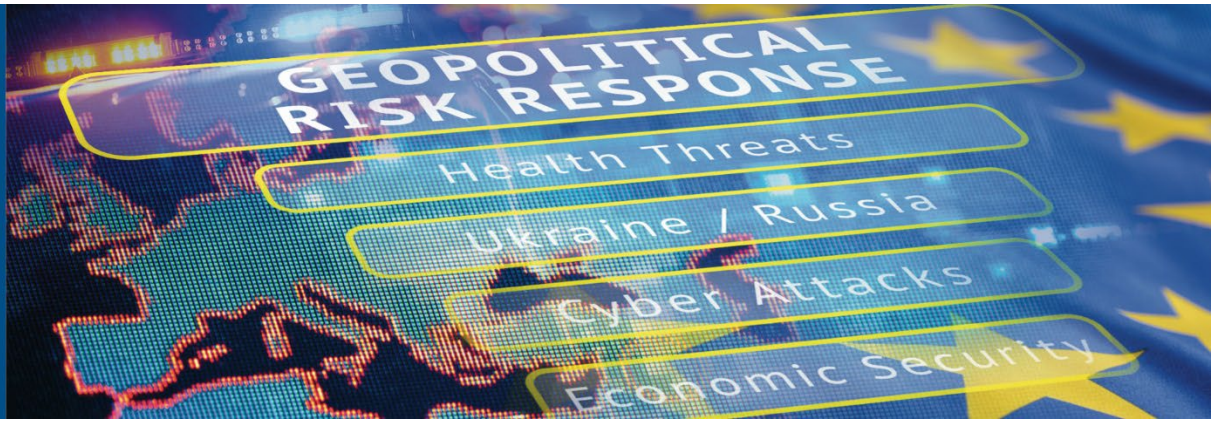

EU GEOPOLITICAL RISK UPDATE KEY POLICY & REGULATORY DEVELOPMENTS

No. 123 | 8 October 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 Fourth Annual Report on Implementation of Recovery and Resilience Facility
- European Commission holds consultation on revision of Rescue and Restructuring Guidelines

Trade / Export Controls

- Adoption of simplification of carbon border adjustment mechanism (CBAM) Regulation
- Council of the European Union extends sanctions against Russia

Medicines and Medical Devices

- European Union prevention, preparedness and response plan for health crises: Call for Evidence
- EU4Health 2025 calls for proposals: Advancing crisis preparedness through diagnostics and medical countermeasures

Cybersecurity, Privacy & Data Protection

- ENISA publishes Threat Landscape Report 2025
- EU Data Act becomes applicable
- EU AI Act - Recent developments

COMPETITION & STATE AID

European Commission releases Fourth Annual Report on Implementation of Recovery and Resilience Facility (see here)

On 8 October 2025, the Commission published the Fourth Annual Report on the Implementation of the Recovery and Resilience Facility.* The Report covers data and information up to 31 August 2025, unless otherwise specified.

Backdrop. To recall, the Recovery and Resilience Facility (RRF) is the cornerstone of the unprecedented €800 billion NextGenerationEU package created in December 2020 to support Europe's pandemic recovery.

Disbursements. The RRF is set to disburse up to €650 billion in grants and loans to EU Member States, whose national recovery plans for implementing the RRF must allocate a significant part of RRF funding to measures for Europe's green and digital transitions.

As of 31 August 2025, total disbursements amounted to €362 billion, reflecting 2,586 milestones and targets (out of 6,985 in total) that the Commission had deemed as satisfactorily fulfilled. Thus, some 44% of the RRF allocation remains to be disbursed.

Challenges. The RRF's implementation has faced the challenge of successive crises, and in particular, Russia's war against Ukraine and the consequent energy crisis, high inflation, and supply chain disruptions. In response, Member States modified their national recovery plans by adding chapters reflecting the REPowerEU Plan launched in 2022 (*see also Jones Day EU Geopolitical Risk Update No. 122 of 31 August 2025*), aimed at reducing dependencies and energy imports from Russia and diversifying the EU's energy supplies.

Report highlights. These include, in particular:

- *RRF accomplishments.* The Member States' concrete outputs and results stemming from the implementation of RRF measures are featured in so-called common indicators covering 14 areas, such as the following (based on the latest reporting round, ending on 31 December 2024):
  - Deploying over 900,000 new or upgraded clean vehicle recharging stations, spurred by investments and reforms supporting charging stations for electric vehicles;
  - Connecting 16 million households to high-speed internet; and
  - Supporting 1.2 million enterprises to develop digital products, services, and apps.
- *Accelerated RRF implementation – an ongoing priority*. The Report emphasizes the need for Member States to fast-track implementation of their national recovery plans, as the RRF comes to a close in 2026. In this respect, the Report refers to the Commission's Communication on NextGenerationEU - The road to 2026 of 4 June 2025, which urges Member States to revise their national plans to only retain measures that can be expected to be fully and timely implemented (*see also Jones Day EU Geopolitical Risk Update No. 122 of 31 August 2025*).

The Commission is currently reviewing a number of payment requests and revised national plans submitted by several Member States (*see below Next steps for deadlines)*.

- *Transparency.* The Member States have improved transparency by releasing information on publicly accessible national websites about the 100 largest final recipients of RRF funds (see here).

  According to the latest Member State reporting in 2025, the majority of the 100 largest final recipients are engaged in measures to promote, in particular:

  – the green transition e.g., sustainable mobility and energy efficiency (23.6% of recipients);

  – smart, sustainable, and inclusive growth, e.g., R&D, building renovation/construction (20.6% of recipients); and

  – the digital transformation, e.g., digital public services and business digitalization (20.5% of recipients).

Next steps. As the RRF approaches its close in 2026, Member States must fulfill all milestones and targets by 31 August 2026 and submit their last payment requests for assessment by 30 September 2026. The Commission will make final payments by 31 December 2026. No payments will be made in 2027.

For an overview of implementation of the RRF and national recovery plans, see the RRF Scoreboard.

* *For the Third Annual Report of 10 October 2024, see here.*

European Commission holds consultation on revision of Rescue and Restructuring Guidelines (see here)

Ahead of the Commission's planned revision of the 2014 Guidelines on State aid for rescuing and restructuring non-financial undertakings in difficulty (Rescue and Restructuring Guidelines), it conducted a call for evidence and public consultation (from 22 August 2025 to 14 November 2025). The Guidelines provide the conditions under which State aid to non-financial undertakings in difficulty may be considered in line with EU rules.

Since the adoption of the current Rescue and Restructuring Guidelines over a decade ago, the Commission notes that European companies are confronted by new challenges in the face of a shifting market and geopolitical context. Notably, the Commission argues that the European steel sector faces serious challenges to its competitiveness, and says that it does so particularly in light of alleged global overcapacity.

The revision of the Rescue and Restructuring Guidelines notably seeks to:

- widen the scope of the Guidelines to include the steel sector, which is currently excluded;
- amend the "undertaking in difficulty" (UiD) definition, in light of certain types of innovative start-ups having a specific growth model (e.g., high upfront innovation costs, covered by subsequent rounds of equity finance), as the current UiD definition may have unintended effects by:

  – inadvertently allowing such start-ups to fulfill UiD criteria, even if they are not in difficulty – this would contradict the objective of

the UiD definition, which is to identify undertakings that will almost certainly fail in the short or medium term; and

- unjustifiably excluding inherently viable undertakings from other types of State aid – this would contradict the objective of supporting and incentivizing innovation by European companies, including in particular start-ups and scale-ups; and

- align the Guidelines with recent EU case-law.

Looking ahead. In view of facilitating the proper revision of the current Rescue and Restructuring Guidelines (set to expire by 31 December 2025); the Commission prolonged their validity for one year (until 31 December 2026).

The revision of the Guidelines will build on feedback gathered during the Commission's consultation process. The forthcoming draft revised Guidelines will also be published for stakeholder consultation and discussion with the Member States.

TRADE / EXPORT CONTROLS

Adoption of simplification of carbon border adjustment mechanism (CBAM) Regulation (see here)

On 8 October 2025, the European Parliament and the Council of the European Union adopted a Regulation to amend Regulation (EU) 2023/956, in view of simplifying and strengthening the EU's carbon border adjustment mechanism (CBAM).*

Backdrop. The amended CBAM Regulation arises from the so-called Omnibus I legislative package of proposals, which seeks to simplify EU rules, boost competitiveness and investment, and support the transition to a more sustainable economy (*see also Jones Day EU Geopolitical Risk Update No. 121 of 14 March 2025*).

CBAM, to recall, addresses greenhouse gas emissions embedded in imports into the EU of certain products in carbon-intensive industries, in view of ensuring equivalent carbon pricing for imports and domestic products. In this respect, the CBAM seeks to prevent the risk of so-called carbon leakage, which jeopardizes the EU's greenhouse gas emissions reduction efforts when businesses (i) increase emissions outside EU borders by relocating production to non-EU countries with less stringent policies to tackle climate change, or (ii) increase imports of carbon-intensive products.

CBAM's scope initially applies to imports of certain goods and selected precursors whose production is carbon-intensive and at greatest risk of carbon leakage: iron and steel, cement, fertilizers, aluminium, electricity and hydrogen ("CBAM goods").

The CBAM is designed to operate in parallel with the EU Emissions Trading System ("EU ETS"),** to mirror and complement its functioning on imported goods. CBAM will gradually replace the existing EU mechanisms to address the risk of carbon leakage, and in particular the free allocation of EU ETS allowances for sectors covered by CBAM.***

Key changes under amended CBAM Regulation, in view of reducing regulatory, administrative, and compliance burdens, include the following in particular:

	– Exempting small importers from CBAM requirements by introducing a new CBAM cumulative annual threshold of 50 tonnes per importer. This is expected to exempt an estimated 90% of importers (e.g., some 180,000 importers), while maintaining some 99% of emissions within the CBAM scope. – Easing compliance for those importers remaining subject to CBAM's scope (e.g., simplifying data collection processes and calculation of emissions). – Facilitating transition to definitive CBAM regime. Following the expiry of the current CBAM transitional phase (ending on 31 December 2025), under the definitive regime (applied as from 1 January 2026) only authorized CBAM declarants may import CBAM goods into the EU. A high number of applications for authorization are thus expected in early 2026. To avoid disruptions for importers while awaiting authorized CBAM status, the amended Regulation provides that pending such authorization, imports of CBAM goods will be allowed under certain conditions. Looking ahead. The Commission conducted a call for evidence, closed on 25 September 2025, which resulted in gathering nearly 250 stakeholder opinions (see here) on the rules on (i) the methodology for calculating emissions embedded in CBAM goods; (ii) the adjustment of CBAM certificates to reflect the EU ETS free allocation; and (iii) the deduction of the carbon price paid in a third country. The results of this call for evidence will inform the Commission in preparing three Implementing Regulations (expected by end-2025) to address the above set of rules. * *Regulation (EU) 2025/2083 of 8 October 2025 amending Regulation (EU) 2023/956 as regards simplifying and strengthening the carbon border adjustment mechanism.* ** *The EU ETS is one of the EU's key climate change mitigation policies and is the world's first carbon market, aimed at providing an efficient mechanism to reduce emissions. Under the EU ETS, companies must obtain emission allowances covering their carbon emissions. The default option is to purchase allowances at an auction, but these can also be allocated for free, which is a transitional method of allocating allowances.* *** *CBAM will equalize the price of carbon paid for EU products operating under the EU ETS and the one for imported goods. This will be done by requiring companies importing into the EU to purchase so-called CBAM certificates to pay the difference between the carbon price paid in the country of production and the price of carbon allowances in the EU ETS.*
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: Among recent developments:

(i) On 3 October 2025, the Council **prolonged the restrictive measures** against those responsible for Russia's destabilizing actions abroad for one year (until 9 October 2026), **in view of Russia's sustained hybrid activities**, including sabotage, disruption of critical infrastructure, cyberattacks, and Foreign Information Manipulation and Interference (FIMI) against the EU and its Member States and partners.

These EU restrictive measures currently apply to 47 individuals and 15 entities. The measures target, for example, the **841st Separate Electronic Warfare Center**, and two high ranking members of its staff. The Warfare Center, one of the strongest electronic warfare groups in Russia, is linked to GPS signal failures in various European countries, primarily affecting the Baltic States. Interference and manipulation of GPS signals have led to obstacles for landing civil aviation planes.

(ii) On 12 September 2025, the Council **prolonged the restrictive measures** targeting those responsible for undermining or threatening the territorial integrity, sovereignty and independence of Ukraine, **for another six months** (until 15 March 2026).

The restrictive measures provide for the freezing of assets and a ban on making funds or other economic resources available to the listed individuals and entities, as well as a travel ban for natural persons, which prevents them from entering or transiting through EU territories.

Altogether, EU restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine now apply to over 2,700 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 (see here).*

* *The 19th package of sanctions, adopted on 23 October 2025 (see here), will be addressed in a forthcoming EU Geopolitical Risk Update. An in-depth analysis of the 19th package is available from the authors of this Update (see contact details below for Nadiya Nychay (Brussels) and Rick van 't Hullenaar (Amsterdam)).*

MEDICINES AND MEDICAL DEVICES

European Union prevention, preparedness and response plan for health crises: Call for Evidence (see here)

On 1 October 2025, the European Commission published a Call for Evidence, which ran until 29 October 2025, on a European Union-level plan for the prevention, preparedness and response plan for future health crises.

Purpose. The initiative aims to promote a coordinated response to cross-border health threats at both the EEA (European Economic Area) and national levels, as well as to complement national prevention, preparedness

	and response plans. It is a key action under the EU Preparedness Union Strategy of March 2025 to tackle cross-sectoral threats and hazards. This forthcoming Union plan also seeks to build on other Commission initiatives, such as the Medical Countermeasures Strategy against public health threats and the Stockpiling Strategy aimed at securing essential goods (e.g., medicines, food, water, fuel) in the event of a crisis (*see also Jones Day EU Geopolitical Risk Update No. 122 of 31 August 2025*). The plan is also intended to reinforce the European Centre for Disease Prevention and Control's (ECDC) role in epidemiological surveillance and threat assessment and the European Medicines Agency's (EMA) crisis preparedness and medicine shortage mechanisms. Scope / approach. According to the Call for Evidence, the scope of the intended Union plan extends to threats of biological, chemical, environmental and unknown origin, and other cross-border health threats. It aims to set out joint arrangements for governance, capacity, and resources, in particular, to: • Secure information sharing; epidemiological surveillance and monitoring; early warning and multi-hazard assessments of short- and long-term risks; risk and crisis communication; multisectoral collaboration; access to medical countermeasures; and emergency research and innovation; and • Ensure stakeholder cooperation. With these goals in mind, the Health Security Committee (HSC) met on 15 October 2025 to discuss the upcoming Union plan (see here). The Commission outlined four guiding approaches for the plan, in view of seeking to: (i) Cover all-hazards, encompassing all types of disruptive events, irrespective of their nature or cause, (ii) Adhere to the One-Health strategy, reflecting the closely linked determinants for the health of humans, domestic and wild animals, plants, and the wider environment, (iii) Bring together the whole-of-government at all levels of administration, and (iv) Draw on the whole-of-society, in view of furthering an inclusive approach preparedness and resilience. Next steps: The Commission's adoption of the Union plan, which will take the form of a Commission Communication, is scheduled for release in Q4 2025.
EU4Health 2025 calls for proposals: Advancing crisis preparedness through diagnostics and medical countermeasures (see here)	On 4 September 2025, the Health Emergency Preparedness and Response Authority (HERA) published two new calls for proposals under the EU4Health programme to strengthen Europe's preparedness against health crises: (1) Diagnostics for vector-borne diseases (see here) • This call for proposal (*EU4H-2025-HERA-PJ-2*) aims at strengthening preparedness against mosquito-borne diseases, such as dengue, Zika, chikungunya, and West Nile virus, stating that: *"Vector-borne diseases are an increasing challenge for public health in the EU."*

- The call will seek to address shortcomings of existing diagnostic tools (i.e. lack of sufficient sensitivity and specificity, cross-reactivity, limited ability to test for several conditions in parallel) by supporting the pursuit of late-stage development of rapid, innovative, and cost-effective diagnostic solutions aimed at: (i) enabling timely detection and diagnosis in resource-limited settings, (ii) reducing reliance on central laboratory infrastructure, and (iii) improving early treatment and help limit transmission.

(2) Medical countermeasures against chemical, biological, radiological, and nuclear (CBRN) threats (see here)

- This call for proposal concerns the development of innovative medical countermeasures for CBRN threats for which there are currently no or only limited treatment options. According to the Commission, CBRN incidents are of low probability but potentially high impact.

  The call for proposal is structured around three sub-topics to develop:

  i. EU4H-2025-HERA-PJ-1-a: Medicinal products (vaccines and treatments) focusing on threat-agnostic and platform-based approaches,* especially for biotoxins (e.g., antivirals, antimicrobials), as well as chemical agents (e.g., antidotes), and radio-nuclear agents (e.g., treatments against acute radiation syndrome).

  ii. EU4H-2025-HERA-PJ-1-b*:* Reusable respiratory personal protective equipment (PPE) and protective suits.

  iii. EU4H-2025-HERA-PJ-1-c*:* Innovative detection and diagnostic tools to rapidly detect individual or a broad range of chemical and biological agents.

These EU4Health actions focus on late-stage development, deployment readiness and integration into health systems. Such actions will operate alongside other EU instruments that support health security, including Horizon Europe, the EU's key funding programme for research and innovation.

Next steps: The EU Funding and Tenders Portal accepted proposals until 4 December 2025.

* *Platform-based approaches concern technologies that can be rapidly adapted to produce different medical countermeasures, such as vaccines, by using a common underlying platform, e.g., mRNA.*

CYBERSECURITY, PRIVACY & DATA PROTECTION

ENISA publishes Threat Landscape Report 2025 (see here)

On 1 October 2025, the European Union Agency for Cybersecurity (ENISA) released its annual Threat Landscape Report for 2025.

This Report analyzed 4,875 cybersecurity incidents reported between 1 July 2024 and 30 June 2025, offering an overview of the key threats and trends shaping the EU's current cyber ecosystem. The Report focuses on both the tactics of threat actors and the broader context of their activity (e.g., geopolitical drivers).

Main findings. The Report reveals a maturing threat environment, featuring the swift exploitation of vulnerabilities and increasing complexity in tracking adversaries. Notably:

- Primary targets: The public administration sector was the most targeted (38.2%), followed by transport (7.5%), particularly maritime, air, and logistics; digital infrastructure and services (4.8%); finance (4.5%); and manufacturing (2.9%). Over half of the incidents (53.7%) affected entities classified as essential under the NIS2 (Network and Information Security) Directive.*
- Threat objectives:
  - Hacktivism dominates incident volume in the EU, with ideology driving 79.4% of recorded incidents.
  - Financially-motivated operations (13.4% of recorded incidents) were primarily carried out by cybercriminal operators (e.g., emptying bank accounts).
  - Cyberespionage campaigns accounted for 7.2% of recorded incidents (e.g., spyware for surveillance purposes).
- Tactics and techniques:
  - Phishing (60%) and vulnerability exploitation (21.3%) were the two leading intrusion access points.
  - Denial of Service ("DDoS") attacks were the most common incident type, accounting for 77% of all reported cases, primarily launched by hacktivist groups, with cybercriminals representing only a small share; and
  - Mobile devices (with Android devices facing a higher level of threat) and Internet-exposed services and devices remain high value targets across all types of threats.

The Report also indicates that, artificial intelligence has become both:

- An enabler of cyber threats: Notably, by early 2025, Large Language Models (LLMs) were estimated to automate more than 80% of phishing and social engineering campaigns, amplifying the scale and sophistication of attacks (e.g., by devising more persuasive phishing emails); and
- A target of cyber threats: The AI supply chain is a target for exploitation, for example, through poisoned hosted machine learning (ML) models and exploiting vulnerabilities of the infrastructure that AI systems rely upon to operate.

Outlook. The Report emphasizes how Europe's digital resilience is being tested by the combined effects of hacktivism and the malicious use of emerging technologies.

Defensive strategies must focus on proactive threat hunting, behavioral detection, and the integration of cyber risk management into broader operational and policy frameworks. Collaboration between private industry and EU and Member State institutions remains essential for countering cyber threats.

* *Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union. Compared to NIS1, the NIS2 Directive introduces several new sectors, including waste water, space, public*

	administration, ICT service management (business-to-business), postal and courier services, and waste management, among others — bringing the total to 18 sectors across essential and important entities.
EU Data Act becomes applicable (see here)	On 12 September 2025, most rules under the EU Data Act became applicable (*Regulation (EU) 2023/2854 on harmonized rules on fair access to and use of data).** The Data Act, in force since 11 January 2024, establishes rules on the fair access to and use of personal and non-personal data across all sectors of the economy. It covers data generated by products connected to the internet (e.g., vehicles, smart watches, and TVs) and related services. The Data Act applies regardless of where the entities controlling or providing access to the data (data holders) are established (*see also Jones Day Commentary "EU Releases Data Act to Facilitate Access and Use of Data", January 2024).* In brief, the EU Data Act: • Introduces rules on business-to-business and business-to-consumer access to data. In particular, manufacturers and service providers must: – Design products and provide services in such a manner that generated data are directly accessible to users; and – Provide information to users on generated data, its accessibility, and users' rights. • Prohibits use of unfair contractual terms on data sharing, setting out a list of terms deemed as unfair (e.g., a term enabling the party that unilaterally imposed the term to terminate the contract at unreasonably short notice). These measures seek to prevent abuse of contractual imbalances in data sharing contracts due to unfair terms imposed by a party with significantly stronger bargaining position. • Provides for a harmonized framework for the access and use of data held by the private sector, by public sector bodies, the EU Commission, the European Central Bank, and EU bodies; • Introduces restrictions to non-EU governmental access and international transfers of non-personal data, by requiring providers of data processing services to take technical, organizational and legal measures to prevent unlawful access and transfers; • Facilitates switching between cloud and other data processing providers, with costs arising from the switching process to be charged to the customers only until 12 January 2027; • Sets out interoperability requirements for participants in data spaces that offer data or data services, data processing service providers, and vendors of applications using smart contracts; and • Requires EU Member States to define penalties for violations of the Data Act, and EU data protection authorities may impose administrative fines as provided in the EU General Data Protection Regulation (GDPR) for certain infringements of the Data Act. On the same day, the European Commission also published (i) the latest Frequently Asked Questions (FAQs) on the Data Act (see here); and (ii) Guidance on the sharing of vehicle data under the Data Act, which is intended to improve repair and maintenance, car sharing, and mobility as a service (see here). This Guidance only concerns the automotive sector,

	including original equipment manufacturers (OEMs), suppliers, aftermarket service providers, and insurance providers. Next steps. The European Commission is developing additional tools to support implementation of the EU Data Act, including, in particular: - a dedicated legal helpdesk to offer companies direct guidance on applying the new rules; - guidance on protecting trade secrets; - model contractual terms for data sharing; and - standard clauses for cloud contracts to ease data exchange. ** The Data Act's obligation to make product data and related service data accessible to the user will become applicable on 12 September 2026. The rules on unfair contractual terms shall apply (i) from 12 September 2025 to contracts concluded after 12 September 2025, and (ii) from 12 September 2027 for contracts concluded on or before 12 September 2025, provided that they are (a) of indefinite duration or (b) set to expire at least 10 years from 11 January 2024.*
EU AI Act - Recent developments	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*). Recent developments. Since our previous update (*see Jones Day EU Geopolitical Risk Update No. 122 of 30 September 2025*), new developments on the EU AI Act notably include: ▪ Draft Guidance on serious AI incidents. On 26 September 2025, the EU Commission published draft Guidance (see here), including a reporting template for serious AI incidents under the EU AI Act, in view of helping providers of high-risk AI systems to detect risks early, ensure accountability, and align with international reporting frameworks. On the same day, the EU Commission launched a public consultation (see here) on the draft Guidance, which ran until 7 November 2025. The AI Office will publish a summary of the results of the consultation. ▪ Draft Code of Practice on transparent generative AI systems. The EU Commission held a public consultation (see here) on a proposed Code of Practice for transparent generative AI systems, which ran until 9 October 2025. The draft Code would require providers and deployers to clearly inform users when they are interacting with AI or AI-generated content, in view of promoting transparency and trust in AI applications. The drafting process is expected to take approximately 10 months, with plans to finalize the Code ahead of the transparency obligations under the AI Act that take effect on 2 August 2026. * *Regulation (EU) 2024/1689 laying down harmonized rules on artificial intelligence*.

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),* ***Margo Cornette*** *(Associate),* ***Cecelia Kye*** *(Consultant), and* ***Justine Naessens*** *(Associate) in the Brussels Office contributed to this Update.*