EU GEOPOLITICAL RISK UPDATE KEY POLICY & REGULATORY DEVELOPMENTS

No. 116 | 26 August 2024

This regular alert covers key policy and regulatory developments related to EU geopolitical risks, including in particular, economic security, Russia's war against Ukraine, health threats, and cyber threats. It does not purport to provide an exhaustive overview of developments.

This regular update expands from the previous Jones Day COVID-19 Key EU Developments – Policy & Regulatory Update (last issue No. 99) and EU Emergency Response Update (last issue No. 115).

LATEST KEY DEVELOPMENTS

Competition & State Aid

- Joint Statement on Competition in Generative AI Foundation Models and AI Products
- European Commission publishes Staff Working Document on Foreign Subsidies Regulation
- European Commission approves further schemes under Temporary Crisis and Transition Framework to support economy in context of Russia's invasion of Ukraine and accelerating green transition and reducing fuel dependencies

Trade / Export Controls

- EU and Singapore issue Joint Statement on concluding negotiations for landmark Digital Trade Agreement
- EU and US hold first high-level Minerals Security Partnership Forum event
- Council of the European Union expands sanctions against Russia, Belarus, and Iran

Medicines and Medical Devices

- Council of the European Union adopts position on proposed Regulation on compulsory licensing for crisis management
- European Commission statement on European General Court's judgment on access to COVID-19 purchase agreements

Cybersecurity, Privacy & Data Protection

- European Artificial Intelligence Act enters into force
- EU Member States publish first report on EU cybersecurity risk evaluation in the telecommunications and electricity sectors

COMPETITION & STATE AID

Competition

Joint Statement on Competition in Generative AI Foundation Models and AI Products (see here)

On 23 July 2024, competition authorities for the EU, UK, and US released a Joint Statement on Competition in Generative AI Foundation Models and AI products*.

Backdrop / objectives. The Joint Statement responds to the transformational potential of AI, including so-called foundation models.** It notes that AI is one of the most significant technological developments in recent decades, which can introduce new means of competing, catalyzing opportunity, innovation and growth. Given this, the authorities commit to safeguarding against tactics that could undermine fair competition, in order to ensure the fair treatment of consumers and businesses.

AI risks. The authorities seek to address AI risks before they become entrenched or irreversible harms, including the following three main risks in particular:

- **Concentrated control of critical inputs**: Some key components (e.g. specialized chips) are vital to developing foundation models. This could possibly create bottlenecks across the layers of technologies and components that make up an AI system (so-called AI stack), which could impact the development and innovation of these tools.
- **Deepening market power in AI-related markets**: Some digital firms already possess strong advantages and substantial market power at multiple levels related to the AI stack. These advantages can allow those firms to extend or entrench their positions on the market, which could harm future competition.
- **Collaboration among key players**: Arrangements between firms developing AI (e.g., partnerships, financial investments) can be used to undermine competitive threats and steer market outcomes at the expense of the public.

Safeguards. The Joint Statement then identifies three main principles to protect competition and foster innovation in the AI ecosystem:

- **Fair dealing**: Firms with market power should engage in fair-dealing and not exclusionary tactics that can undermine competition and discourage innovation.
- **Interoperability**: Fostering interoperability will enhance competition and innovation in the AI field. If interoperability is claimed to harm privacy and security, this will be carefully examined.
- **Choice**: Choice among diverse AI products should be ensured through competitive processes, such as by scrutinizing how companies may employ “lock-in” mechanisms to prevent companies or individuals from seeking other options.

The Joint Statement also identified other competition risks associated with AI, for example, the risk of using algorithms to enable competitors to exchange competitively sensitive information. The authorities further committed to

	monitor and address any specific risk that may arise in connection with other AI developments and applications. * *Joint Statement on Competition in Generative AI Foundation Models and AI Products presented by Margrethe Vestager, Executive Vice-President and Competition Commissioner; Sarah Cardell, Chief Executive Officer, U.K. Competition and Markets Authority; Jonathan Kanter, Assistant Attorney General, U.S. Department of Justice; and Lina M. Khan, Chair, U.S. Federal Trade Commission.* ** *A foundation model (also known as large AI model) is a machine learning or deep learning model that is trained on broad data such that it can be applied across a wide range of use cases. Foundation models have transformed AI, driving well-known generative AI applications like ChatGPT.*
State Aid	
European Commission publishes Staff Working Document on Foreign Subsidies Regulation (see here)	On 26 July 2024, the European Commission released a Staff Working Document (SWD) that seeks to clarify how it will apply and make assessments under the Foreign Subsidies Regulation (FSR) (*Regulation (EU) 2022/2560 of 14 December 2022 on foreign subsidies distorting the internal market*), which started to apply on 12 July 2023. To recall, in the Commission's view, the FSR will help level the playing field in relation to companies that receive subsidies from outside the EU, given the Commission's power to investigate such aid with the aim of ensuring that it does not create distortions in the EU. If the Commission deems that such distortions arise, the Commission can deploy a wide range of redressive measures, which include the repayment of a foreign subsidy, the prohibition of an M&A transaction, or the rejection of a tender in a public procurement. (*see also Jones Day EU Emergency Response Update No. 110 of 23 November 2023*). The SWD sets outs, in particular, initial clarifications on the following: • Assessment of the existence of a distortion caused by a foreign subsidy on the internal market in various contexts (e.g., distortions caused by unlimited guarantees, which can take many forms and may go beyond an explicit statement or legal act referring to the undertaking concerned, for instance, where an undertaking benefitting from an unlimited guarantee may receive a loan from a private bank that *prima facie* appears to be on market terms, but whose conditions actually reflect the existence of such guarantee); • Application of the balancing test to weigh the positive and negative effects of foreign subsidies distorting the internal market (e.g., the Commission's balancing assessment will include information received on possible positive effects, which may be provided by all relevant stakeholders (the undertakings under investigation, the EU Member States, and other third parties)). Looking ahead. The SWD's initial clarifications will be further developed through case practice and EU case law. The Commission will also publish guidelines on applying certain FSR provisions at the latest by 12 January 2026.

European Commission approves further schemes under Temporary Crisis and Transition Framework to support economy in context of Russia's invasion of Ukraine and accelerating green transition and reducing fuel dependencies (see here)	The Commission approved additional measures under the State aid Temporary Crisis and Transition Framework (TCTF) to support the economy in the context of Russia's invasion of Ukraine and in sectors key to accelerating the green transition and reducing fuel dependencies (as most lately amended on 2 May 2024 and 20 November 2023). Among the most recently approved State aid schemes under the TCTF (up to 26 August 2024): – Amendments to an existing Italian scheme supporting companies active in Southern Italy in the context of Russia's war against Ukraine, with modifications to the existing scheme such as a budget increase by €2.9 billion, bringing the overall budget from €11.4 billion to €14.3 billion. – €158 million Dutch scheme to support the investments for the production of equipment necessary to foster the transition to a net-zero economy, in line with the Green Deal Industrial Plan. – €10.82 billion French scheme to support offshore wind energy to foster the transition to a net-zero economy. – €50 million Austrian scheme to support primary agricultural producers in the context of Russia's war against Ukraine. – €400 million Italian scheme to support investments in the decarbonisation of industrial production processes to foster the transition towards a net-zero economy, in line with the Green Deal Industrial Plan. – Amendment to an existing Romanian scheme, including an overall €54.4 million (RON 270.7 million) budget increase, to support tomato and garlic producers in the context of Russia's war against Ukraine. – -€200 million Finnish scheme to support the production of renewable fuels of non-biological origin and the deployment of energy storage to foster the transition towards a net-zero economy, in line with the Green Deal Industrial Plan. – €1.5 billion French scheme to support sustainable biomethane production to foster the transition to a net-zero economy. – €25 million Slovak scheme to support livestock producers in the context of Russia's war against Ukraine. – €750 million Dutch State aid scheme to support the decarbonisation of industrial processes to foster the transition to a net-zero economy. – €1.2 billion Spanish State aid scheme to support investments in the production of renewable hydrogen to foster the transition to a net-zero economy. – Amendments to an existing Dutch scheme, including a €50 million budget increase, to support agricultural producers in the context of Russia's war against Ukraine.

TRADE / EXPORT CONTROLS

EU and Singapore issue Joint Statement on	On 25 July 2024, the EU and Singapore (the Parties) issued a Joint Statement upon concluding negotiations for a Digital Trade Agreement*

concluding negotiations for landmark Digital Trade Agreement (see here)	(DTA), which will benefit businesses and consumers that engage in digital trade.** As noted by the Commission, this DTA is "*the first EU agreement of its kind, reflecting the EU's aspiration to be a global standard-setter for digital trade rules and cross-border data flows*." The DTA reflects the strategic significance of digital trade and Southeast Asia's pivotal role, given the considerable growth of its digital economy. In this respect, over half of the total trade in services between the EU and Singapore is already digitally delivered and represented 55% of total EU-Singapore trade in 2022 (worth €43 billion). The DTA is expected to further bolster EU-Singapore trade relations, notably by: – **facilitating digitally-enabled trade in goods and services** (e.g. through the use of electronic contracts and signatures; and a re-affirmed commitment to develop or maintain single window customs systems to facilitate a single, electronic submission of all information required by customs and other legislation for the export, import, and transit of goods); – **ensuring cross-border data flows without unjustified barriers** (e.g. not prohibiting the transfer of data into the territory of a Party); and – **reinforcing trust in digital trade** (e.g., protecting personal data; limiting spam). Alongside the DTA negotiations, the EU and Singapore also held the second Trade Committee meeting under the EU-Singapore Free Trade Agreement (EUSFTA), which entered into force on 21 November 2019. The DTA will serve as a key complement to the EUSFTA by reinforcing this trade connection and providing further opportunities for growth. Next steps. The EU and Singapore will now pursue their respective approval processes in view of formally signing and concluding the DTA. The DTA will become binding on the Parties under international law only after completion by each Party of its internal legal procedures necessary for the entry into force of the agreement. * *This text was published for information purposes only and may undergo further modification and is without prejudice to the final outcome of the agreement.* ** *Digital trade covers trade in goods and services enabled by the internet and other technologies (e.g., items ordered online for physical delivery; use of technologies in production or distribution processes, such as real-time tracking of deliveries; and transferring data across borders.*
EU and US hold first high-level Minerals Security Partnership Forum event (here)	On 18 July 2024, the EU and US co-chaired the inaugural high-level event for the Minerals Security Partnership (MSP) Forum, which was the first major gathering of its 23 member countries. To recall, the MSP Forum was announced on 5 April 2024 by the EU, US, and other Minerals Security Partnership (MSP)* partners (*see also Jones Day EU Emergency Response Update No. 114 of 6 May 2024*). The MSP Forum provides a new cooperation platform for critical raw materials (CRMs), focusing on minerals and metals supply chains most relevant for

	clean energy technologies, e.g., lithium, cobalt, nickel, manganese, graphite, rare earth elements, copper, and others. During this first high-level event, the EU and US notably communicated the MSP Forum's primary objectives and a roadmap for the Forum, including as concerns its two work streams: • **project development** to support and accelerate investment opportunities and implementation of sustainable CRM projects; and • **policy dialogue** to promote diversification and resilience of supply chains, strengthen sustainable CRM production and local capacities, promote regulatory cooperation to enhance fair competition and predictability, and foster high environmental, social, and governance (ESG) standards in CRM supply chains. The event also formally welcomed eight new MSP Forum member countries (Argentina, Greenland, Kazakhstan, Mexico, Namibia, Peru, Ukraine, and Uzbekistan). These new members significantly reinforce and diversify the Forum's objective of partnering with resource-rich countries and countries with high demand for these resources to explore mutually beneficial projects. Various potential member countries also joined the event to better understand the benefits of joining the MSP Forum. ** The MSP is a collaboration between the EU and 14 countries (Australia, Canada, Estonia, Finland, France, Germany, India, Italy, Japan, Norway, Republic of Korea, Sweden, UK, and U.S.) to catalyze public and private investment in responsible critical minerals supply chains globally.*
Council of the European Union expands sanctions against Russia, Belarus, and Iran (see here)	The EU relies on restrictive measures (sanctions) as one of its tools to advance its Common Foreign and Security Policy (CFSP) objectives, such as safeguarding EU's values, fundamental interests, and security; preserving peace; and supporting democracy and the rule of law. Sanctions include measures such as travel bans (prohibition on entering or transiting through EU territories); asset freezes; prohibition on EU citizens and companies from making funds and economic resources available to the listed individuals and entities; ban on imports and exports (e.g., no exports to Iran of equipment that might be used for internal repression or for monitoring telecommunications), and sectoral restrictions. Among the most recent developments to the EU sanctions regimes: **Russia**: On 22 July 2024, the Council renewed EU restrictive measures for another 6 months (until 31 January 2025) in view of Russia's continuing actions destabilizing the situation in Ukraine (see here). These measures notably target high-value sectors of the Russian economy and further enable the EU to counter the circumvention of sanctions. Additionally, on 28 June 2024, the Council listed two individuals and four entities for circumventing EU sanctions and materially supporting the Russian government (see here), including through circumvention schemes and illegal weapon trade schemes with the Democratic People's Republic of Korea (DPRK) in support of the Russian Government. Altogether, EU restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine now apply to over 2,200 individuals and entities.

The Council's overview of EU sanctions against Russia over Ukraine (since 2014) is also available here. To recall, EU restrictive measures taken against Russia, as first introduced in 2014 in response to Russia's actions destabilizing the situation in Ukraine, have significantly expanded following Russia's military aggression against Ukraine, starting on 23 February 2022 in adopting the so-called first package of sanctions. The Council adopted the 14th package of sanctions on 24 June 2024 (*see also Jones Day EU Emergency Response Update No. 115 of 24 June 2024*).*

* *An in-depth analysis of the 14th package of sanctions against Russia is available from the authors of the EU Geopolitical Risk Update (see contact details below for Nadiya Nychay (Brussels) and Rick van 't Hullenaar (Amsterdam)).*

Belarus and Iran. In the context of Russia's invasion of Ukraine, the EU has also adopted sanctions against these two countries, and most lately:

- Belarus. On 29 June 2024 (see here), the Council adopted further restrictive measures targeting the Belarusian economy, in view of the regime's involvement in Russia's war against Ukraine. The restrictive measures notably concern:
  - Exports, e.g., export restrictions on goods that could enhance Belarusian industrial capacities;
  - Imports, e.g., prohibitions on importing directly, or indirectly purchasing or transferring, gold, diamonds helium, coal and mineral products including crude oil from Belarus.
  - Services, e.g., prohibiting the provision of certain services to the Belarus government and to any natural or legal person acting on its behalf or at its direction, such as accounting, legal advisory, or market research services.
  - Anti-circumvention, e.g., EU exporters' future contracts must contain the so-called "no-Belarus clause," which contractually prohibits the re-exportation to Belarus or re-exportation for use in Belarus of sensitive goods and technology, battlefield goods, firearms and ammunition.
  - Protecting EU exporters, e.g., EU operators may claim compensation from damages caused by Belarusian individuals/companies due to sanctions implementation and expropriation, provided that such EU operator lacks effective access to remedies, for example, under a relevant bilateral investment treaty.

    For an overview of EU restrictive measures against Belarus, see here.

- Iran. On 15 July 2024 (see here), the Council prolonged EU restrictive measures until 27 July 2025 in view of Iran's military support for Russia's war against Ukraine and for armed groups and entities in the Middle East and the Red Sea region.

  The sanctions regime applies to 12 persons and nine entities, with existing restrictive measures subject to annual review.

  For an overview of EU restrictive measures against Iran, see here.

MEDICINES AND MEDICAL DEVICES

Council of the European Union adopts position on proposed Regulation on compulsory licensing for crisis management (see here)

On 26 June 2024, the Council adopted its negotiating position on the proposed Regulation on compulsory licensing for crisis management ("proposed Regulation").

Issue. A compulsory license allows a government to permit a third party to use an intellectual property right without the rights-holder's authorization. In crisis situations, such as a pandemic or natural disaster, compulsory licensing can facilitate access to essential products and technologies. This is particularly useful, for example, when the patent holder cannot produce the necessary quantities of a key product.

Currently, since only EU Member States regulate compulsory licensing mechanisms, this can lead to a fragmented approach during cross-border crises and does not foster the cross-border supply chains that are key to the EU internal market.

Response. On 27 April 2023, the European Commission released the proposed Regulation (see here), aimed at ensuring that a "Union compulsory license" would only be granted following the activation of an emergency or crisis mode at the EU level and would be closely tied to other crisis instruments. The Union compulsory licensing mechanism is intended as an alternative in crises when voluntary agreements are not feasible, in view of ensuring appropriate territorial coverage to include cross-border supply chains.

The Council's negotiating mandate introduced several modifications to the initial proposed Regulation, and in particular:

- Emphasizes the 'last resort' nature of any compulsory licensing decision, such that it should only be used when voluntary agreements are not available or adequate;
- Establishes remuneration for the license rights-holder, potentially exceeding the previously established cap of 4% of revenue generated by the licensee;
- Strengthens the roles of the advisory body and national intellectual property experts in the decision-making process; and
- Protects rights-holders from having to disclose trade secrets.

Next steps. The Council's negotiating position now provides the Council presidency with a mandate to negotiate with the European Parliament, which had earlier adopted its position on the proposed Regulation on 13 February 2024.

European Commission statement on European General Court's judgment on access to COVID-19 purchase

On 17 July 2024, the European Commission issued a statement on the European General Court's judgements issued that day in two cases on access to documents concerning the Commission's purchase agreements with pharmaceutical companies for COVID-19 vaccines (see *T-689/21 Auken and Others v Commission* and *T-761/21 Courtois and Others v Commission*, available here and here).

Disputed access to documents. Between 2020 and 2021, the European Commission signed contracts with several pharmaceutical companies to

agreements (see here)	purchase COVID-19 vaccine doses. In January 2021, Members of the European Parliament ("MEPs"), in the name of public interest, requested access to these documents from the Commission. The Commission granted partial access only and stated that the redacted version of the documents had been made public on the Commission's website. It contended that the passages had been redacted on the basis of the exceptions relating to the protection of privacy, integrity of the individual, protection of commercial interests, and protection of the decision making process of the institutions. The MEPs challenged that decision before the General Court. The General Court largely supported the Commission, which it found entitled to provide only partial access in light of the protection of commercial interests covering certain contract clauses (e.g., concerning intellectual property rights, location of production sites, delivery schedules). However, the General Court also ruled that the Commission should have: – provided more explanations to justify refusing access to certain provisions in the contracts (e.g., the Commission did not explain how access to provisions on vaccine donations and resales could undermine the commercial interests of the undertakings concerned). – provided the personal data related to the members of the negotiation teams, composed of Member State representatives and Commission officials. The Commission further highlighted that in these cases, it needed to strike a difficult balance between the right of the public to information and the legal requirements arising from the COVID-19 contracts themselves. It also noted that in many cases in the past, the European Court of Justice had recognized the need to protect the business interests of a contractual partner. Next steps. The Commission stated that it will carefully study the General Court judgments and their implications, and it reserves its legal options.

CYBERSECURITY, PRIVACY & DATA PROTECTION

European Artificial Intelligence Act enters into force (see here)	On 1 August 2024, the European Artificial Intelligence Act (AI Act)* entered into force. To recall, the AI Act is the world's first comprehensive EU regulation aimed at governing artificial intelligence. Its main goal is to ensure trustworthy AI to protect the safety and fundamental rights of people and businesses and to establish a harmonized internal market for AI in the EU. Scope. The AI Act applies to public and private actors inside or outside the EU when an AI system is placed on the EU market, or if its use has an impact on people located in the EU. The AI Act notably applies a uniform framework across the EU, based on forward-looking definition of AI according to product safety rules and a risk-based approach, and in particular:

- Minimal risk: The vast majority of AI systems fall into this category (e.g., AI-enabled recommendation systems, spam filters). Operators of such AI systems are not subject to any obligations under the AI Act, due to their minimal risk to individuals' rights and safety.
- Limited risk: For risks associated with lack of transparency in AI usage, the AI Act imposes specific transparency obligations on operators of AI systems (e.g., chatbots that interact with individuals, such that users must be informed that they are interacting with a machine).
- High risk: AI systems identified as "high-risk" may harm people's safety and fundamental rights (e.g., AI systems used to assess whether a person can receive a loan, certain medication, etc.). Operators of high-risk systems must comply with strict requirements, such as risk-mitigation systems, high quality of data sets, logging of activity, human oversight, and a high level of accuracy and cybersecurity.
- Unacceptable risk: The AI Act prohibits AI systems considered as clearly threatening fundamental rights of individuals. These include systems that manipulate human behavior to circumvent the user's free will (e.g., toys with voice assistance encouraging dangerous behaviors), systems that perform social scoring activities, and certain applications of predictive policing based solely on profiling people.

The AI Act also introduces rules applicable to general-purpose AI models (i.e., highly capable AI models designed to perform a wide variety of tasks like generating human-like text).

Oversight / penalties. Member States have until 2 August 2025 to designate national competent authorities to oversee the application of the rules for AI systems and conduct market surveillance activities. The Commission's AI Office will be the key implementation body for the AI Act at EU-level, as well as the enforcer for the rules for general-purpose AI models (*see also Jones Day EU Emergency Response Update No. 115 of 24 June 2024*). Three advisory bodies will help the AI Office to implement the AI rules: the European Artificial Intelligence Board, a scientific panel of experts, and an advisory forum.

Companies failing to adhere to the AI Act are subject to fines of:

- Up to €35 million or 7% of global annual turnover of the preceding financial year (whichever is higher) for violations of banned AI applications;
- Up to €15 million or 3% of global annual turnover of the preceding financial year (whichever is higher) for violations of other obligations; and
- Up to €7.5 million or 1% of global annual turnover of the preceding financial year (whichever is higher) for providing incorrect information to notified bodies and national competent authorities in reply to a request.

Next steps : The majority of rules under the AI Act will start applying on 2 August 2026. However, prohibitions on AI systems deemed to present an unacceptable risk will already apply after six months, and rules for general-purpose AI models will apply after 12 months.

	The Commission also initiated the AI Pact for the transitional period prior to the AI Act's full implementation. It is also developing guidelines to detail how the AI Act should be implemented, in consultation with stakeholders. * *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*
EU Member States publish first report on EU cybersecurity risk evaluation in the telecommunications and electricity sectors (see here)	The Member States, supported by the Commission and ENISA, published the first report on EU cybersecurity risk evaluation and scenarios for the telecommunications and electricity sectors.* Risks. The report highlights a number of technical and non-technical risks, including those arising in both the telecommunications and electricity sectors: • Supply chain risks are viewed as the main threat and are particularly high for 5G rollouts and renewable energy infrastructures. • Ransomware and destructive malware ("data wipers") are also a key area of risk, in particular, where operational technology is used. Among the risks specific to the electricity sector, these include "malicious insiders", who are considered as a particularly high risk. The phenomenon is due to the difficulty in adequately vetting new personnel and attracting local cybersecurity talent. In the telecommunications sector, among the main threats, these include ransomware attacks on the vast databases of sensitive information held by the mobile subsector; and attacks originating from large bot networks (attackers using vulnerable devices such as home routers, legacy personal computers, and IoT devices to create large botnets, i.e., groups of devices under the control of a malicious actor and used for other types of attacks). Mitigation. The report provides recommendations across four areas to mitigate these risks: • Resilience and cybersecurity strength can be improved through, e.g., sharing good practices on mitigating ransomware, vulnerability monitoring, human resources security and asset management; closer cooperation between relevant authorities, including the Member States' Computer Security Incident Response Team (CSIRTs); and Member States must also carry out self-assessments for the targeted sectors, in compliance with other EU directives. • Collective cyber situational awareness and information sharing needs reinforcing, e.g., through the ability to detect and monitor cyber threats and incidents in the wider geopolitical context, and combating growing cyber influence operations and disinformation campaigns conducted by state-sponsored actors. • Contingency planning, crisis management, and operational collaboration need reinforcing through, e.g., enhanced communication lines between sectors and cybersecurity authorities, including at an EU level.

- Supply chain security should be further addressed through, e.g., a preliminary assessment of supply chain cybersecurity risks stemming from dependencies on high risk third-country providers of critical hardware and software components; and the development of an EU framework for supply chain security.

Next steps: The report encourages Member States, ENISA, and the Commission to implement measures as soon as possible. This includes, in particular, initiating cyber exercises at national and EU-wide level, including sectoral exercises in the telecommunications and energy sectors.

* *This follows a report drafted by the same stakeholders in February 2024 on cybersecurity and resilience of the EU's communication infrastructures and network (see here).*

LAWYER CONTACTS

Kaarli H. Eichhorn
Partner, Antitrust & Competition Law; Government Regulation; Technology
Brussels
keichhorn@jonesday.com
+32.2.645.14.41

Dr. Jörg Hladjk
Partner, Cybersecurity, Privacy & Data Protection; Government Regulation; Technology
Brussels
jhladjk@jonesday.com
+32.2.645.15.30

Nadiya Nychay
Partner, Government Regulation; Antitrust & Competition Law
Brussels
nnychay@jonesday.com
+32.2.645.14.46

Cristiana Spontoni
Partner, Health Care & Life Sciences; Government Regulation
Brussels
cspontoni@jonesday.com
+32.2.645.14.48

Rick van 't Hullenaar
Partner, Government Regulation; Investigations & White Collar Defense
Amsterdam
rvanthullenaar@jonesday.com
+31.20.305.4223

Dimitri Arsov *(Associate),* ***Lucie Fournier*** *(Associate),* ***Mihai Ioachimescu-Voinea*** *(Associate),* ***Cecelia Kye*** *(Consultant), and* ***Justine Naessens*** *(Associate) in the Brussels Office contributed to this Update.*