely that network operators will continue to explore network sharing arrangements as 5G deployments mature. However, operators must be cognisant of how such arrangements may be viewed by competition authorities.

Thomas Jones
Partner
Australia

Patrick Cordwell
Associate
Australia

5G/6G

Spain – 5G regulation →

Another spectrum auction in Germany? →

Neutral host networks →

5G network sharing →

Over the **next two to three years**, *China, the US, Europe, and Japan will be aggressively building out their 5G infrastructures, with China having already far outpaced the rest*

There will be nearly **600 million** *new 5G subscribers in 2023*

Fixed wireless access and private networking will continue to be **5G focal points** *for the time being*

Source: GlobalData

Artificial Intelligence

The disruptive nature of content-generating AI

In 2022, the development of image and text generating AIs (e.g., Midjourney, Dall-E or GPT-3) has progressed to the point where even private users are able to achieve impressive results in free trial versions and with little effort. In the near future, this technology will extend to other media types - such as 3D models, videos or even whole virtual worlds. This will inevitably lead to a massive disruption of the industries that previously created this content “by hand”.

Instead of spending dozens or even hundreds of hours painstakingly creating a digital art image or modelling a 3D character for a video game, the future skill in demand will be feeding the AI with sophisticated prompts to achieve the desired results – in other words, the ability to guide and supervise the generative AI. Since this is such a recent development, we can only guess what impact this revolution will have on society and on the legal advice sector.

Oliver Belitz
Associate
Germany

Artificial Intelligence

Assisted and autonomous driving and AI

Well-known car manufacturers are continuing their unabated research and testing in the field of autonomous driving. Car manufacturers are building new research, development and testing centres for self-driving cars.

Companies investing in research are looking into how vehicles can solve unforeseen problems and dangerous life threatening situations using AI based simulation software. This technological evolution will be complemented by more comprehensive regulations in the field.

Niccolò Anselmi
Associate
Italy

Gian Marco Rinaldi
Counsel
Italy

Marta Breschi
Associate
Italy

Artificial Intelligence

AI and cloud services

AI and machine learning (ML) are increasingly being used to integrate cloud-based applications and services.

The rapid pace of change in the cloud sector makes it difficult for companies to keep up with the latest innovations. Indeed, the cloud is increasingly being referred to as the 'intelligent cloud', which is becoming smarter and smarter through the integration of AI and ML and is no longer just a place to store and archive the data.

Niccolò Anselmi
Associate
Italy

Gian Marco Rinaldi
Counsel
Italy

Marta Breschi
Associate
Italy

Artificial Intelligence

AI regulation

From Sci-fi novels to growing business opportunities, AI is getting a lot of attention from society. Today, AI is still very far from any self-conscious machine or deadly robot as it is mostly based on big-data processing with machine learning and deep learning, yet, possibilities for new solutions and efficient decision-making tools seem endless for developers. While the tech industry is demonstrating how innovation is a market driver and creates economic growth through new solution based on AI, the EU legislator wants to anticipate by regulating AI-producers liability. Given the high level of technicity of AI products, the new EU Directive proposition of 28 September 2022 opts for a middle ground solution and creates a presumption of causality where an injury could be related to such products, setting aside a solution based on strict liability. The Directive also create a right of access to the information on the technology to help victims obtaining evidence on the producer's liability. If adopted, the proposed Directive could give rise to numerous tort actions from victims who would find it easier to receive compensation. These actions could also imply multiple motions and cross motion to limit sensitive information and/or trade secret to be communicated.

Djazia Tiourtite
Partner
France

Artificial Intelligence

AI liability

The European Union is currently working on a liability framework for AI, which is expected to make great strides in 2023. The Commission has already published 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 artificial intelligence ("AI Liability Directive"). The proposals introduce game changers for product and non-contractual liability, which companies manufacturing, importing, distributing, selling, operating, integrating or modifying AI-systems and AI-enabled goods will be affected by. For example, frameworks are introduced for claiming disclosure of evidence from defendants and lightening the burden of proof for claimants with presumptions of defectiveness/fault/causality. 2023 will see progression of the legislative process, which may entail broadening of the framework to include strict liability and insurance obligations.

Shima Abbady
Associate
Netherlands

Artificial Intelligence

Generative AI and IP

2022 was a breakthrough year for generative AI systems. Image and text creation systems have impressed many and opened up a wider cultural debate around the nature of creativity and the role for automated content generation in our society.

As thoughts turn to commercial applications 2023 will be the year when the rubber hits the road for the legal issues associated with these systems. From an IP perspective there will be two key issues. The first will be the impact of using material protected by copyright and other related rights when training generative AI systems. Commercial users of generative AI systems will be particularly keen to know if they are exposed to any potential liability through use of systems training on third party copyright materials. This will interplay with the evolving international landscape for text and data mining exceptions and other fair use type exceptions to IP rights. The second key IP issue will be whether the outputs of generative AI systems qualify for IP protection and, if not, whether there are other effective ways of protecting investments made in its creation. While this question has been debated in IP circles for the past few years, the answer will take on much more commercial significance in 2023.

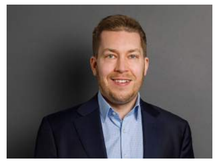
Toby Bond
Partner
UK

Artificial Intelligence

Smart products and AI

Companies engaged with AI solutions, whether as manufacturer, distributor or user, are surely looking at the obvious developments pertaining to the AI Act and AI Liability reforms' negotiations on an EU level. However, these are not the only legal frameworks which will set future standards for AI regulations. The EU proposals for the Machinery Regulation as well as the Product Safety Regulation are less obvious but equally relevant to businesses in the AI supply chain, in particular for smart/connected products.

With "machineries" being broadly defined covering most IoT equipment, products under the Product Safety Regulation will cover any (smart) products as fallback. Both initiatives shall address the risks of machineries/ products resulting from AI, e.g. in terms of considering the learning and predictive functionalities of a smart product for the product conformity assessment. This has the potential to heavily impact the legal requirements which allow the distribution of smart products equipped with AI in the EU.



Nils Lölfing
Counsel
Germany

Artificial Intelligence

AI – assessments

The Artificial Intelligence Act (AIA) is progressing well in Council and Parliament and is likely to be passed in 2023. It will bring a classification of AI systems according to risk. For high-risk systems, so-called conformity assessments are needed in addition to data protection impact assessments. Given that bigger corporate are doing already various assessments, it is important to adopt the assessment methodology and integrate new requirements to the existing methodology. This might require working across various units to avoid duplicate work. Similarly, the AIA requires a “by design” approach, meaning that potential risks need to be identified and addressed before an AI product is placed on the market. This needs to be coordinated with Privacy by Design efforts.

Tobias Bräutigam
Partner
Finland

Artificial Intelligence

Human centric AI

The Digital Single Market is well and truly on its way and the meaning of the EU's 'human centric approach' is taking shape. Human intervention, human review, and human oversight are some of the new concepts introduced in recent legislation relating to automated processes. Life has been brought back to the idea of a 'right to explanation', being pushed by both the EDPB and EDPS. However, 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 automated decision-making systems to an increased use of counterfactuals in order to meet the demands of legislators while facing the reality of AI. One thing is for certain, costs related to the use and development of automated decisions-making solutions are on the rise.

Hans Kaldéren
Trainee
Sweden

Mattias Lindberg
Partner
Sweden

Artificial Intelligence

Potential risks of necromarketing or using an image of a dead celebrity

According to Spanish law, image rights are protected after the death of the relevant holder, with the deceased estate having the exclusive right to take legal action, in order to enforce such rights. This is important for the so-called necromarketing or when using the image of dead celebrities in movies, videogames, metaverse, etc (for example, via holograms in live concerts). In many countries, there are no specific laws dealing with images of dead celebrities. In this context, it is important to underline that, when considering the use of images of dead third parties, it is not only rights such as copyright, related rights, and trademarks that must be taken into consideration, but also image rights which may require the corresponding authorisation. Therefore, the use of AI in relation to image rights will lead to increased litigation.

David Fuentes
Associate
Spain

Artificial Intelligence

The disruptive nature of content-generating AI →

Assisted and autonomous driving and AI →

AI and cloud services →

AI regulation →

AI liability →

Generative AI and IP →

Smart products and AI →

AI – assessments →

Human centric AI →

Potential risks of necromarketing or using an image of a dead celebrity →

96 countries are deploying AI technologies for surveillance purposes

AI market will be worth $188.3 billion in 2030

Generative software-based AI will be increasingly used in creative writing, coding, and sustainable product design

Source: GlobalData

Quantum Computing

Standardisation of quantum computers

Small and imperfect quantum computers already exist, and we currently witness the so-called noisy intermediate scale quantum (NISQ) era. The practical usefulness of quantum computers still remains to be demonstrated. In the coming years, providers of quantum computing solutions will try to establish as good a market position as possible before the technology is expected to progress to the next level. Full-scale quantum computers can decrypt some of nowadays most commonly used encryption protocols. Encrypted data that is, e.g., intercepted and stored by a third party today could be decrypted by a future quantum computer. Classical cryptographic schemes to counter this threat have been developed under the name post-quantum cryptography, which standard organisations are currently testing. They are expected to be standardised in the next few years. Companies are advised to follow this process closely in order to keep up with the latest recommendations, avoiding technical vulnerabilities and accusations of inadequate data protection.

Juliana Kliesch
Associate
Germany

Quantum Computing

Future of quantum computing

While it is still very early to see the full potential of quantum computing and its commercial adoption, 2023 could bring some important advances in this technology. We may witness a few quantum hybrid applications going into production that could solve certain difficult practical problems significantly faster than a traditional computer would. Progress will also be probably made in the area of error correction which is critical to make quantum computing actually useful in future. From a practical perspective, it is likely that companies will explore the potential use cases for quantum computing and will also start grappling with the issue of post-quantum cryptography in the context of their data security. We will likely see a further rise in patenting activity, as companies seek to protect their quantum technologies. There will undoubtedly be more government initiatives and involvement in the funding of various quantum-related projects and an increase in private investments in quantum technologies.

Vojtech Chloupek
Partner
Czech Republic

Quantum Computing

Standardisation process for quantum technologies

Although quantum computer and other quantum technologies remain at a relatively early stage in the technology adoption life cycle, the time now appears right to get involved in the standardisation process for quantum technologies. A Joint Technical Committee on Quantum Technologies of the European standardisation organisations CEN-CENELEC will commence work in March 2023. There is also work going on in the ETSI and ITU in regard to communication and in particular quantum key distribution (QKD). For quantum computing, standardisation would be required on such wide-ranging topics, from well-defined software layers and interfaces between them, quantum key distribution protocols and other communication protocols to having standardised interfaces/connections in the entire new category of quantum computing hardware. Early involvement in the standardisation process provides the opportunity to shape such future standards and contribute to the further development and adaption of quantum technologies. There are legal implications however for companies participating in such standardisation bodies that must be paid attention to.

Peter van Gemert
Counsel
Netherlands

Quantum Computing

Standardisation of quantum computers →

Future of quantum computing →

Standardisation process for quantum technologies →

Universal quantum computers would threaten the security of encryption

Fully-fledged commercial quantum computers are not expected for **10, 20,** *or even* **30 years***

China is committing at least **$15bn** *in quantum computing over the next five years**

***Source:** GlobalData

Metaverse

Operating models, stakeholders and contractual relationships in the upcoming metaverse

Currently, no one really knows how *the* future metaverse will look like. Will there be one overarching metaverse (as the prefix “meta” implies) – or several isolated ones? Will the metaverse be run by one or more operators? Will one company make it to the top of the operator hierarchy and be able to set the technical, economical, and legal framework for all the others (like major app-store operators today)? Or will several companies act as co-operators at eye level? Further, the metaverse will be home to a multitude of types of interacting stakeholders in addition to the operator(s): providers of “subworlds”, sellers of goods, providers of services, active users (those who create content themselves) and passive users (those who only participate) – to name only a few. The combination of these complexities allows us to conclude that the currently established (mostly bilateral) contractual concepts need to be closely assessed – and possibly overhauled – to be ready for the metaverse.

Oliver Belitz
Associate
Germany

Metaverse

A new home for media, entertainment, and sport events

Major companies, such as Walmart and Gucci have jumped into the metaverse with both feet. However, new marketing approaches are needed to draw their peers into their virtual venues on a regular basis. Thus, the challenge of an attractive presence in the metaverse is to continuously create unique and interactive experiences for users.

Since many young people: (i) now use (gaming) metaverses as their first social network and (ii) are used to on-demand entertainment, these creative marketing efforts are likely to grow massively over the next years. This includes sports tournaments (e.g. football, basketball), gaming competitions (e.g. go-cart race in the digital mall), concerts, and movie events. Analogue companies can sell digital equivalents to their products carried on NFTs: Clothing (such as virtual jerseys for a sporting event), vehicles (for a virtual drive-in movie), or consumer goods (virtual drinks for concerts).

Simon Hembt
Associate
Germany

Metaverse

EU metaverse initiative

During the second quarter of 2023, the European Commission will take its first steps into the metaverse, with a non-legislative initiative on virtual worlds. The Commission plans to propose tools to develop open, human-centric virtual worlds to create more opportunities for businesses and service sectors. According to the Commission, virtual worlds will have to be centred on EU values and rules and no single private player should hold the key to this public square or set its terms and conditions. Nevertheless, Europe's ability to impact virtual worlds will depend on its strength in developing cutting-edge technologies and building a sustainable online ecosystem to attract both private and public capital.

Francine Cunnigham
Regulatory and Public Affairs Director
Belgium

Paolo Sasdelli
Regulatory and Public Affairs Advisor
Belgium

Metaverse

Arbitration in the metaverse – virtual world, real consequences

Despite the development of cross-border trade and investment, legal systems have remained primarily based on national laws, and dispute resolution has relied on national court enforcement mechanisms to bring ultimate effect to contractual obligations. Even where international legal systems have evolved, parties have relied upon courts or arbitral tribunals seated within a national legal framework to hear and decide claims and produce judgments and awards capable of final effect.

But now comes the metaverse.

In a virtual world made up of virtual assets and transactions for those assets, what law applies?

Where do parties go to enforce contractual promises, demand payment, or compensation when deals go wrong? The answer is likely to involve decentralised dispute resolution chosen by the parties, or the platform providers, using non-national decision-makers with only the smallest connection (if any) with real-world national legal systems. This is international arbitration. Parties need to know how to make it work now, and what to look out for as arbitration and enforcement passes between the real and virtual worlds.

Nicholas Peacock
Partner
UK

Metaverse

Payments in the metaverse

Over the last couple of years we have seen dramatic advances in digital payments technology, from third party payments APIs embedded into neo banking apps to international cross boarder payments facilitated through the use of “stablecoins” running a blockchain. With the Web3 era well underway, we are now seeing millions’ of pounds worth of crypto currency, NFTs and digital assets transacted through blockchain technology, with a relatively small number of gatekeepers charging high percentage transaction fees for facilitating these transactions. As we move towards a larger Metaverse or greater interoperability between metaverse worlds, there could be considerable opportunity for new fintech’s as well as established financial institutions and payments providers to step into the space and act as the interface between the fiat currency and digital asset world, pioneering new standards for safe, smooth and secure transactions at more competitive rates.

Christina Fleming
Associate
UK

Metaverse

The Dubai Metaverse Strategy

The interest in developing the metaverse has continued to grow internationally. The development of the metaverse has been supported in the United Arab Emirates (UAE) through the Dubai Metaverse Strategy. The Strategy aims to turn Dubai into one of the world's leaders for the metaverse community, establish Dubai as one of the world's top 10 metaverse economies and develop global standards, infrastructure and regulations to accelerate the metaverse's adoption.

This development has also been seen with the establishment of the Dubai Virtual Assets Regulatory Authority (VARA) being set up in The Sandbox metaverse and plans to establish the UAE's Ministry of Economy in the metaverse also. This development shows the UAE's consistent support of technology and innovation and we expect that the development and adoption of the metaverse will continue to grow in the region throughout 2023.

Jessica White
Associate
UAE

Gregory Man
Partner
UAE

Metaverse

Special dispute resolution organs for metaverse-related cases

In a recent copyright infringement case involving a seller of an NFT avatar and the buyer who printed and sold T-shirts showing the NFT avatar, the "Metaverse Arbitration Tribunal" set up by Guangzhou Arbitration Commission caught the eyes of many for being the first arbitration case in China that was heard and decided completely in a metaverse environment.

The tribunal utilises the metaverse technology by building the tribunal inside a metaverse world called "Mega City" lead by the tech giant Baidu. Parties of a case attend the arbitration hearings in the metaverse using blockchain technology for verification of identity and evidence. Arbitrators are assisted with "virtual assistants" on conducting legal research and summarising big data of past cases for reference in the current case.

With the metaverse concept gaining traction in China and blockchain technology already utilised in many aspects of the judicial process, it is an exciting prospect to see if more Chinese courts and arbitration bodies can participate and utilise metaverse-related technologies to transform the judicial process and beyond.

Frank Tian
Trademark Associate
China

Hank Leung
Partner
China

Metaverse

Metaverse and NFTs risks in relation to IP and image rights

NFTs are digital tools with wide-ranging possibilities and legal issues. NFTs can be used in the metaverse and can represent both physical and digital assets. In any case, as a general rule, obtaining a mere NFT does not entail the acquisition of proprietary rights over the tokenised 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 Spain, the regulation in relation to NFTs is not clear which will probably lead to interesting legal developments and case-law in the next few years.

David Fuentes
Associate
Spain

Metaverse

Operating models, stakeholders and contractual relationships in the upcoming metaverse →

A new home for media, entertainment, and sport events →

EU metaverse initiative →

Arbitration in the metaverse – virtual world, real consequences →

Payments in the metaverse →

The Dubai Metaverse Strategy →

Special dispute resolution organs for metaverse-related cases →

Metaverse and NFTs risks in relation to IP and image rights →

Citi Global Insights said that the metaverse could be worth **$13 trillion** *by 2030*

Metaverse's growth will depend on the maturity of underlying technologies - AR, VR, AI, cloud, and blockchain, among others

AR and VR market was worth **$11 billion** *in 2020 and will reach* **$204 billion** *in 2030, expanding at a CAGR* of 33% over the 10-year period*

*compound annual growth rate
Source: GlobalData

ESG

Corporate Sustainability Reporting Directive

Adopted by the European Commission in November 2022, the CSRD requires that all large companies in the EU disclose data on the impact of their activities on people and the planet and any sustainability risks they are exposed to. The disclosure of this information will help investors, consumers, policymakers, and other stakeholders to evaluate large companies' non-financial performance.

The CSRD aims to standardise sustainability data and increase the availability of such data externally. To be fully prepared, businesses must take the time now to understand and prepare which sustainability data that must be collected, how to collect such data and when to disclose it.

Ariana Sohrabi
Associate
Sweden

Mattias Lindberg
Partner
Sweden

ESG

Green tech on track?

With the European Declaration on Digital Rights and Principles for the Digital Decade adopted on 14 November 2022, the Commission, Council and Parliament are committed to supporting the development and use of sustainable digital technologies that have minimal environmental and social impact, and developing and deploying digital solutions with positive impact on the environment and climate.

2023 will be the year that several Brussels green tech related regulatory initiatives may be agreed upon or end in disagreement, just before the start of the new electoral period in 2024. Next year will considered crucial for achieving the Commission's green tech ambitions with four initiatives:

1. Ecodesign regulation – manufacturers of smartphones and tablets manufacturers will be under the obligation to allow independent repairers access to spare parts and repair instruction for a period of at least 7 years;

2. Right to repair initiative – aims to encourage the repair and refurbishment of products. As the Regulatory Scrutiny Board rejected the initial draft, the Commission needs to come up with a new proposal in 2023;

3. Common chargers – the related directive will enter into force by end 2024 so that manufacturers have one year to arrange for mandatory USB-C charging ports for electronic devices like mobile phones, tablets and e-readers, digital cameras and game consoles, headphones and loudspeakers, wireless microphones and keyboards, and portable navigation systems. For laptops, a common charger will be mandatory by 2026. Member states will need to come up with implementing acts in 2023; and

4. Data centers – the Commission's action plan to incentivise data centers and telecom infrastructure to become more sustainable by 2025 is introducing a labelling scheme followed up possibly with binding regulatory initiatives in the event the market does not succeed with self-regulation.

Feyo Sickinghe
Counsel
Netherlands

ESG

ESG and tax

Tax transparency and tax payments are key in the ESG matter.

The taxation and the tax transparency do play a key role in the broader framework of sustainability. This is due to the fact that taxes are the first sources in financing national and global priorities and reducing inequality. Therefore, an ethical behaviour which takes care of complying with international and local legislation is more and more one of the key performance indicators for business enterprises.

As a result, the management of tax risks is becoming part a diligent governance of the multinational groups, considering also the reputational risk deriving from breaching tax rules.

In 2023, we expect more companies entering into cooperative compliance regime that fiscal administrations are promoting. Such regime, which has been developed by the Organisation for Economic Co-operation and Development (OECD) on the basis of positive international experience, has the main purposes of achieving the standards of tax certainty, anticipating the dialogue with the Tax Administration in view, also, to pay a fair and sustainable amount of taxes.

Annarita De Carne
Counsel
Italy

Giuliana Polacco
Senior Counsel
Italy

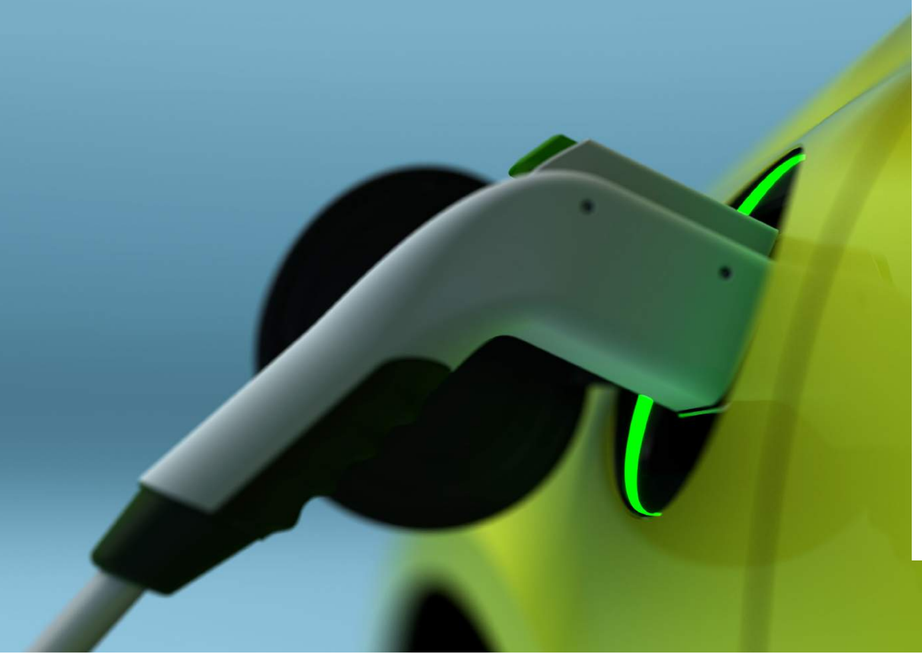
ESG

ESG contracts

Weight given to ESG issues will translate into contracts in a more scientific and measurable way. Performance metrics will track, record and test environmental and sustainability issues. Plastic production and use, recycling and innovation during the contract term will also increase in focus, as will fuel consumption through the delivery, transportation and supply cycles.

Deirdre Kilroy
Partner
Ireland

ESG



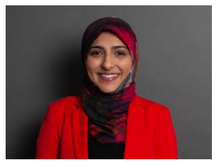
People risks & compliance

The pandemic provided an opportunity for many technology companies to grow at an exponential rate, increasing not only in size and headcount but also in terms of their geographical footprint. Early indications are that 2023 will see risk and compliance at the forefront of the people management agenda, with many of these high growth companies now looking to review and audit their workforce practices.

Contingent labour models have and continue to be popular with technology companies that are seeking to cautiously test new markets, geographies and product lines, in an effort to scale at a pace competitive with their peers. For those businesses reliant on a sizeable contingent workforce, we can expect a renewed focus on compliance considerations relevant to these workers in areas such as employment, immigration, tax and data security (please find our employment structures heatmap here).

Talent attraction and retention is likely to continue to be an important aspect of the people management agenda in 2023. The importance of holding on to key employees in a competitive environment cannot be overstated. In recent years we have seen a rise in 'employee activism' in the Tech & Comms sector and employees are more focussed than ever on buying into an employer's purpose and values, with ESG being particularly at the forefront. We expect this trend to continue in the year ahead and ESG credentials are therefore likely to become key tool for businesses when seeking to hire and retain top talent.

Ian Hunter
Partner
UK

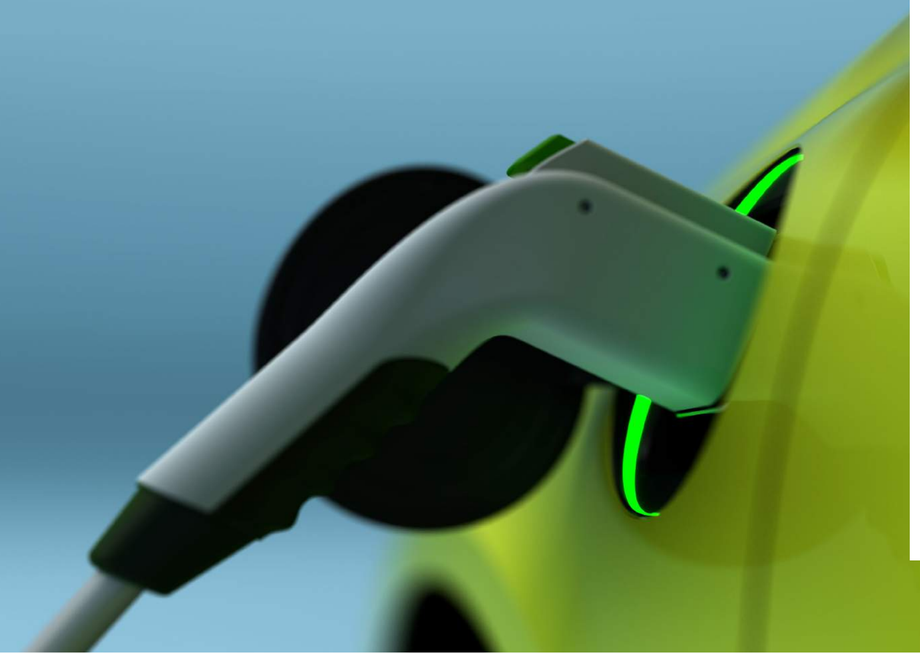


Furat Ashraf
Associate
UK

Charles Hill
Associate
UK

ESG

Corporate Sustainability Reporting Directive →
Green tech on track? →
ESG and tax →
ESG contracts →
People risks & compliance →



70% *ESG executives believed that setting ESG targets positively impacted revenue*

80% *of companies plan to increase their investments to meet ESG goals*

2023	2030	2050	2060	2070
The implementation of the Paris Agreement by member countries will be evaluated for the first time	The deadline for signatories possessing 90% of the world's forests to halt and reverse forest loss and land degradation	The deadline for Europe to become carbon neutral	The deadline for China to become carbon neutral	Deadline for India to be carbon neutral

Source: GlobalData

Cyber Security

Cyber security – EU legislation

The EU cyber security landscape developed in 2022 as we predicted in our forecast last year. We witnessed the EU legislators finalising their work on three major cyber security Acts (NIS2 Directive, the Directive on the Resilience of Critical Entities and the Digital Operational Resilience Act). In addition, the Commission's draft of the European Cyber Resilience Act was, as expected, published in the third quarter of 2022.

In 2023, companies will focus on shifting their activities from a general in-scope evaluation to much more in the direction of precise definition and implementation of measures required to comply with the new EU cyber security legislation. Besides entities active in the financial sector, this will concern inter alia data centre, cloud computing service and social networking services platform providers as well as certain groups of manufacturers.

Natallia Karniyevich
Associate
Germany

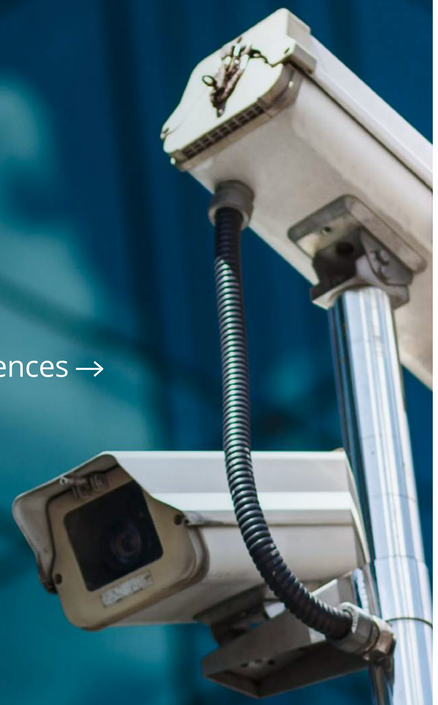
Cyber Security

Tightening regulation of NI-ICS

With the transposition of the European Electronic Communications Code, the number-independent electronic communications services (NI-ICS) have become subject to telecommunications regulation. Even though the regulatory framework for these services is looser than for traditional telecommunications, providers of NI-ICS have begun to realise that the burden is non-negligible. Examples for this are the newly applicable obligations originating from the ePrivacy Directive 2002/58/EC, security standards applicable to electronic communications services as well as demands in a few member states (notably Germany and France) that NI-ICS providers must enable lawful interception. This trend will probably continue in the coming year.

Valerian Jenny
Senior Counsel
Germany

Cyber Security



Data breaches and cyber security in the spotlight

Following a string of high-profile data breaches in Australia, the Australian Information Commissioner and Privacy Commissioner (Commissioner) intends to foster a cultural change in the data collection practices of businesses in Australia in 2023, by challenging technology companies to take greater responsibility for the prevention of data breaches, and adopt a proactive privacy-by-design approach. As part of this cultural shift, the Commissioner encourages entities to reassess cyber security measures and practices; the types of information collected; and whether information that is no longer required is deleted.

Additionally, the Commissioner anticipates the passing of a new privacy regime next year which could require entities to undertake privacy impact assessments; and create a baseline standard for information handling practices (which means less emphasis on lengthy privacy policies and notices with a shift away from the current notice-consent based regime). The Commissioner also desires the power to make privacy codes itself (rather than through industry consultation, as is currently required under Australian privacy laws); and changes which would require the information handling practices of entities that handle or deal with large amounts of data to be certified by OAIC accredit auditors.

Alex Gulli
Associate
Australia

Hamish Fraser
Partner
Australia

Alex Dimovski
Graduate
Australia

Cyber Security

Telecoms security and resilience

We are seeing a strong focus in the UK on telecoms security. Ofcom (the regulator) has new strengthened powers and we expect them to use them to enforce the new telecoms security regime that entered into force in October 2022. Further the Government has also confirmed that it will be broadening the scope of the cyber security regime to capture managed service providers with a core focus being to enhance supply chain resilience which often seen as a weak link in cyber defences. It will be necessary for digital services providers, telecoms operators and operators of critical infrastructure to be prepared. In parallel, in the EU, the new cyber security regime has been finalised with the adoption of NIS2 and it will now be necessary to follow the implementation phase over the next year as well prepare for compliance with the regime being expanded to cover new sectors, including data centres, CDNs, managed service providers, space and other sectors.

Antony Rosen
Legal Director
UK

Cyber Security

NIS2

The final text for the NIS2 Directive has been approved by the EU Parliament on 10 November 2022 and adopted by the Council of the European Union on 28 November 2022, and is expected to be published on EU Official Journal by the end of 2022. All EU Member States shall have 21 months to implement NIS2 Directive into national laws. In 2023, we will see EU Member States beginning the process of implementing the Directive to meet the deadline.

NIS2 Directive requires EU Member States to provide some material implementation activities, specific provisions are significantly different from the original NIS Directive, for example, relevant sectors and entities falling within the scope of NIS2 Directive are materially increased and in-scope entities shall adopt specific cyber security measures with regard to specific matters. Incident notification requirements are updated and made more stringent, and sanctions aimed at being harmonised at a EU-level.

Due to its new approach, with more detailed obligations to be met and measures to be adopted, implementation of NIS2 Directive may require further interventions in local cyber security legislation by EU Member States.

As for Italy, in the course of 2022 the national cyber security perimeter has been concluded with issuance of the last implementing provisions, and specific provisions regulating powers and attributions of the Italian Cyber Security Authority (created in 2021). In 2023 the Italian Cyber Security Authority will therefore start its full operations, with an increased control on cyber security matters.

Gian Marco Rinaldi
Counsel
Italy

Niccolò Anselmi
Associate
Italy

Marta Breschi
Associate
Italy

Cyber Security

Continued legislative attempts in formulating cyber security law and offences

For two consecutive Policy Address in 2021 and 2022, the Hong Kong government announced that it is planning to introduce a cyber security law, focusing on operators of public utilities and other critical information infrastructure and their obligations to protect such infrastructure against cyber-attacks. We expect the government to be launching the public consultation exercise on this legislative proposal by 2023. Against this backdrop, it is also notable that the Hong Kong Law Reform Commission released the Consultation Paper in July 2022 proposing the New Cybercrime Offences, which aim to rein in cybercrime with tougher penalties of up to life imprisonment. These proposed offences focus on cyber-dependent crimes, those that can be committed only through the use of information and communications technology devices, where the devices are both the tool for committing the crime and the target of the crime. In conjunction with the government's attempt in introducing a cyber security law, consolidated legislative efforts are expected to focus on formulating a general framework for protection of cyber security in Hong Kong.

Wilfred Ng
Partner
Hong Kong

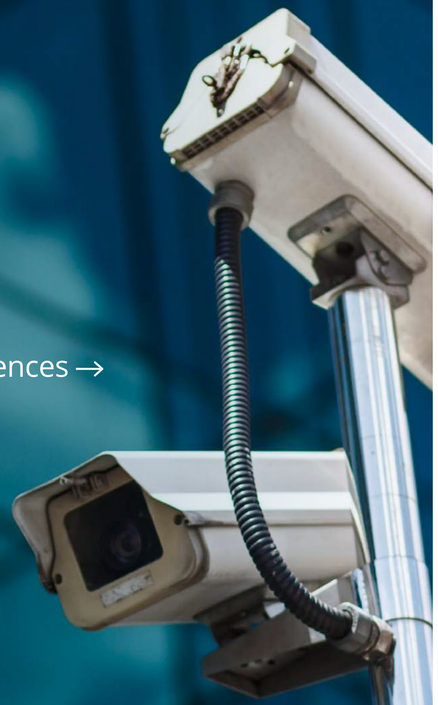
Cyber Security

Cyber security wars

Cyber security wars will continue. Fraudsters will use big data sets, AI, GPS simulation and device emulators to achieve their aims. Governments will continue to increase incentives for businesses to protection data and assets from these with an increased focus on regulation.

Deirdre Kilroy
Partner
Ireland

Cyber Security



Cyber security – EU legislation →

Tightening regulation of NI-ICS →

Data breaches and cyber security in the spotlight →

Telecoms security and resilience →

NIS2 →

Continued legislative attempts in formulating cyber security law and offences →

Cyber security wars →

The global cyber security industry will grow from **$125.5 billion** *in 2020 to* **$198.0 billion** *at a CAGR of 9.5%*

54% *of respondents to a survey on IoT said they could not use IoT data effectively due to security and privacy concerns*

80% *of cyber attacks now begin in the supply chain*

Cloud security incidents were up **10%** *from the previous year*

Source: GlobalData

Cloud & IoT

Semiconductor and chip shortages

The semiconductor and chip shortage crisis will continue into 2023. Uncertainty surrounding the crisis has led some companies to increase their investment in the construction of semiconductor plants. However, the construction of new plants takes time and currently the demand continues to increase, caused by the rise of IoT devices, the inclusion of semiconductors even in products that did not use them before and by the increasing use of electronic devices due to smart working.

Niccolò Anselmi
Associate
Italy

Gian Marco Rinaldi
Counsel
Italy

Marta Breschi
Associate
Italy

Cloud & IoT

IoT regulatory actions

As the new Directive 2019/771 will soon finally be implemented in all Member States, we will see more regulatory actions in the IoT field. The Directive introduces the concept of “goods with digital elements”, which encompasses a wide range of devices with digital functions. This is the first step towards regulating such products (the next step being the Data Act).

The Directive sets out obligations for product conformity with the contract, requires sellers to provide consumers with updates, including security updates, introduces a harmonised liability regime, and provides for certain information obligations towards consumers. In 2023, the regulators will start to enforce these new rules on sellers in many EU countries.

Pawel Lipski
Partner
Poland

Cloud & IoT

Impact of war

The war in Ukraine has caused many businesses to suddenly recognise that what they had previously seen as a disadvantage of cloud services - storing data in a distributed manner in different geographical locations - has suddenly become an advantage that determines the superiority of cloud solutions over on premises solutions. It can therefore be predicted that there will be another wave of cloud deployments among both business users and public administrations.

Tomasz Zalewski
Partner
Poland

Cloud & IoT

Responsibilities for integrated services in connected vehicles

The automotive industry is encountering more questions surrounding the responsibilities for integrated services provided by third parties. This is driven by the fact that car manufacturers have been focusing on developing connected vehicles for some time and in parallel, the legal environment has changed and the awareness of consumers has increased. Many car manufacturers face the challenge of clearly dividing the data protection responsibilities between themselves and the third party service providers in the vehicle. Also, new consumer legislation stipulates stricter requirements on actors integrating third party services into their products, which might lead unforeseen consequences in regard to consumer liability. There will be a need for our clients to stay on top of their compliance work and clients that do so will come out on the other side even more competitive.

Erik Myrberg
Associate
Sweden

Mattias Lindberg
Partner
Sweden

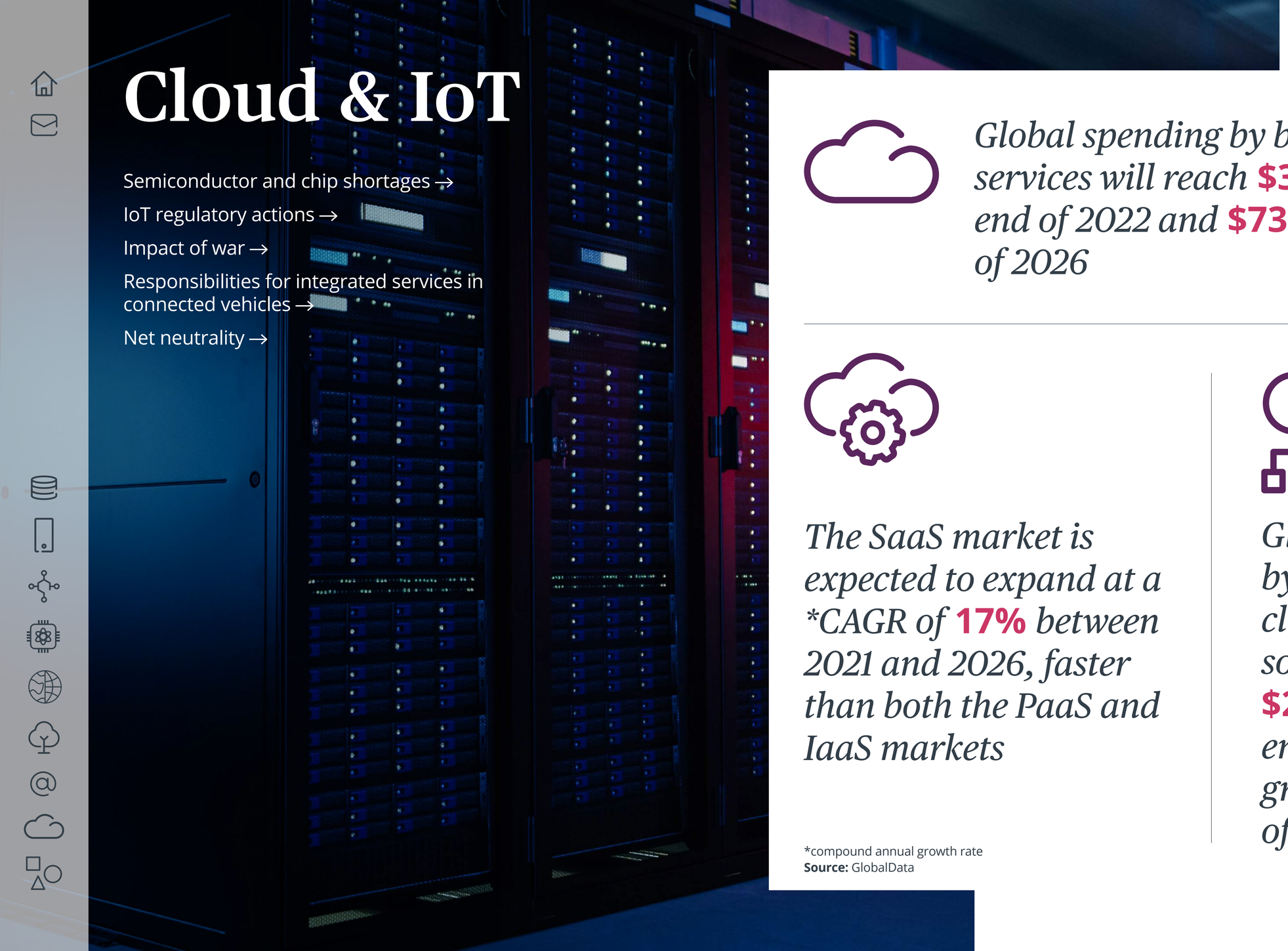
Cloud & IoT

Net neutrality

Whilst the EU through BEREC has issued updated guidance on net neutrality and in particular the prohibition on zero rating, Ofcom in the UK is consultation on changes to the UK regime which will allow for greater flexibility. Ofcom's consultation close in January 2023 so we can expect certainty in the first half of 2023. Ofcom is proposing to continue to allow zero rating, traffic management to be exercised in certain circumstances. Ofcom is also considering the potential pros and cons of introducing a charging regime that will allow internet service providers to charge content providers to carry traffic but noted ultimately this will be for the Government to decide (there is an ongoing debate about this issue at the EU level too).

Antony Rosen
Legal Director
UK

Cloud & IoT



Semiconductor and chip shortages →

IoT regulatory actions →

Impact of war →

Responsibilities for integrated services in connected vehicles →

Net neutrality →

Global spending by businesses on cloud services will reach **$398.1 billion** *by the end of 2022 and* **$738 billion** *by the end of 2026*

*The SaaS market is expected to expand at a *CAGR of* **17%** *between 2021 and 2026, faster than both the PaaS and IaaS markets*

Global spending by businesses of cloud infrastructure solutions will reach **$297.5 billion** *by the end of 2026, having grown at a CAGR of 13.1%*

*compound annual growth rate
Source: GlobalData

NFT, Tokens and Blockchain

Brand protection and enforcement of new technologies

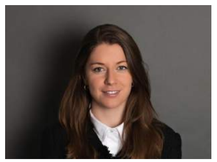
2023 will be a big year for brand owners developing their strategies for brand protection and enforcement around new technologies, especially NFTs and the metaverse. As these technologies become more established, we're going to see diverse questions arising in this area. Courts will be making decisions in cases that are already on foot, and new disputes will crop up. Meanwhile, after a UK court allowed service of proceedings to be effected by NFT, we can expect these technologies to offer new means for procedural creativity in litigation as well.

Nick Aries
Partner
USA

NFT, Tokens and Blockchain

NFT projects remain popular as regulatory scrutiny increases

NFT projects have continued in popularity throughout 2022 with retail brands and entertainment companies alike. This year music festivals Coachella and Tomorrowland both launched new NFT projects, offering unique benefits and experiences for concert-goers. This trend of tokenisation of rights and benefits as a way to drive consumer engagement is likely to continue (despite the average price observed on the markets of all NFTs traded reportedly dropping) with the increased utility of NFTs and tokens as metaverse-type projects expand being a relevant factor. With greater commercial viability also comes greater regulatory scrutiny. UK regulators remain focused on interventions to reduce risks in the crypto sector, including in relation to marketing and financial promotions and stablecoins. On 4 November 2022, the UK Digital, Culture, Media and Sport (DCMS) Committee also launched an inquiry into NFTs and the blockchain and it is likely to examine whether more regulation is needed, ahead of a UK HM Treasury review. The inquiry closes in January 2023.



Christina Fleming
Associate
UK

NFT, Tokens and Blockchain

DLT market infrastructure, securities tokenisation, SME financing

Regulation (EU) 2022/858 on Distributed Ledger Technology (DLT) market infrastructure provides a pilot scheme for certain crypto-assets falling into the category of financial instruments, which will apply from 23 March 2023. This extraordinary measure sets the regulatory framework for testing the impact of transformative distributed ledger technologies in the financial sector. DLT market operators can benefit from significant temporary exemptions by complying with specific licenses. As financial instruments that are allowed to be traded on DLT multilateral trading facilities and registered on the DLT securities settlement systems must meet certain conditions in terms of issuer's market capitalisation (in the case of equity) or issue value (in the case of plain vanilla bonds), the typical target issuer is expected to be an unlisted small or medium-sized firm. This provides an excellent opportunity for SMEs, the backbone of the European economy, to access the capital markets at a reasonable cost. With the right stimulus and support, SMEs can find ways to finance their investments through the tokenisation of securities in this market infrastructure. By bringing known forms of financial instruments into the world of crypto-assets and investing in them, speculative retail demand for asset-unrelated tokens can be turned into financial savings that support the real economy. As SMEs become more familiar with the underlying technology, and with intensive advisory support, we are likely to see a phased approach to these new types of markets over the next few years.

Giuseppe D'Agostino
Of Counsel
Italy

NFT, Tokens and Blockchain

The development of virtual asset financial regulation in the UAE

Adoption of NFTs, tokens and blockchain has continued to gain traction globally. The UAE has continued its development of virtual asset financial regulation in 2022 reflecting its focus on becoming a global hub for FinTech. Recent financial regulations include the establishment of the Dubai Virtual Assets Regulatory Authority (VARA) as the first financial services regulator in the region focused solely on the regulation of virtual assets. In addition, the Dubai Financial Services Authority (DFSA) recently implemented a new crypto token regime in the Dubai International Financial Centre (DIFC). Blockchain has continued to develop in the region with support from the Dubai government which reports that blockchain business in Dubai have increased by 24% annually (faster than the global average). We expect to see further developments for virtual assets and blockchain in the UAE throughout 2023 including the development of financial regulations for DeFi.

Jessica White
Associate
UAE

Gregory Man
Partner
UAE

NFT, Tokens and Blockchain

Continued growth of bitcoin

The Global Crypto Adoption Index published in September 2022, showed that in Europe the investment in cryptocurrencies is over $1.3 trillion from July 2021 to June 2022.

If this is not enough to understand the increasingly important role of bitcoin, Google recently announced that thanks to a partnership with Coinbase (one of the largest exchange platforms for digital currencies) from 2023, it will accept bitcoin payments for its cloud services.

This trend is set to grow increasingly as blockchain and cryptocurrencies enable companies to create new business opportunities in the digital economy.

Niccolò Anselmi
Associate
Italy

Gian Marco Rinaldi
Counsel
Italy

Marta Breschi
Associate
Italy

NFT, Tokens and Blockchain

Brand protection and enforcement of new technologies →

NFT projects remain popular as regulatory scrutiny increases →

DLT market infrastructure, securities tokenisation, SME financing →

The development of virtual asset financial regulation in the UAE →

Continued growth of bitcoin →

Taxation of digital rights and assets →

More judicial opinions on legal characteristics of NFTs may be expected →

Registration of NFT/blockchain-related trademarks may become easier →

NFT proprietary right →

Taxation of digital rights and assets

With expansion of digital rights and assets, governments worldwide are interrogating their transactions for tax consequences. The tax legislation in many countries is not sophisticated to capture revenues from transactions involving digital assets.

The OECD has already issued a publication *"Taxing Virtual Currencies"* which includes an analysis of the approaches and policy gaps across the main tax types (income, consumption and property taxes) and *"considers the tax implications of a number of emerging issues, including the growing interest in stablecoins and 'central bank digital currencies'; as well the evolution of the consensus mechanisms used to maintain blockchain networks and the dawn of decentralised finance"*.

In 2023, we expect to see legislation aimed at regulating the tax aspects of cryptocurrencies and digital assets, in order to reduce tax evasion in the sector and give consistent guidelines to investors.

Annarita De Carne
Counsel
Italy

Giuliana Polacco
Senior Counsel
Italy

NFT, Tokens and Blockchain

More judicial opinions on legal characteristics of NFTs may be expected

Unlike many parts of the world, crypto currency activities are banned in China, in part due to China's foreign exchange controls and concerns on use of crypto currencies for money laundering and bribery. In China, NFTs are not banned or officially recognised, some interesting cases involving NFTs are outlined below:

1. In what is widely regarded as the first NFT-related judicial decision in China, the Hangzhou Internet Court found that the use of third party's copyrighted artwork to mint and sell NFTs constitutes copyright infringement and the NFT trading platform, is liable for failing to conduct reasonable due diligence and to take down the infringing NFT.

   Major Chinese tech companies such as Tencent, Alibaba and Baidu have set up their digital platforms for domestic users to trade "digital collectibles" - China's own version of NFT.

2. In a recent dispute involving the sales of "blind box" (where a physical / virtual box or pack is filled with unknown random content from a selection of merchandize and sold to consumers) of NFT / digital collectibles, the Hangzhou Internet Court recognised that minted NFTs possess the necessary quality as digital property since they are valuable, scarce and transactable.

   Chinese tech companies have invested heavily in the NFT market, we may expect to see the number of disputes arise in the upcoming year.

Frank Tian
Trademark Associate
China

Hank Leung
Partner
China

NFT, Tokens and Blockchain

Registration of NFT/blockchain-related trademarks may become easier

As China adopts its own version of the Nice Classification of goods/services and limits registration of goods/services to a list of standard and predefined items, for many applicants, it has been frustrating to try to register NFT/metaverse-related trademarks. In the past year however, although registration of crypto / metaverse related trademarks and description of goods/services are still not allowed, it has been observed that some "virtual environment" related items have been accepted, in particular in Class 9 relating to software / digital contents used in connection with the virtual environment. This appears to coincide with trends in other where the generic concept of "virtual goods" cannot be registered but more specific virtual goods/services are accepted.

There are speculations that NFT-related goods and services will work their way into the new version of the Nice Classification. If so, it would be interesting to see if these will be accepted by the Chinese Classification eventually.

Frank Tian
Trademark Associate
China

Hank Leung
Partner
China

NFT, Tokens and Blockchain

NFT proprietary right

In 2022, the Singapore High Court granted an application for an interlocutory injunction to restrain the defendant from dealing an NFT, recognising that it can give rise to proprietary rights. The court rejected the notion that NFTs are mere information and should not be granted property status - instead applying the test in the English case of *National Provincial Bank Ltd v Ainsworth* [1965], which provided that where property is definable and has a recognisable owner the rights therein can be assumed by third parties and have a degree of permanence.

The recognition of NFTs as property is expected to lend weight to their use of transferring ownership of digital assets, and also physical assets such as artwork and real estate. As an urgent ex parte application, the court did not have the benefit of submissions from the defendant, and Singapore courts may decide differently if the issue were to be fully considered at trial.

Pin-Ping Oh
Partner
Singapore

NFT, Tokens and Blockchain

Brand protection and enforcement of new technologies →

NFT projects remain popular as regulatory scrutiny increases →

DLT market infrastructure, securities tokenisation, SME financing →

The development of virtual asset financial regulation in the UAE →

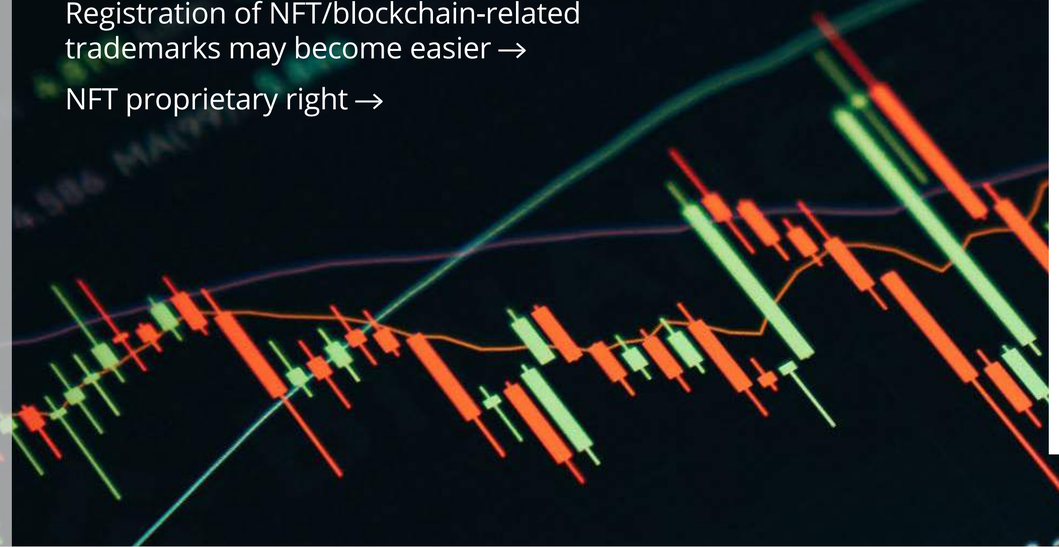
Continued growth of bitcoin →

Taxation of digital rights and assets →

More judicial opinions on legal characteristics of NFTs may be expected →

Registration of NFT/blockchain-related trademarks may become easier →

NFT proprietary right →



GlobalData estimates that the global blockchain market will be worth almost ***$200 billion*** *in 2030*

2020	2025	2030
$3.6B *in global blockchain revenues*	**$24.1B** *in global blockchain revenues*	**$198.6B** *in global blockchain revenues*

The popularity of ***mobile games, esports, and NFTs*** *will boost ecommerce sales, primarily in regions such as Asia-Pacific, Latin America, and the Middle East*

There are similar number of ***blockchains patents*** *within the insurance industry as other key themes such as data analytics, AI, and cybersecurity*

Source: GlobalData

Country contacts

Australia

Alex Dimovski, *Graduate*
+61 2 9226 9888
alex.dimovski@twobirds.com

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

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

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

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

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

Frank Tian, *Trademark Associate*
+86 10 5933 5688
frank.tian@twobirds.com

Hank Leung, *Partner*
+86 10 5933 5688
hank.leung@twobirds.com

Jacqueline Che, *Associate*
+86 10 5933 5688
jacqueline.che@twobirds.com

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

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

Czech Republic

Vojtech Chloupek, *Partner*
+420 226 030 518
vojtech.chloupek@twobirds.com

France

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

Finland

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

Germany

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

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

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

Oliver Belitz, *Associate*
+49 (0)69 74222 6000
oliver.belitz@twobirds.com

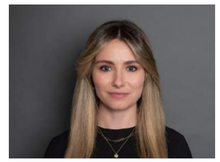
Simon Hembt, *Associate*
+49 (0)69 74222 6000
simon.hembt@twobirds.com

Valerian Jenny, *Senior Counsel*
+49 (0)69 74222 6000
valerian.jenny@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



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

Italy

Annarita De Carne, *Counsel*
+39 02 30 35 60 00
annarita.decarne@twobirds.com

Gian Marco Rinaldi, *Counsel*
+39 02 30 35 60 00
gianmarco.rinaldi@twobirds.com

Giuliana Polacco, *Senior Counsel*
+39 02 30 35 60 00
giuliana.polacco@twobirds.com

Giuseppe D'Agostino, *Of Counsel*
+39 02 30 35 60 00
giuseppe.dagostino@twobirds.com

Marta Breschi, *Associate*
+39 02 30 35 60 00
marta.breschi@twobirds.com

Niccolò Anselmi, *Associate*
+39 02 30 35 60 00
niccolo.anselmi@twobirds.com

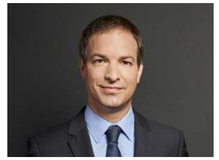
Netherlands

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

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

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

Piotr Dynowski, *Partner*
+48 22 583 79 00
piotr.dynowski@twobirds.com

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

Singapore

Pin-Ping Oh, *Partner*
+65 6534 5266
pin-ping.oh@twobirds.com

Spain

Alejandro Sola, *Associate*
+34 91 790 6000
alejandro.sola@twobirds.com

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

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

Sweden

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

Beatrice Duke, *Associate*
+46 85 063 2043
beatrice.duke@twobirds.com

Erik Myrberg, *Associate*
+46 (0)8 506 320 00
erik.myrberg@twobirds.com

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

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

UAE

David Bintliff, *Partner*
+971 4 309 3222
david.bintliff@twobirds.com

Gregory Man, *Partner*
+971 4 309 3222
gregory.man@twobirds.com

Jessica White, *Associate*
+971 4 309 3222
jessica.white@twobirds.com

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

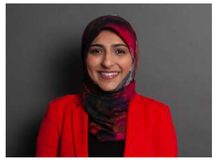
UK

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

Bryony Hurst, *Partner*
+44 (0)20 7415 6000
bryony.hurst@twobirds.com

Charles Hill, *Associate*
+44 (0)20 7415 6000
charles.hill@twobirds.com

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



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

Ian Hunter, *Partner*
+44 (0)20 7415 6000
ian.hunter@twobirds.com

Nicholas Peacock, *Partner*
+44 (0)20 7415 6000
nicholas.peacock@twobirds.com

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

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

USA

Nick Aries, *Partner*
+1 415 231 6568
nick.aries@twobirds.com