EU GEOPOLITICAL RISK UPDATE KEY POLICY & REGULATORY DEVELOPMENTS

No. 120 | 4 February 2025

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

- European Commission Releases Communication on Competitiveness Compass for the EU
- European Commission approves €48 million French State aid measure to support new factory for producing lithium-ion batteries for electric vehicles
- European Court of Auditors to reorient focus of auditing COVID-19 recovery funds

Trade / Export Controls

- Council of the European Union extends sanctions against Russia
- European Commission issues Recommendation on reviewing outbound investments in technology areas critical for EU economic security

Medicines and Medical Devices

- EU Health Technology Assessment Regulation becomes applicable
- European Commission unveils action plan to protect the health sector from cyberattacks

Cybersecurity, Privacy & Data Protection

- Cyber Solidarity Act and targeted amendment to Cybersecurity Act enter into force
- Digital Operational Resilience Act (DORA) becomes directly applicable
- EU AI Act – Recent legal developments and guidelines

COMPETITION & STATE AID

Competition

European Commission Releases Communication on Competitiveness Compass for the EU (see here)

On 30 January 2025, the Commission released a Communication on a Competitiveness Compass for the EU, which presents its five-year plan to boost Europe's competitiveness.

This is the Commission's first major initiative of its new mandate, building on the Draghi Report of 9 September 2024 on the future of European competitiveness. The Compass outlines the Commission's workplan to address Europe's vulnerabilities arising from a lack of innovation and lagging productivity growth by comparison to other major economies The Compass states that Europe's freedom, security, and autonomy will depend more than ever on its ability to innovate, compete, and grow.

The Compass focuses on **three core action areas**:*

(i) Closing the innovation gap by driving productivity through innovation, e.g., by facilitating the establishment of start-ups and conditions for scaling up and investing in state-of-the-art infrastructures.

In this respect, competition policy plays a key role, and to keep pace with the global race to develop cutting edge technologies and innovations, the Compass indicates that competition policy must adapt to evolving markets to better enable companies to grow and compete in global markets. This calls for, in particular, revised Horizontal Merger Control Guidelines such that innovation, resilience, and the investment intensity of competition in certain strategic sectors are given proper consideration in light of the European economy's urgent needs.

(ii) Pursuing a joint roadmap for decarbonization and competitiveness, towards achieving Europe's ambitious goal to reach a decarbonized economy by 2050, by integrating decarbonization policies with industrial, competition, economic and trade policies e.g., by promoting the competitiveness of clean technology manufacturers.

On the role of competition policy, companies (especially energy intensive ones) need a flexible and supportive State aid framework to support their efforts to switch to clean technologies. In the new Clean Industrial Deal, in particular, the Commission seeks to set out how well-targeted, simplified State aid can spur investment for decarbonization, while avoiding market distortions.

(iii) Reducing excessive dependencies and increasing security by better integrating open strategic autonomy and security considerations in EU economic policies, e.g., by introducing a European preference in public procurement for strategic sectors and technologies through revision of directives on Public Procurement.**

These three core areas will be supported by a set of so-called horizontal enablers for competitiveness, such as:

- Simplification, aiming at significantly reducing regulatory and administrative burdens;

	– Lowered barriers to the Single Market, in particular through a Horizontal Single Market Strategy to modernize the governance framework, removing intra-EU barriers and preventing the emergence of new ones; and – Enhanced coordination of policies at EU and national level, including introducing a Competitiveness Coordination Tool, aimed at aligning industrial and research policies and investments at the EU and national levels in selected key areas and projects deemed of strategic importance and of common European interest. Progress on the Competitiveness Compass will be annually monitored and reported through the Annual Single Market and Competitiveness Report, most lately published on 29 January 2025 (see here). * *Many of the Compass's recommendations are also already reflected in Commission President Ursula von der Leyen's Political Guidelines 2024-2029 and mission letters to members of the new College of Commissioners (see also Jones Day Commentary, "European Commission President Unveils Proposed New Team of EU Commissioners and Political Priorities" of 25 September 2024 (here)).* ** *For more on the planned revision of the Public Procurement Directives, see also Jones Day EU Geopolitical Risk Update No. 119 of 31 December 2024.*
State Aid	
European Commission approves €48 million French State aid measure to support new factory for producing lithium-ion batteries for electric vehicles (see here)	On 31 January 2025, the Commission approved a €48 million French State aid measure to support Envision AESC France in the first phase of a new factory for producing lithium-ion batteries for electric vehicles in Douai, France. The Commission assessed the measure under EU State aid rules, in particular Article 107(3)(a) of the TFEU (which allows Member States to promote the economic development of the most disadvantaged areas of the EU) and the 2022 Regional Aid Guidelines (RAG).* According to the Commission, the measure will contribute to its Political Guidelines 2024-2029, which lay out the Commission's new plan for Europe's sustainable prosperity and competitiveness, including by responding to the dangers of economics dependencies and the crucial need for resilient supply chains. In particular, the new Douai plant will create jobs and promote both regional development and the green transition of the regional economy. The plant, designed to be carbon neutral, will produce lithium-ion batteries for electric vehicles with an annual capacity of 9 GWh in its first phase. Looking ahead. The project is expected to create some 1,000 direct jobs in Douai, as well as other indirect jobs in the region. Subsequent phases of the plant may extend to production of stationary electrical storage (combined with solar and wind generation). The non-confidential version of the decision will be made available under the case number SA.109228 in the State aid register on the Commission's competition website once confidentiality issues are resolved.

	* *The Commission's 2022 RAG sets out the conditions for considering regional aid as compatible with the internal market and the criteria for identifying the areas fulfilling the conditions of Article 107(3)(a) and (c) of the TFEU. On this basis, Member States notified their regional aid maps to the Commission for approval.* *Earlier, in December 2024, the Commission also notably approved €81 million Spanish State aid measure to support production of semiconductor-grade synthetic diamonds under Article 107(3)(a) and the RAG (see Jones Day EU Geopolitical Update No. 119 of 31 December 2024).*
European Court of Auditors to reorient focus of auditing COVID-19 recovery funds (see here)	On 27 December 2024, the European Court of Auditors (ECA) announced that in 2025-2026, its core auditing work would remain focused on the €800 billion NextGenerationEU (NGEU) package for Europe pandemic recovery, and in particular, its core instrument, the Recovery and Resilience Facility (RRF). To recall, the RRF was established in February 2021 by RRF Regulation (EU) 2021/241 (running until end-2026) in response to the COVID-19 crisis to support faster and more resilient Member State recovery. It is the EU's largest funding instrument to date, at over €700 billion. EU Member States must allocate a significant part of RRF funding to measures for the twin green and digital transitions. The ECA's audits had initially focused on the RRF's design and its weaknesses (e.g., concerns about the traceability and transparency of funds disbursed). In 2025-2026, the ECA will shift its focus to assessing the RRF's actual implementation. The ECA will first review its RRF audit work to date and publish a consolidated report in Spring 2025 to spotlight risks, challenges, and opportunities. The ECA's new audits will then focus on, e.g., digital transformation, reforms in energy efficiency, and Member State control systems for procurement, State aid, and fraud prevention. Looking ahead. EU policymakers will be discussing the shape of the EU's new long-term budget from 2027 onwards (multi-annual financial framework) and must take into account the ECA's findings on the RRF and NGEU. As ECA President Tony Murphy stated before the European Parliament, the EU must assess current challenges and risks before considering reforms and moving on to future plans, in order to foster a future that promotes solidarity, accountability, and trust among EU citizens.
TRADE / EXPORT CONTROLS	
Council of the European Union extends sanctions against Russia (see here and here)	The EU employs restrictive measures, commonly known as sanctions, as a key instrument to advance its Common Foreign and Security Policy (CFSP) objectives. These objectives include safeguarding the EU's values, fundamental interests, and security; preserving peace; and supporting democracy and the rule of law. Sanctions encompass a range of measures, including travel bans that prohibit entry or transit through EU territories, asset freezes, and restrictions on EU citizens and companies from providing funds and economic resources to listed individuals and entities. Additionally, sanctions may include bans on imports and exports, such as prohibiting the export to Iran of equipment that could be used for internal repression or telecommunications monitoring, as well as sectoral restrictions.

	Russia: On 27 January 2025, the Council renewed EU restrictive measures for another 6 months (until 31 July 2025) in view of Russia's continuing actions destabilizing the situation in Ukraine. These measures encompass a wide array of sectoral measures, notably including limitations on trade, finance, energy, technology and dual-use goods, industry, transport, and luxury goods, as well as further enabling the EU to counter the circumvention of sanctions. Also on 27 January 2025, the Council listed three Russian individuals for targeting Estonia with a series of cyberattacks. Altogether, EU restrictive measures with respect to malicious cyber activities threatening the Union or its Member States now apply to 17 individuals and 4 entities. The Council provides an overview of EU sanctions against Russia concerning Ukraine (since 2014), available here. To recall, the EU's restrictive measures against Russia, initially introduced in 2014 in response to Russia's destabilizing actions in Ukraine, have significantly expanded following Russia's military aggression against Ukraine, beginning on 23 February 2022, with the adoption of the first package of sanctions. The Council adopted the 15th package of sanctions on 16 December 2024 (*see also Jones Day EU Geopolitical Risk Update No. 119 of 31 December 2024*) and the 16th package of sanctions on 24 February 2025 (see here).* * *The 16th package of sanctions against Russia will be reported in the forthcoming Jones Day EU Geopolitical Risk Update No. 121, and an in-depth analysis of the 16th package 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)).*
European Commission issues Recommendation on reviewing outbound investments in technology areas critical for EU economic security (see here)	On 15 January 2025, the Commission issued a Recommendation on reviewing outbound investments in technology areas critical for the economic security of the Union.* Context. The Recommendation is part of the Commission's broader European Economic Security Strategy, introduced in June 2023, which addresses Europe's shortcomings in adequate preparedness for new and emerging risks.** The Recommendation follows the Commission's White Paper on Outbound Investments (January 2024) and related public consultation results (July 2024), which support the Commission's proposed step-by-step approach to monitor and assess these investments. Objectives. In unveiling the Recommendation, Maroš Šefčovič, Commissioner for Trade and Economic Security; Interinstitutional Relations and Transparency, stated: *"[T]he geopolitics of today means that we must have a deeper understanding of the potential risks [that providing and attracting investment] may entail. The assessment of EU outbound investment in key technology areas will allow us to have a clearer picture of potential threats we face. With this knowledge, we will be better equipped to strengthen our economic security and guide future policy choices, while enhancing a robust and open investment environment in the EU."* The Recommendation urges EU Member States to review outbound investments made by EU investors in third countries, in view of ensuring that these investments do not compromise the EU's strategic interests or technological leadership. In this respect, the Commission advocates for

enhanced cooperation among national authorities to assess risks and safeguard economic security.

While recommendations are non-binding, they often serve to influence behavior and encourage alignment with EU goals. The Commission's authority and the political significance of its recommendations typically prompt voluntary compliance, such as adjusting national policies.

Scope of monitoring / transactions: The Recommendation identifies three high-risk technology sectors for monitoring of outbound investments: semiconductors; artificial intelligence ("AI"); and quantum technologies.

On the scope of transactions, the Recommendation calls for reviewing five areas: mergers and acquisitions; asset transfers; joint ventures; venture capital; and greenfield investments. Member States are urged to review new, ongoing, and completed transactions since 1 January 2021, with the potential to extend to earlier ones if Member States identify specific concerns.

Monitoring tools and information gathering: The Recommendation encourages Member States to implement voluntary or mandatory filings of transaction information. Member States are also encouraged to gather comprehensive data to assess risks of outbound investment transactions in critical technology areas.

Next steps: Member State assessments of transactions, with the Commission's support, will focus on technology leakage and geopolitical factors, with progress reports due by 15 July 2025 and a final report due by 30 June 2026 that addresses identified risks and implementation progress. Implementing these measures along these timelines is likely to be challenging, given the expected need to enact national legislation. Ultimately, the information collected will form the basis for further discussions on EU-wide screening of outbound investments.

* *See also Jones Day Commentary, "The Rise of Outbound Investment Screening: The U.S. and EU Initiate Measures" of 10 February 2025.*

** *See also Jones Day EU Emergency Response Update No. 103 of 24 June 2023.*

MEDICINES AND MEDICAL DEVICES

EU Health Technology Assessment Regulation becomes applicable (see here)

On 12 January 2025, the Health Technology Assessment Regulation became applicable ("HTA Regulation" (EU) 2021/2282 of 15 December 2021). The HTA Regulation is a key step towards accelerating and broadening access to new medicines.

Backdrop. Health technology assessment ("HTA") is an evidence-based scientific process that enables national authorities to assess the relative effectiveness of new or existing health technologies.* HTA focuses, in particular, on the added value of a health technology compared to other new or existing technologies.

New EU-level approach. In order to improve and streamline the evidence base for assessing new health technologies, such as new medicines, medical devices and diagnostic tools, the HTA Regulation creates an EU-level framework for HTA, and in particular:

	• Establishes an HTA Coordination Group composed of representatives from national HTA bodies. Its key tasks are to coordinate and adopt the joint HTA work carried out by its subgroups (e.g., for identifying emerging health technologies) under the HTA Regulation and to adopt methodological and procedural guidance documents for joint work; • Requires Member States' HTA bodies to conduct Joint Clinical Assessments ("JCA") of new medicines and certain high-risk medical devices, which provide a scientific analysis of clinical evidence on the relative effects of a health technology on health outcomes. In this respect: – The procedure for health technology developers is streamlined by requiring only a single EU-level submission file for JCA (rather than, as in the past, multiple parallel submissions to the different national HTA systems). – Member States must give due consideration to the JCA reports in the national HTA; and • Provides for Member States to engage in further voluntary cooperation, e.g., for health technologies other than medicines and medical devices, or for assessing non-clinical HTA aspects (such as economic, ethical, organizational, social, and legal aspects). The HTA Regulation thereby aims to support national authorities in making more timely and informed decisions on pricing and reimbursement, while respecting the Member State competences. It additionally aims to offer more clarity and predictability concerning the clinical evidence requirements for HTA. Looking ahead. The HTA Regulation will initially apply to new active substances to treat cancer and to all advanced therapy medicinal products (ATMPs). They will be expanded to orphan medicinal products in January 2028, and to all centrally authorized medicinal products as of 2030. Selected high-risk medical devices will also be assessed under the HTA Regulation as of 2026. The HTA Regulation's implementing acts and guidelines are published on the European Commission's website (see here). Furthermore, the Commission has issued factsheets (see here, here and here) and a Q&A (see here) on the new health technology assessment. * *Health technologies are medicinal products, medical devices, medical and surgical procedures and measures for disease prevention, diagnosis or treatment used in healthcare.*
European Commission unveils action plan to protect the health sector from cyberattacks (see here)	On 15 January 2025, the Commission presented the European Action Plan on the Cybersecurity of Hospitals and Healthcare Providers ("Action Plan"), a deliverable of Commission President Ursula von der Leyen's Political Guidelines 2024-2029. Backdrop. Hospitals and healthcare systems are facing increasing threats driven by the high value of patient data, including electronic health records. Over the past four years, the health sector has become the most attacked industry in the EU, including during the COVID-19 pandemic when health infrastructure was increasingly targeted by cyberattacks. The stakes are particularly high as the sector undergoes a vital digital transformation.

Objectives. The Action Plan aims to strengthen the cybersecurity and resilience of Europe's hospitals and healthcare providers, which will require a unified EU-level approach that gathers the necessary resources, expertise, and tools to effectively tackle cyber threats. To achieve this, ENISA is viewed as best placed to establish, within its organization, a dedicated European Cybersecurity Support Centre ("Support Centre") for hospitals and healthcare providers.

The Support Centre will progressively develop a comprehensive service catalogue to respond to the needs of hospitals and healthcare providers, setting out available services for preparedness, prevention, detection, and response, as identified under the Action Plan's four priorities and accompanying proposed actions for each of these:

1. Enhanced prevention: The healthcare sector's ability to prevent cybersecurity incidents should be strengthened through enhanced preparedness measures such as, for example, developing guidance on implementing critical cybersecurity practices; a regulatory mapping tool to simplify compliance; as well as developing cybersecurity learning resources for healthcare professionals.

2. Better detection and identification of threats: The Support Centre will, for instance, aim to establish an EU-wide early warning subscription service for the health sector that delivers near-real-time alerts on potential cyber threats for hospitals and healthcare providers by 2026.

3. Response to cyberattacks to minimize impact: A rapid response service for the health sector under the EU Cybersecurity Reserve (created under the Cyber Solidarity Act*) should be established. The Reserve will provide incident response services from trusted private service providers. As part of the Plan, national cybersecurity exercises can take place along with the development of playbooks to guide healthcare organizations in responding to specific cybersecurity threats, including ransomware.

4. Deterrence: Furthermore, cyber threat actors should be deterred from attacking healthcare systems, such as by fostering cross-border investigations through greater sharing of indicators of compromise and other relevant data, and an increased focus on high-value targets and key criminal facilitators.

The Action Plan will be implemented in conjunction with healthcare providers and the wider health ecosystem, Member States, and the cybersecurity community. Specific actions will be rolled out progressively in 2025 and 2026.

* *For more details on the Cyber Solidarity Act, see below Section on Cybersecurity, Privacy & Data Protection.*

CYBERSECURITY, PRIVACY & DATA PROTECTION

Cyber Solidarity Act and targeted amendment to Cybersecurity Act	On 4 February 2025, the Cyber Solidarity Act* and the targeted amendment to the Cybersecurity Act** entered into force. The new laws are part of the EU cybersecurity legislative package and aim to strengthen the EU's solidarity and capacity to detect, prepare for, and

enter into force (see here and here)	respond to cybersecurity threats and incidents (see also *Jones Day EU Emergency Response Update No. 113 of 2 April 2024*). More specifically: (1) The Cyber Solidarity Act is one of the building blocks towards EU cyber resilience, along with notably the EU Cyber Resilience Act and the EU NIS 2 Directive. In particular, the Act establishes: - A European Cybersecurity Alert System, a network of National and Cross-border Cyber Hubs to provide real-time situational awareness and enable authorities and other relevant entities to effectively respond to cybersecurity threats and incidents; - A Cybersecurity Emergency Mechanism to provide enhanced preparedness and response capabilities to significant and large-scale cyber incidents, e.g., through a new EU Cybersecurity Reserve (a mechanism consisting of incident response services from trusted providers from the private sector that are ready to intervene at the request of Member States, EU institutions, or associated third countries); and - A European Cybersecurity Incident Review Mechanism to review and assess significant or large-scale cyber incidents, including the effectiveness of actions under the above-referred Emergency Mechanism. (2) The targeted amendment to the Cybersecurity Act of 2019 aims to enhance EU's cyber resilience by enabling the future adoption of European certification schemes for so-called "managed security services." The targeted amendment recognizes the increasing importance of managed security services in preventing, detecting, responding to, and recovering from cybersecurity incidents. These services include, for example, incident handling, penetration testing, and security audits. The establishment of European certification schemes for these managed security services will help to increase their quality and comparability, foster the emergence of trusted cybersecurity service providers, and avoid fragmentation of the internal market. * *Regulation (EU) 2025/38 of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents.* ** *Regulation (EU) 2025/37 of 19 December 2024 amending Regulation (EU) 2019/881 as regards managed security services.*
Digital Operational Resilience Act (DORA) becomes directly applicable (see here)	On 17 January 2025, the Digital Operational Resilience Act ("DORA")* became directly applicable (*see also Jones Day Commentary, Understanding DORA: Digital Operational Resilience Act Now in Effect for Financial Entities and ICT Service Providers, 16 January 2025*). DORA aims to strengthen the digital operational resilience framework for financial entities in the EU and complements other EU cybersecurity laws (e.g., above-referred EU Cyber Resilience Act and EU NIS 2 Directive). DORA applies to a wide range of financial entities, such as banks, insurance companies, and crypto-asset service providers. DORA also imposes new obligations on the management bodies of financial entities and on "critical" information and communications technology ("ICT")

	service providers that support financial entities, subjecting them to direct oversight by EU financial regulators. To comply with DORA, in-scope financial entities must adopt robust measures across various key areas, e.g.: - Develop and maintain a comprehensive ICT risk management framework capable of identifying, monitoring, preventing, and mitigating ICT-related risks, with regular reviews and internal audits; - Establish processes to detect, respond to, and report ICT-related incidents and major operational or security payment-related incidents to the relevant supervisory authorities; - Put in place a robust digital operational resilience testing program; and - Develop and regularly review ICT third-party risk management strategy, including mandatory provisions in contracts with ICT service providers. Enforcement. Supervisory authorities will oversee compliance and have wide-ranging powers, such as access to documents and data. Member States must establish penalties for non-compliance, which may include criminal fines, remediation orders, and personal fines and sanctions on senior management. Next steps. - Financial entities should map relevant ICT services, evaluate their current ICT risk management practices for compliance with DORA and revise contractual arrangements with ICT service providers. Where necessary, they should update and formalize ICT governance frameworks, incident response protocols, and third-party monitoring procedures. - ICT service providers serving financial entities should review customer contracts to ensure alignment with DORA requirements and should also accordingly revisit arrangements with their subcontractors to ensure compliance across the supply chain. * *Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector.*
EU AI Act – Recent legal developments and guidelines	The EU AI Act, which entered into force on 1 August 2024, aims to guarantee that AI systems placed on the European market and used in the EU are safe and respect fundamental rights and EU values (*see also Jones Day Commentary, EU AI Act: First Rules Take Effect on Prohibited AI Systems and AI Literacy, 28 February 2025*). First compliance deadline. The Act sets out staggered phases for compliance with the various areas that it regulates. The first compliance deadline occurred on 2 February 2025, with the following provisions taking effect: - Definition of AI systems. To assist providers and other relevant persons in determining whether a software system constitutes an AI system subject to the AI Act, the Commission issued non-binding Guidelines on the definition of an AI system to facilitate effective and uniform application of the rules.

- Prohibited risk category. This prohibition effectively bans the use of AI systems deemed to pose "unacceptable risks." Towards ensuring its proper and consistent application, the Commission published non-binding Guidelines on prohibited AI systems and practices.
- AI Literacy. This rule requires all providers and deployers of AI systems (even AI systems classified as low-risk or no risk) to ensure that their personnel have a sufficient level of understanding of AI, including its opportunities and risks, to use AI systems effectively and responsibly. To comply, companies must implement AI governance policies and training programs for their employees to comply.

  The Commission has launched a living repository of AI literacy practices from AI systems' providers and deployers to encourage learning and knowledge exchange on AI literacy.

Other measures to ensure uniform application of the AI Act are progressing. Key developments notably address general purpose AI ("GPAI") models:

- Code of Practice. The Commission issued a third draft General Purpose AI Code of Practice for developers of GPAI models (i.e., AI systems that can perform multiple tasks across different domains and contexts). The draft Code, expected to be finalized by May 2025, will serve as a guideline for developers to adhere to the AI Act's provisions.
- The Commission also unveiled a template on 17 January 2025 for summarizing training data used in GPAI models, which is a key component of the forthcoming GPAI Code of Practice (*see also Jones Day Commentary "European Commission's AI Code of Practice and Training Data Summary Template" of 5 February 2025*).

Next steps. The next major compliance deadline is 2 August 2025, when EU Member States must designate national authorities for AI Act enforcement. On this date, rules also take effect regarding penalties, governance, and confidentiality. On 2 August 2026, most other AI Act obligations become effective.

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