Bird & Bird

Tech & Comms - 2022 Challenges, Opportunities and Predictions

One firm.
Your firm.

As 2021 draws to a close we look back on a year of change, transition and innovation. The impact of the Covid pandemic can be seen across all industries as it has accelerated the digitalisation of the world around us. Digitalisation has brought new business opportunities, workplace changes and busy legislative agendas for authorities around the world as they consider the power, flow and security of data.

We have once again asked our global team of Tech & Comms specialists to highlight some of the challenges and opportunities they expect to see in the year ahead. Covering the many aspects of technology, we have grouped these predictions in four categories: data, regulation, smart infrastructure and new tech. There are strong connections between these four groups, with new tech generating vast amounts of data, leading to new regulatory frameworks and requiring significant investment in new infrastructures.

As businesses continue to explore the opportunities offered by the data economy, our teams see an increased focus on the mobility and security of data as well as the collaboration around data. 2022, we predict, will see a notable uptick in regulatory and legislative activity as many countries start to implement their ambitious agendas for stimulating the development of new tech and infrastructures whilst balancing demands for security, integrity and protection of individuals, networks and society.

What issues do we expect to be at the top of the agenda for tech businesses and the users of their services in 2022? Data continues to be a dominant theme, with Artificial Intelligence vying for pole position and the first signs of what may come next: the metaverse. We have highlighted a range of developments in areas such as **AdTech, Mobility, Cybersecurity, Data Localisation and Regulation, 5G, Sustainability, Net neutrality** and **Online Safety** all of which we believe will have a significant impact over the next 12 months and beyond.

Data

AdTech

Regulators across Europe have now very much found their feet with their new powers under the GDPR regime. We are already starting to see more investigations into data privacy practices, and increasingly high penalties being handed down where non-compliance is found. The UK's ICO is no different in this respect and one particular area where we expect they will focus their attention in the coming year is AdTech. They have made plain their intention to scrutinise the AdTech industry and have already taken steps to investigate the practices of some of the bigger players. However, we would not expect their interest to stop with those at the top of the AdTech ecosystem - with more complaints being received from data subjects relating to issues such as unlawful cookie placement, it seems likely that at some point they will also seek to make examples of companies lower down the food chain where significant non-compliance has occurred. As penalties increase, and the risk of follow-on litigation continues to grow, it also seems likely that we will see companies fighting back harder against enforcement decisions.

Bryony Hurst
Partner | United Kingdom

Data

Cybersecurity - Australian standards

The bar is lifting in respect of data and information security practices of companies as cybersecurity has become a key regulatory focus in Australia, with various regulators running test cases in respect of poor cyber practices in areas of law not expressly regulating cybersecurity, such as corporations and consumer law, for example ASIC v RI Group. Simultaneously, the Australian Federal government is also considering new ways to regulate cybersecurity standards in Australia, including within its consideration: the introduction of minimum expectations for businesses to manage cybersecurity risks, mandatory product standards for smart devices and clearer legal remedies for consumers. The Government has also recently passed the first tranche of reforms to the Security of Critical Infrastructure Act 2018, with the underlying rules and second tranche expected to follow in 2022. These reforms impose stricter security obligations on those organisations responsible for critical infrastructure in various sectors.

Sophie Dawson
Partner | Australia

Emma Croft
Associate | Australia

Data

Cybersecurity - EU legislation

Forthcoming digitisation in the current global context as well as the use of new technological developments in particular for critical sectors like health, energy, finance, telecommunication and transport with simultaneous enormous increase of cyberattacks will put cybersecurity at the heart of the digital transformation and the day-to-day activities of the companies. New upcoming European legislation (including inter alia the proposal for a revised NIS Directive, the draft Directive on the Resilience of Critical Entities, the draft Digital Operational Resilience Act as well as the European Cyber Resilience Act which is expected in the third quarter of 2022) will boost this trend. 2022 will be a year of evaluations, identification of new requirements potentially relevant for companies as well as the steps needed to be in full compliance once the new rules are in force.

Dr. Natallia Karniyevich
Associate | Germany

Data

Cybersecurity - Insurance

In 2022, we will see even more global cybersecurity breaches. Cybersecurity and connected data protection advice became increasingly important in 2021 and we expect this trend will continue, leading to an increase in the use of cyber insurance. Another result of that increasing awareness is that we will see even more regulatory fines and the rise of derivative claims and compensation litigation. All organisations must be prepared for a potential data breach, but especially the organisations handling vast amounts of personal data, sensitive information or that will suffer large economic loss in the event of an incident. With larger companies have already assessed their policies, their security measures and cybersecurity insurances we will see an increasing need for all the other companies to assess its policies, its security measures and cybersecurity insurances.

Mattias Lindberg
Partner | Sweden

Data

Data Act

As a central pillar of its data strategy, the European Commission is expected to unveil its proposed Data Act in early 2022. This initiative will aim to increase access to and further the use of data, so that more public and private actors can benefit from techniques such as 'Big Data' and 'Machine Learning'. To this end, the regulation may put forward fair, reasonable, proportionate, transparent and non-discriminatory (FRAND) terms for access to and use of non-personal data, possibly complemented by model contract terms. We can also expect transparency obligations for manufacturers of connected objects. However, private companies will be wary of any obligations to open up access to their data for new market entrants and potential concerned implications for trade secrets.

Francine Cunningham
Regulatory & Public Affairs Director | Belgium

Data

Data Act - AI opportunities

New legislation related to AI may not only pose risks (such as the draft EU AI Act) but also opportunities. Under the European strategy for data, the Commission has recognised the need to increase data sharing incentives among businesses and individuals as there is not enough data available for innovative re-use, including in the development of AI. The proposal for the Data Governance Act (where Council and the European Parliament reached a provisional agreement at end of November), will boost the availability of data as the engine of AI and Machine Learning. The Data Act which is currently drafted by the European Commission and published in Q1 2022, will inter alia promote fairness in data access and be implemented in business-to-business relationships. Companies should position themselves to benefit from these new opportunities emerging on the horizon (with those affected by data access looking at how this may impact their competitive position).

Dr. Nils Loelfing
Associate | Germany

Data

Data, intelligent & connected vehicles

With increased connectivity and personal data information being exchanged, there are more legal requirements and potential disputes around liability, privacy, regulations and communication issues in the B2C and B2B area.

In China, auto data regulations have been introduced by the sectoral regulator for the automotive industry to strike a balance between the privacy rights of individuals and the promotion of Intelligent and Connected Vehicles (ICVs) technology. The importance imposed on personal data for the ICV development has been making considerable progress in other countries. With the PRC Personal Information Protection Law (PIPL) and PRC Data Security Law (DSL) coming into force, we expect more legal actions in relation to the use of data for connected vehicles in the future, which will pose compliance issues for companies operating in the automotive and transport industries.

Sven-Michael Werner
Partner | China

James Gong
Partner | China

Amanda Ge
Senior Managing Associate | China

Clarice Yue
Counsel | China

Tiantian Ke
Associate | China

Data

Data generated by connected vehicles

Connected vehicles will continue to generate more and more data. Manufacturers of connected vehicles will face increasing European legal challenges regarding personal data access requests, privacy notices, data minimisation, transfers of data, privacy-by-design solutions, police requests for log file data, e-mail minimisation, data security, right-to-repair rules, and technical access conditions to vehicle data.

Lawrence Freeman
Senior Counsel | Belgium

Data

Data localisation

Following more than two decades of rapid globalisation, and as a result of an increased focus on cybersecurity, we are seeing a shift to data localisation. Governments are looking to keep data within national borders and the ability to localise data will be just as important as the ability to globalise data previously was. It has never been more important to understand data issues.

Sophie Dawson
Partner | Australia

Jessica Laverty
Associate | Australia

Data

Data privacy litigation

In the UK, there has been a sharp increase in the number of claims filed in the High Court based on UK GDPR complaints. These range from individual complaints relating to one-off data breach incidents, through to group actions based on allegations of sustained and deliberate GDPR violations. Many thought class actions might explode in 2022, but this seems less likely now as a result of a recent Supreme Court decision which has, essentially, put the brakes on the ability to bring opt-out class actions for low-value data protection breaches. That said, the claimant data privacy bar is well-developed and well-funded in the UK and shows no signs of backing down. Some recent decisions by the courts may force them to get more creative in the way group actions are structured going forwards. In 2022, we will probably continue to see a steady number of data class actions being brought in the UK courts, and certainly no slowdown in the number of individual damages claims being brought, especially in a post-data breach scenario.

Bryony Hurst
Partner | United Kingdom

Data

Data protection & data security in China

There has been a great deal of regulatory activities in 2021 relating to technology and data worldwide, which will also have a significant impact in the digital economy and tech investment in 2022. Following the global trend, China has this year passed the Personal Information Protection Law (PIPL) and Data Security Law (DSL), to further enhance data protection. Moreover, the "China GDPR" has been finalised and will be implemented, therefore companies doing business with China should take active and prompt action to assess the impact of data legislations and respond to any compliance gaps.

James Gong
Partner | China

Amanda Ge
Senior Managing Associate | China

Clarice Yue
Counsel | China

Tiantian Ke
Associate | China

Data

Digital Governance Act

The EU is attempting to create a framework using the Data Governance Act (DGA) that encourages the re-use of data, by increasing trust in data intermediaries and strengthening data sharing mechanisms. It introduces the concept of data altruism and sets out conditions for the re-use of public sector data that is subject to existing protections like commercial confidentiality, IP rights or data protections. It aims to address the balance between rights over data and the interests in sharing data for the benefit of the economy. A European Data Innovation Board will be established to ensure the consistent application of the new rules. We expect the DGA to enter into force in 2022, creating opportunities for data intermediaries, data altruism and re-use of public sector data as per 2023.

Feyo Sickinghe
Of Counsel | Netherlands

Data

Digital Markets Act and Antitrust

In the Brussels EU antitrust community, 2022 is seen as another crucial year for the Tech & Comms sector. The year 2022 is likely to see the adoption of the Digital Markets Act and a crucial question is what this will generally mean for EU antitrust enforcement. Arguably, some practices that can be tackled under the DMA are under scrutiny already by the EC's antitrust enforcers, such as the use of non-public business data (e.g., in the ongoing Amazon marketplace investigation), and self-preferencing practices (e.g., Google Shopping, recently confirmed by the General Court).

Hein Hobbelen
Partner | Belgium

Louis Delvaux
Associate | Belgium

Andrea Whelton
Paralegal | Belgium

Data

NFTs – Risks

NFTs have changed consumer engagement with blockchain technology. The concept of Bored Apes, Cryptokitties and Top Shots have garnered considerable attention, not to mention astronomical amounts of money. With greater commercial viability comes greater regulatory scrutiny and a heightened risk for fraudulent activity, including misuse of third party intellectual property (copyfraud). Balancing the desire for engaging with customers through exciting NFT ventures poses numerous regulatory, contractual, IP, consumer law and reputational issues for organisations to consider. The high level activity in the NFT market will almost invariably also lead to increased litigation, which will have to address complex jurisdictional issues and difficulties in identifying the ultimate infringers in an area rife with pseudonymity.

Rebecca O'Kelly-Gillard
Partner | United Kingdom

NFTs – Further expansion

NFTs have captured the imagination of brands and consumers alike in 2021 (from digital art to music downloads) and this will only increase in 2022. As more consumers embrace the digital world and digital collectibles more brands will seek to exploit their content via NFTs made available on marketplaces. This will expand beyond NFTs in the arts and sports worlds to NFTs in gaming and the metaverse: think wearing your limited edition virtual trainers (recorded in a NFT) on your avatar in the metaverse or in a game.

Jonathan Emmanuel
Partner | United Kingdom

Data

Text & data mining

The UK currently lacks an exception to copyright and database rights for commercial text and data mining activities comparable to that recently adopted in the EU, under Article 4 of the Digital Copyright Directive. This potentially puts the UK at a competitive disadvantage in attracting certain types of AI research and development, as businesses may choose to train their AI systems in jurisdictions with more permissive exceptions. With this in mind, in October 2021 the UK Intellectual Property Office launched a public consultation on whether the UK should expand its text and data mining exceptions. Organisations involved in AI development should consider making a submission to the consultation and keep a close eye on any draft legislation which emerges when planning their approach to using AI training data covered by third party IP rights.

Toby Bond
Senior Associate | United Kingdom

Smart Infrastructure

Australia - sovereign space capability

The largest space project in Australia is beginning to take flight. The JP9102 tender for an Australian Defence Satellite Communications System closes on 10 January 2022, with down-selection anticipated in Q3 2022. The objective of the project is to provide sovereign space communications for the Australian Defence Force. The tender covers space, ground and control segments and will provide coverage over areas of strategic interest in the vicinity of Australia. At present, this capability is provided by satellites with a mixed payload of commercial and military. JP9102 seeks to increase the capacity, resilience, agility and flexibility of the ADF's military satellite communications. To date, four major international companies have announced bids for the project. It also presents a significant opportunity for local players to be involved and will help the Australian government realise its stated ambition of growing the Australian space industry to A$10-12B by 2030. The project is also strategically significant in a world where the weaponisation of space presents a growing threat to the global environment.

Thomas Jones
Partner | Australia

Matthew Bovaird
Senior Associate | Australia

Smart Infrastructure

Australia - new infrastructure laws

In November 2021, the Australian Parliament passed legislation amending the Security of Critical Infrastructure Act 2018. The changes aim to protect Australia's critical infrastructure against national security risks. Eleven new industry sectors must now comply with the Act, including the communications, space technology and defence industry sectors. The Act has also introduced new classes of critical infrastructure assets, such as a critical telecommunications or broadcasting assets. Under the Act, certain entities must notify the government about cybersecurity incidents affecting their critical infrastructure assets. The government also has the power to directly intervene and take over computer systems during cyberattacks, as a last resort. This is only the first phase of the new reforms. Compliance with this new framework will become a significant matter for tech clients in the new year.

Thomas Jones
Partner | Australia

Lubna Sherieff
Clerk | Australia

UK - new national security regime

The National Security and Investment Act 2021 which introduces a new national security screening regime enters into force on 4 Jan 2022. This will require mandatory notifications of transactions in 17 “sensitive areas of the economy” (communications, computing hardware, data infrastructure, quantum, space and satellite technologies), where one of the ‘trigger’ events occurs. Types of transactions covered include acquisitions of above 25% of the shares or voting rights in entities active in the UK and internal corporate restructurings. Transactions (subject to a mandatory notification) must be cleared prior to closing or will be void. Finally, the UK government has a residual ability to review transactions closed after 12 November 2020. In case of uncertainty voluntary notifications can be made and there is also scope for informal engagement. The standard review period, which applies to all notified acquisitions, lasts up to 30 working days. Transactions which raise security concerns can be called in for a further 30 working day review.

Anthony Rosen
Legal Director | United Kingdom

Peter Willis
Partner | United Kingdom

Tech & logistics

We expect the debate on how tech can be used to solve some of the challenges regarding logistics to continue. In 2022 the ESG trend will continue to have an impact and that mandatory requirements regarding, for example, sustainability plans, will be a part of both private and public procurements. But more difficult to predict is what will happen in other areas where tech and logistics crossover. For example, in connection with some of the highly debated e-scooter issues in the Stockholm area, we anticipate that attention will once again be on how suppliers will manage the supply chain issues and we also anticipate that discussions on how new tech solutions may be used to reduce negative effects. We anticipate that the main focus will shift from traditional physical supply chain legal issues to the ones that are specific to the use of digital supply chains. Increasing discussions on where the legal and ethical limits will be when for example using in-app pushes and notification to encourage correct behaviour. The technical solutions are ready - but are the citizens?

Mattias Lindberg
Partner | Sweden

Telecommunications Security Act 2021

The Telecommunications Security Act 2021 (the Act) received Royal Assent on 17 November 2021 and is designed to increase telecoms security by strengthening the obligations on providers of Electronic Communication Services (ECS) and Networks (ECN). The Act replaces section 105A-D Communications Act 2003 provisions with more detailed provisions (sections 105A to 105Z29), including more stringent security measures, power to introduce supplementary legislation, issuing new codes of practice setting out the procedures and technical measures that service providers will need to adopt and gives increased monitoring and enforcement powers to Ofcom. The security measures include making sure telecoms providers securely design, construct and maintain network equipment that handles sensitive data; reduce supply chain risks; carefully control access to sensitive parts of the network; and make sure the right processes are in place to understand the risks facing their public networks and services. The Act also introduces new powers for the government to manage the risks posed by 'high risk vendors' in the telecoms network supply chain and even ban some suppliers, if that equipment is considered to be a risk to safety and security.

Anthony Rosen
Legal Director | United Kingdom

Matthew Buckwell
Associate | United Kingdom

New Tech

5G rollout and adoption

Southeast Asian countries continue to push towards increasing the adoption of 5G at varying rates. Singapore is expected to remain the frontrunner in the 5G rollout and adoption, with the Info-communication Media Development Authority having recently concluded the first stage of its 5G spectrum auction. The Singapore Government is targeting 50% 5G coverage by end-2022, and full nationwide coverage by end-2025. The introduction of high-speed low latency 5G coverage is expected to catalyse and provide increased opportunities for the creation of a broader 5G ecosystem in Singapore, with several public and private sector trials already underway to determine viable use cases.

Other countries in the region are also expected to push towards increasing 5G deployment. The Malaysian Government has recently announced that it is reviewing the industry structure and is considering whether to stick with previous plans for a single wholesale 5G network or whether to allow multiple operators to facilitate increased competition. In Indonesia, operators have commenced limited rollout of commercial 5G services since the latter part of 2021, following initiatives by the Indonesian Government to reform existing spectrum for 5G use. This remains a space to be watched and further developments can be expected in the coming year.

Shawn Ting
Counsel | Singapore

New Tech

Spain - Artificial Intelligence sandbox

Spain will execute a sandbox project to test the proposal for an EU Regulation on AI. This pilot programme is a new way for the EU to check future Regulations, allowing volunteer companies and government entities to check how the proposed Regulation would work. This is a great opportunity for all stakeholders to participate and influence in the upcoming EU AI legal framework.

Victor Horcajuelo
Counsel | Spain

New Tech

Artificial Intelligence solutions

Artificial intelligence solutions will become increasingly ubiquitous as they are deployed in a range of industry sectors. These solutions are built on sophisticated software systems comprising of complex algorithms and deploying cutting edge computing techniques. Many of the issues which arise in the context of traditional software systems also arise for AI solutions, so there is no need for businesses to adopt a totally new approach to AI contracting. However, due to the intricacies of the way in which AI systems are developed and operated, there are certain areas where a different or more nuanced approach is required. For example: (i) lack of transparency about why decisions are made by the system may impact a supplier's willingness to take responsibility for faults; (ii) there could be questions whether any intellectual property actually exists in the content generated by AI solutions; and (iii) when AI uses personal data, then data protection issues, such as privacy by design and accountability for the decisions made by the system, will be paramount.

Will Bryson
Senior Associate | United Kingdom

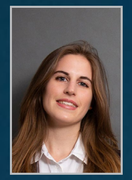
New Tech

Assisted and autonomous driving

Assisted driving is now becoming one of the main elements of the automotive industry's future mobility vision, along with electrification and data sharing. In recent months, major car manufacturers have announced plans to produce self-driving electric robotaxis which could be on the road as early as 2023.

Gian Marco Rinaldi
Counsel | Italy

Niccolò Anselmi
Associate | Italy



Marta Breschi
Associate | Italy

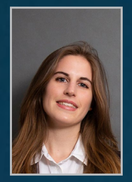
New Tech

Continued growth of bitcoin

A 2021 report by market intelligence platform Blockdata, points out that the bitcoin network processed around $489 billion per quarter in 2021, which is higher than PayPal's $302 billion. Thanks to three fundamental factors such as the growth in the average amount per transaction, the increase in the price of bitcoin and the growth in the number of transactions, it is clear that the use of bitcoin is expected to grow.

Gian Marco Rinaldi
Counsel | Italy

Niccolò Anselmi
Associate | Italy



Marta Breschi
Associate | Italy

New Tech

Ethical aspects of technological solutions

There is a clear trend to automate an increasing number of aspects of business activity. In particular, the use of AI systems has brought a clear advance pushing the limits of automations. However, the automation of business processes is not a trivial replication of automation systems used in manufacturing. The automated process may have a significant impact on human rights as automation requires embedding various assumptions into systems that are often not neutral from the ethical point of view. One of the reactions for this situation is the planned legal regulations of production, distribution and use of AI systems. However, even now there is a clear trend to verify the ethical aspects of all technological solutions at the earliest stages of their design. This trend is likely to develop in 2022.

Tomasz Zalewski
Partner | Poland

New Tech

Remote working

The trend towards atypical working in the technology sector is likely to continue during 2022, as businesses slowly settle into agile and flexible working policies implemented in the wake of the pandemic. Notwithstanding that it is the technology companies that were largely leading the push towards more flexible practices during last year, it seems that many companies in the sector are now treading more cautiously for fear of losing the innovation, collaboration and firm culture that comes from working together in an office. Overwhelmingly businesses have sought to balance these interests with employee expectations and the competition for key talent by adopting hybrid working models, but these do come with their own challenges. We expect to see legal disputes and/or more regulation or policy with respect to the “right to disconnect”, working time, health and safety, indirect discrimination, performance management and business protection.

Ian Hunter
Partner | United Kingdom

Furat Ashraf
Senior Associate | United Kingdom

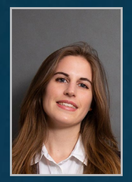
New Tech

Semiconductor and chip shortages

Worldwide shortages of semiconductors and chip may cause material issues in the relationships between equipment manufacturers and suppliers, which may result in redefinitions of the economical balances or termination of the contractual relationships. Major players in the sector are considering making huge investments in the construction of a new manufacturing site to overcome the crisis. This could lead to serious price imbalances and a potential risk of monopolisation by certain companies in the sector.

Gian Marco Rinaldi
Counsel | Italy

Niccolò Anselmi
Associate | Italy



Marta Breschi
Associate | Italy

New Tech

Smart contracts - risks

Smart contracts, where some or all of the contractual obligations are defined in and/or performed automatically by a computer program, are becoming increasingly prevalent in commercial life. Growth in this area is driven by increasingly sophisticated technology and the perceived advantages that smart contracts bring by way of increased efficiency, security and transparency. The UK Law Commission has recently concluded that the current legal framework is able to facilitate and support the use of smart contracts but identified issues that parties should consider to increase certainty and party autonomy. The Law Commission also highlighted the inherent difficulties in determining the geographical location of acts, actors and intangible objects when dealing with digital assets and smart contracts in the virtual world, which gave rise to conflict of law issues in relation to matters such as governing law and court jurisdiction in the event of disputes. The Law Commission has been tasked by the UK Government to make recommendations for reform to ensure that the law in this area remains relevant and up to date. The findings are expected to be published in the first part of 2022.

Jeremy Sharman
Partner | United Kingdom

Prashant Kukadia
Associate | United Kingdom

New Tech

Supply chain disruption

The continuing shortage of semi-conductors is disrupting supply chain and delivery commitments across the Tech & Comms sector. Already many such disruptions are resulting in formal proceedings (court litigation and international arbitration), as parties try to force manufacturers and suppliers to prioritise them, and to recoup losses suffered on delayed projects/on-sales. Parties involved in such disputes will need to consider their strategic options and leverage both as claimants or defendants/respondents, as well as mitigating their exposure through available insurance and third-party claims.

Nick Peacock
Partner | United Kingdom

New Tech

Supply chain sustainability - Blockchains

While the management of the supply chain becomes more complex and facing new challenges, blockchain technology is increasingly perceived and used as a suitable tool, to improve efficiency, transparency and traceability. The use of blockchain is allowing a significant progress in the management of the supply chain, not only in terms of reducing costs, collaboration and integration with partners and gaining speed, but also to meet compliance obligations and CSR commitments of organisations, particularly by allowing traceability and accountability in relation to the origin and authenticity of materials or energy sources, ethical labour practices and other sustainability requirements.

Pablo Berenguer
Partner | Spain

New Tech

Sustainability focused technology

In the wake of COP26 and an increasing public awareness of the urgency of climate change, there has been an increasing trend in the number of new developments and solutions that marry technology with sustainability-focused initiatives. Along with several ongoing projects in the electric vehicle and connected cars industry that have been underway for some time, we are also seeing new initiatives to use smart technology to reduce single-use packaging in the bars and restaurant supply chains, as well as in the management of toxic waste disposal. In view of the increased investor demand in this sector, we can expect even more developments and technology launches in this varied space in the next year.

Jeremy Tan
Partner | Singapore

Elaina Foo
Associate | Singapore

New Tech

- 5G rollout and adoption
- Spain - Artificial Intelligence sandbox
- Artificial Intelligence solutions
- Assisted and autonomous driving
- Continued growth of bitcoin
- Ethical aspects of technological solutions
- Remote working
- Semiconductor and chip shortages
- Smart contracts - risks
- Supply chain disruption
- Supply chain sustainability - Blockchains
- Sustainability focused technology
- Metaverse

Metaverse

The wonders of the metaverse - fully immersive virtual worlds - is only just beginning. In 2022 many organisations will be exploring the potential to create new virtual worlds, built on blockchain protocols with their own in-world token, that can be visited by their customer's avatars for a number of purposes: to connect, to watch virtual concerts, to browse and buy NFTs via virtual shop fronts. We expect things to get particularly interesting as corporates (perhaps running and operating their own "private" metaverses and not necessarily run on open blockchain protocols) and "crypto-states" (running "public" metaverses operating on public blockchain protocols and therefore built and owned by their participants) compete for the attention of the consumer.

Jonathan Emmanuel
Partner | United Kingdom

PART I

Regulation

Artificial Intelligence Act and liability

The Artificial Intelligence Act aims to create a regulatory framework for prohibited, high, medium and low risk AI-systems. It establishes an oversight and enforcement structure with specific assessment and compliance obligations for providers of AI systems. The EU is working towards the revision of the product liability directive and will be introducing a liability scheme for AI systems that is likely to affect providers in all sectors of the digital economy.

Feyo Sickinghe
Of Counsel | Netherlands

PART I

Regulation

Artificial Intelligence Act and privacy

The EU's plan to make its proposed AI Act into a global standard will take shape in the course of 2022. This "human-centric" approach to AI, divides such technology into various categories: from unacceptable and high risk, to limited and minimal risk. Overall, the higher the risk, the stricter the rules for providers and users of AI systems. Member states will continue discussing the proposal in the European Council, while the European Parliament is now starting work on the proposal after a long delay caused by a competency battle between various committees. We can expect a strong debate over potentially banning the use of facial recognition systems in public spaces. Other points of contention include industry self-assessment, transparency of algorithms and the interplay with privacy, intellectual property and competition laws. Additionally, the EU is expected to set new rules of the game regarding the liability of AI systems.

Francine Cunningham
Regulatory & Public Affairs Director | Belgium

PART I

Regulation

CpaaS to face more scrutiny in Europe

After an initial phase of consolidation, Communications Platform as a Service providers (CPaaS) are now well established in Europe. They will keep seeing their valuation soar in 2022. CPaaS providers offer a wide range of services driven by the pandemic context requiring even more dematerialized and converged customer relationships (email, voicemail, telephone, SMS, notifications, etc.). Telecom regulatory authorities are taking notice. It is likely that CpaaS providers will face even more scrutiny next year as the new EU telecom framework is progressively being transposed across member states (e.g., France) and some tension is being observed around the allocation and use of numbering resources.

Willy Mikalef
Counsel | France

PART I

Regulation

Cybersecurity – DORA

The EU is proposing a new regulation to harmonise cybersecurity requirements to improve the resilience of financial institutions. The Digital Operational Resilience Act (DORA) is expected to finally be passed in 2022, which will streamline the ICT risk management across the EU. Although subject to the principle of proportionality and while many financial institutions will already be applying some of DORA's requirements, the new regulation will require substantial efforts to be compliant. The new requirements are quite comprehensive and imposes a few requirements to the contracts between the financial institutions and their service providers. Certain critical ICT third-party service will be subject to direct oversight by Financial Regulators. However, a unified framework across Europe will help the institutions with operations in multiple countries.

Jan Ussing Andersen
Partner | Denmark

PART I

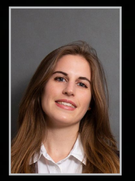
Regulation

Cybersecurity - NIS 2 Directive

Works on NIS 2 Directive will go on, and could be issued in the course of 2022. Member states will need to align their national systems to the new provisions, which will extend the scope of application (and start implementation of pre-existing local cybersecurity provisions). However, preparatory works and discussions on NIS 2 are likely to raise concerns and issues on the current status of cybersecurity legislation across EU. In addition, the national cybersecurity perimeter, as introduced in 2019, will be completed by issuance of the last implementing provisions; the Italian Cybersecurity Agency, as created in 2021, will begin its full operations. These facts will result in an increased sensitiveness and awareness on cybersecurity themes in Italy, with a more active control and action by the competent authorities.

Gian Marco Rinaldi
Counsel | Italy

Niccolò Anselmi
Associate | Italy



Marta Breschi
Associate | Italy

Growing threats posed with digitalisation and the surge in cyberattacks has created a need for revisions of the existing NIS Directive framework, in order to strengthen the security requirements, in particular relating to the security of supply chains, streamline reporting and other regulatory obligations, as well as to introduce stricter supervisory and enforcement requirements, including harmonised sanctions across the EU. The proposed expansion of the scope of the NIS2 Directive to various new entities and sectors, such as telecommunications, social media and public administration, would create significant new compliance challenges, but should assist in increasing the level of cybersecurity in Europe in the longer term, and help reduce inconsistencies in applying NIS regulation throughout the single market that could have been observed before.

Piotr Dynowski
Partner | Poland

PART I

Regulation

Digital Markets Act

As part of its mission to curtail the market power of large platforms, the EU is expected to adopt new rules that allows the European Commission to designate so called gatekeepers of core platform services and search engines. The self-executing remedies regarding use of data, data access platform and device neutrality, interoperability, portability of data, leveraging access to other core platform services, advertising and distribution channels (side loading). The new rules aim to create more room for competition and innovation by smaller market players. Other stakeholders and national authorities get to play a bigger role in the designation of gatekeepers and enforcement. The trilogue between the European Commission, the Council and the Parliament starting in January 2022, may result in a final text to be adopted in 2022, hence starting the process of designation of gatekeepers by the end of 2023.

Feyo Sickinghe
Of Counsel | Netherlands

PART I

Regulation

Digital Services Act

With huge pressure from the incoming French Presidency of the EU to get online platform regulation over the line, the next six months will see intense negotiations on the most sensitive issues in the proposed Digital Services Act (DSA). The DSA aims to introduce new obligations for online businesses providing services in the EU, with the aim of keeping users safe from illegal goods, content or services online. Member states in the European Council already adopted their general position in November 2021 and the European Parliament is expected to adopt its position soon. The three-way negotiations between the EU institutions (Council, Parliament and Commission) are set to begin in early 2022 to bring out the final agreement. We can expect animated discussions around potential restrictions on targeted advertising, deadlines for removing illegal content and the enforcement powers from the European Commission and national authorities.

Francine Cunningham
Regulatory & Public Affairs Director | Belgium

PART I

Regulation

Electronic identification, authentication and trust services

Application of new guidelines on electronic documents in Italy from 1 January 2022, will increase companies' awareness to the creation of e-documents, conservation and archiving. This will result in the need for companies to provide new resourcing and entrusting professional roles (e.g., the so-called conservators and third-party supporting companies in conservation and archiving activities). Further rules are being implemented to further align with local legislation to eIDAS requirements.

Gian Marco Rinaldi
Counsel | Italy

Niccolò Anselmi
Associate | Italy

Marta Breschi
Associate | Italy

The coronavirus pandemic has triggered an unforeseen acceleration in the digital transformation and contributed to a global rise in the prominence of various tools for remote authentication and remote contracting. In view of this the European Commission has presented a proposal for the revision of the eIDAS Regulation aimed at achieving 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). The aim of this initiative is also to create a universal pan-European single digital ID and extend the benefits of eIDAS to the private sector. This will definitely create significant new opportunities for various Digital Identity and Trust Services providers.

Piotr Dynowski
Partner | Poland

PART I

Regulation

European Electronic Communications Code Implementation - EU

Twelve EU member states have yet to (fully) implement the European Electronic Communications Code (EECC) in 2022. While implementation of the EECC was supposed to have taken place before the start of 2021, many member states are still lagging behind. The EECC marks a significant revision of the regulatory framework for telecommunications. One of the major points of this revision is that the regulations will not apply to providers such as over-the-top (OTT) players, which offer a variety of services, such as (interpersonal) communication, content and cloud services. While the EECC was intended to fully harmonise the European telecommunications regulations, many member states have taken different approaches in implementing it. Although the EECC is a next step to further harmonise these different approaches, it can lead to differences between member states and legal/regulatory uncertainty. For companies offering electronic communications networks and services on an international basis, a country-by-country assessment of key topics cannot be avoided.

Raoul Grifoni Waterman
Associate | Netherlands

European Electronic Communications Code Implementation - Italy

The Legislative Decree transposing the European Electronic Communications Code into Italian law is set to enter into force in 2022. The final text was approved by the Italian Government on 4 November 2021 and its publication in the Italian Official Journal is expected before the end of the year. The newly adopted Bill is aimed at striking a balance between consumer protection and business investments. In particular, the new legislative provisions are set to change the terms relating to the end users' right of withdrawal and to the duration of the contractual obligations between telco operators and consumers. In parallel, an extension of the enforcement powers of the Italian Communications Authority is also due to be introduced with the new Bill.

Federico Marini Balestra
Partner | Italy

Lucia Antonazzi
Associate | Italy

PART I

Regulation

European Electronic Communications Code Implementation - Spain

2022 will see the implementation of the European Electronic Communications Code (EECC) in Spain, the Spanish Parliament is currently debating the Bill for an entire new Act on telecommunications. Following EECC, this new Act will be enforceable on several relevant communication services offered by OTT (NI-ICS) requiring companies to adapt their performance to a good range of regulatory and compliance obligations (ePrivacy obligations, security measures, new fees).

Victor Horcajuelo
Counsel | Spain

PART I

Regulation

Free choice of end user equipment

Pursuant to new guidelines of the Consumer & Markets Authority, consumer users will be able to freely choose modems, routers to connect to their electronic communications network provider. The goal is to create a more competitive market for end user equipment and free choice for consumers. Network providers will need to facilitate free choice of consumer equipment in 2022.

Feyo Sickinghe
Of Counsel | Netherlands

PART I

Regulation

Net neutrality

The Court of Justice of the European Union issued judgments in three cases regarding net neutrality and zero-rating in September 2021. In all three cases, IPSs offered a zero-rated subscriptions to consumers. Zero-rated subscriptions have a data limit, but the use of certain applications or services does not count towards data consumption. The judgments, in the end, only ruled that additional limitations in the subscriptions were incompatible with the Net Neutrality Regulation. However, the wording of the ruling seems to leave room for the interpretation that zero-rating as such is also prohibited under the Net Neutrality Regulation. As there is some ambiguity, BEREC launched a consultation regarding the compliance of zero-rating. While the results have already been presented by BEREC in October 2021, a consultation of the draft updated BEREC Guidelines will follow in March 2022. ISPs should be aware of this ongoing discussion about the interpretation of the Net Neutrality Regulation.

Raoul Grifoni Waterman
Associate | Netherlands

PART II

Regulation

Online safety

A wave of new regulation is on its way in Europe and elsewhere, with the goal of holding platforms more closely to account for unlawful and harmful content hosted on their sites. The Digital Services Act in the EU is making its way through the legislative channels, the draft UK Online Safety Bill will soon be laid before Parliament for debate, and Australia's Online Safety Act comes into force early next year too. There remain opportunities for stakeholders to influence the content of the EU and UK legislation, and if any of the proposed controls/measures are likely to give rise to business-critical obstacles then companies should take advantage of these opportunities whilst they still can. However, once the laws are settled, the major challenge for platforms, especially those with global audiences, is going to be scrutinising the requirements set out in each different regime and identifying and implementing the lowest common denominator approach to ensure compliance across them all.

Bryony Hurst
Partner | United Kingdom

Outsourcing to German financial institutions

In 2022, the German financial regulator BaFin will take a closer look at outsourcing to counteract concentration risks. From 1 January 2022, financial institutions must notify BaFin of the intention and execution of outsourcing, material changes and serious incidents in the context of existing material outsourcing arrangements that may have a material impact on the institution's business activities. The financial institution will have to maintain an outsourcing register for all material and non-material outsourcing, allowing the regulator easy access. Outsourcing providers based outside the EEA that provide a material outsourcing service or acting as subcontractor for material outsourcing will have to appoint a domestic representative (process agent) in Germany.

Dr. Michael Jünemann
Partner | Germany

Johannes Wirtz, LL.M.
Counsel | Germany

PART II

Regulation

Reform of Australia's electronic surveillance framework

The Australian Government has just published the discussion paper entitled 'Reform of Australia's electronic surveillance framework' as part of its consultation process to develop a new electronic surveillance framework by 2023. The Government plans to repeal the Surveillance Devices Act 2004, Telecommunications (Interception and Access) Act 1979 and parts of the Australian Security Intelligence Organisation Act 1979 in favour of a "single, streamlined and technology-neutral Act". The existing laws were criticised by a recent review into Australia's intelligence sector as leading to "unclear and confusing laws". The new Act would govern telecommunications interception, covert access to stored communications, and the use of listening and tracking devices under a single law. The government is seeking submissions by 11 February 2022. The new legislation is also likely to see OTT and Unified Comms providers subject to similar requirements for interception and data retention as traditional carriers. This reflects a global trend towards virtualisation of networks and use of encrypted apps and tunnels for communications.

Thomas Jones
Partner | Australia

Lubna Sherieff
Clerk | Australia

PART II

Regulation

Reforms to reduce harmful scam calls and messages

The number of scam calls increased significantly in 2021, with the Australian Competition and Consumer Commission's 'Scamwatch' reporting that it received over 16,000 scam messaging reports. One common scam involves attempts to install malware on phones by asking users to access something through a fake link in a text message. The government has now amended regulations under the Telecommunications (Interception and Access) Act 1979 to assist mobile providers in preventing malicious scams. The amendment introduces matters a court needs to consider in determining whether the identifying and blocking of malicious SMS messages is 'reasonably necessary' for an employee of a carrier to perform their duties. These include matters such as the community expectation that malicious messages should be blocked and the financial or psychological harm caused by malicious messaging. The requirement that an act is 'reasonably necessary' forms part of an exception, which allows carriers to intercept or access communications to operate or maintain telecommunications systems. Australia's communications regulator, the ACMA, is also in the process of introducing new measures for telecommunications service providers to undertake identity verification checks for high-risk customer interactions and has taken a more robust approach to enforcement of the IPND Code to ensure that details for customers are valid. We will watch with interest to see what impact both these measures will have on spam calling.

Matthew Bovaird
Senior Associate | Australia

Dylan McGirr
Paralegal | Australia

PART II

Regulation

Regulation of digital platforms in the UK

We can anticipate legislation to enshrine the UK's proposed regulation of digital online platforms with Strategic Market Status ('SMS'). The new ex-ante regime will focus on the most powerful digital firms with "substantial, entrenched market power" in at least one digital activity. The new SMS regime will be enforced by the Digital Markets Unit (DMU), which is already established and sits within the CMA. It will monitor digital markets in the UK, designate firms with SMS, enforce a mandatory code of conduct and implement pro-competition interventions to address the root cause of market power and have strong enforcement powers (including fines). Mergers involving SMS firms will also need to be notified to the CMA with an anticipated new size of transaction threshold and we also expect a lower burden of proof to be placed on the CMA in challenging tech transactions.

Anthony Rosen
Legal Director | United Kingdom

Matthew Buckwell
Associate | United Kingdom

PART II

Regulation

Regulation of new technologies

The undeniable potential of non-fungible tokens (NFTs), that reaches far beyond the art market, raises serious concerns from the legal perspective. Even though the European Commission is contemplating regulating the market of crypto-assets, NFTs fall outside the scope of the proposed regulations. Therefore, when launching a project that involves issuing NFTs, a careful analysis of the legal landscape, current as well as future, is essential, particularly in terms of financial regulations. Safety and business continuity of the technological aspects of the modern economy, combined with potential threats to our human, privacy and autonomy, pushed the European Commission to prepare a set of draft regulations attempting to regulate the use of technology as such, rather than certain branches of the economy using such technology. Two examples are DORA (Digital Operational Resilience Act) and the draft Regulation on AI. We expect more regulations aimed at particular technologies in the future, which may significantly affect the way these technologies are or could be utilised by the industry.

Kuba Ruiz
Counsel | Poland

Michal Smiechowski
Senior Associate | Poland

Regulation of the internet and content

Increasing regulation of privacy and content on the internet; Governments are moving to address the perceived social impacts of social media and online content more generally. There will be plenty of developments to watch in Australia in 2022: a new framework for online safety will commence in January, including Basic Online Safety Expectations (BOSE) and a world-first adult cyber abuse scheme; draft privacy and defamation laws targeted at social media companies will be debated and likely enacted; and public consultation will continue in relation to the comprehensive overhaul of the reach, enforcement and effect of Australia's privacy laws.

Sophie Dawson
Partner | Australia

Julie Cheeseman
Partner | Australia

Strengthened consumer regulation for communications providers in the UK

In December 2020, the UK implemented the European Electronic Communication Code by way of updating the Wireless Telegraphy Act 2006 and the Communications Act 2003. Ofcom has also updated its rules (the General Conditions) with new requirements to be applied from December 2021 and further changes introduced in June 2022. The key changes include: banning mobile providers from selling locked mobile devices; enhanced rules on switching and early termination fees, to reduce disincentives for switching, end of contract notification requirements and annual best tariff information, new rules on bundles of services (e.g., voice, broadband and Pay TV and the provision of handsets); more detailed contractual requirements including contract summaries, additional transparency and information requirements, new broadband switching processes and accessibility requirements for users with disabilities.

Anthony Rosen
Legal Director | United Kingdom

Matthew Buckwell
Associate | United Kingdom

PART II

Regulation

Tech Antitrust Investigations

The European Commission (EC) has some tech antitrust investigations in the pipeline which are closely followed in the antitrust community and across the globe. Moreover, in the field of broadband, the EC is expected to publish the complete updated guidelines on how much public money member states can spend for such development and under which conditions. This can be tens of billions of euros in possible investments in a variety of areas, including increased broadband coverage, mobile infrastructure and take-up measures such as connectivity and social vouchers, this is closely followed in the State aid community.

Hein Hobbelen
Partner | Belgium

Louis Delvaux
Associate | Belgium

Andrea Whelton
Paralegal | Belgium

PART II

Regulation

Tech Merger Regulations

In the field of mergers, the EC has indicated that it will continue to use tools such as interim measures (recently applied by the EC in the ongoing Illumina/GRAIL merger investigation) to tackle risks of serious and irreparable damage to competition in fast-moving digital markets. The EC has also encouraged the use Article 22 of the Merger Regulation to allow it to review acquisitions by innovative digital companies that ordinarily would not require notification to the EC. The year 2022 will be another exciting year for the Brussels antitrust enforcement!

Hein Hobbelen
Partner | Belgium

Louis Delvaux
Associate | Belgium

Andrea Whelton
Paralegal | Belgium

PART II

Regulation

Whistleblowing

In 2022 most member states would have implemented the Whistleblowing Directive and some clients would like to widen the scope of reportable issues. This poses challenges from a data protection point of view, as data subjects rights may only be restricted to a small number of cases.

Tobias Bräutigam
Senior Counsel | Finland

Against the sharp rise in employee activism within the technology sector, and prominent examples of so-called tech whistleblowers, there is likely to be a renewed focus on internal reporting channels and processes for dealing with whistleblowing complaints. We anticipate more detailed legislation in this area during 2022 on account of the EU Whistleblowing Directive which requires all EU member states to implement legislation obliging all companies with 50 or more workers to: (i) put in place appropriate reporting channels to enable those workers to report breaches of EU law; and (ii) ensure that those making whistleblowing reports are legally protected against retaliation for having done so. The deadline for putting place any new domestic legislation that is needed to ensure compliance is 17 December 2021. Once implemented, such legislation is likely to have an impact beyond Europe and we can expect technology businesses to review and strengthen their global whistleblowing policies and procedures to align their approach and seek to avoid employee complaints entering the public domain.

Ian Hunter
Partner | United Kingdom

Furat Ashraf
Senior Associate | United Kingdom

PART II

Regulation

Data Retention Regulation

Early 2022, the Danish Supreme Court will decide, whether to invalidate the Danish data retention rules on the general obligation for telco providers to store all data on the location, duration and identity of callers and respondents for 1 year as being against basic human rights to privacy, personal data and freedom of speech. The case follows the ECJ rulings in the Digital Rights Irelands case, the Tele2/Watson case, the La Quadrature case and several similar local European cases. The Danish Justice Department has now proposed new data retention rules to avoid risk of all data retention stopping after the Supreme Court ruling. The first of its kind in the EU, which proposes a scheme of both general and targeted data retention. The proposal has been delayed because of material broad criticism, as still violating basic rights of privacy, personal data and freedom of speech. It will be interesting to see, whether the Danish proposal will fly in DK and potentially spread to other member states.

Julie Bak-Larsen
Partner | Denmark

E-signature and eIDAS Regulation

With COVID-19 and working from home, companies have adopted more and more e-signatures for their contractual documents; this trend has started in 2020 and is still increasing in 2021. The eIDAS (electronic IDentification, Authentication and trust Services) Regulation No 910/2014 of 23 July 2014 is not new, but sets up notably three level of signatures: simple, advanced and qualified, depending of the level of security and authentication of the signatory wished (e.g., pin by SMS or by ID card). Companies needs to know what type of signature to use for a particular document; a consumer credit might not need the same level of risk as a simple quotation or a commercial contract. Bird&Bird France has attended several events with Docusign related to these legal aspects of the e-signature.

Morgane Basque
Counsel | France

Country Contacts

Lawyers from our offices in **Australia, Belgium, China, Denmark Finland, France, Germany, Hong Kong, Italy, the Netherlands, Poland, Singapore, Spain, Sweden**, and the **United Kingdom** have highlighted a range of developments involving the Tech & Comms sector.

Australia

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

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

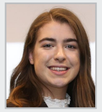
Jessica Laverty, *Associate*
+61 2 9226 9888
jessica.laverty@twobirds.com

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

Sophie Dawson, *Partner*
+61 2 9226 9888
sophie.dawson@twobirds.com

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

Belgium



Andrea Whelton
Paralegal
+3222826070
andrea.whelton@twobirds.com

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

Hein Hobbelen, *Partner*
+32 (0) 2282 6023
hein.hobbelen@twobirds.com

Lawrence Freeman, *Senior Counsel*
+32 (0)2 282 6000
lawrence.freeman@twobirds.com

Louis Delvaux, *Associate*
+32 (0)2 282 6000
louis.delvaux@twobirds.com

Country Contacts

China

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

Clarice Yue, *Counsel*
+ 852 2248 6000
clarice.yue@twobirds.com

Amanda Ge, *Senior Managing Associate*
+86 10 5933 5688
amanda.ge@twobirds.com

Tiantian Ke, *Associate*
+86 21 2312 1288
tiantian.ke@twobirds.com

Sven-Michael Werner, *Partner*
+86 21 2312 1288
svenmichael.werner@twobirds.com

Denmark

Jan Ussing Andersen, *Partner*
+45 61 61 30 10
jan.ussing@twobirds.com

Julie Bak-Larsen, *Partner*
+45 30 85 13 40
julie.bak-larsen@twobirds.com

Finland

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

France

Morgane Basque, *Counsel*
+33 (0)1 42 68 6000
morgane.basque@twobirds.com

Willy Mikalef, *Counsel*
+33 (0)1 42 68 6000
willy.mikalef@twobirds.com

Germany

Johannes Wirtz, LL.M., *Counsel*
+49 (0)69 74222 6000
johannes.wirtz@twobirds.com

Dr. Michael Jünemann, *Partner*
+49 (0)69 74222 6000
michael.juenemann@twobirds.com

Dr. Natallia Karniyevich, *Associate*
+49 (0)211 2005 6000
natallia.karniyevich@twobirds.com

Dr. Nils Loelfing, *Associate*
+49 (0)211 2005 6000
nils.loelfing@twobirds.com

Country Contacts

Italy

Federico Marini Balestra, *Partner*
+39 06 69 66 7006
federico.marinibalestra@twobirds.com

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

Lucia Antonazzi, *Associate*
+39 06 69 66 70 00
lucia.antonazzi@twobirds.com

Marta Breschi, *Associate*
+39 06 69 66 70 00
marta.breschi@twobirds.com

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

Singapore

Elaina Foo, *Associate*
+65 6534 5266
elaina.foo@twobirds.com

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

Shawn Ting, *Counsel*
+6564289823
shawn.ting@twobirds.com

Spain

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

Victor Horcajuelo, *Counsel*
+34 91 790 6000
victor.horcajuelo@twobirds.com

Poland

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

Michał Śmiechowski, *Senior Associate*
+48 22 583 79 00
michal.smiechowski@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

Sweden

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

Country Contacts

The Netherlands

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

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

United Kingdom

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

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

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

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

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

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

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

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

Peter Willis, *Partner*
+44 (0)20 7415 6696
peter.willis@twobirds.com

Prashant Kukadia, *Associate*
+44 (0)20 7415 6000
prashant.kukadia@twobirds.com

Rebecca O'Kelly-Gillard, *Partner*
+44 (0)20 7415 6000
rebecca.okelly@twobirds.com

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

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

twobirds.com

Abu Dhabi & Amsterdam & Beijing & Bratislava & Brussels & Budapest & Casablanca & Copenhagen & Dubai & Dusseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & San Francisco & Shanghai & Singapore & Stockholm & Sydney & Warsaw