EU GEOPOLITICAL RISK UPDATE KEY POLICY & REGULATORY DEVELOPMENTS

No. 119 | 31 December 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

- European Commission publishes call for evidence and public consultation on Public Procurement Directives
- European Commission approves €1.3 billion Italian State aid measure to support semiconductor advanced packaging facility
- European Commission approves €81 million Spanish State aid measure to support production of semiconductor-grade synthetic diamonds
- 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

- Council of the European Union expands sanctions against Russia, Belarus, and Iran
- European Commission hosts Minerals Security Partnership to advance critical raw materials projects

Medicines and Medical Devices

- European Commission signs second HERA Invest agreement for €20 million against antimicrobial resistance
- EMA launches European Shortages Monitoring Platform

Cybersecurity, Privacy & Data Protection

- ENISA publishes first biennial Report on the State of Cybersecurity in the EU

- New EU Product Liability Directive enters into force
- Cyber Resilience Act enters into force

COMPETITION & STATE AID

Competition

European Commission publishes call for evidence and public consultation on Public Procurement Directives (see here)

On 13 December 2024, the Commission published a call for evidence and a public consultation on the planned revision of the Public Procurement Directives that regulate public procurement in the EU.*

Backdrop / objectives. The Commission indicates that some 250,000 public authorities in the EU spend around 14% of EU GDP (over €2.4 trillion per year) on purchasing services, works and supplies. Public authorities are the principal buyers in various sectors (e.g., energy, transport, waste management, the provision of health services).

Last reformed in 2014, the Public Procurement Directives have sought to ensure transparency and integrity in public spending and strengthen competition in the EU for the provision of public goods and services with respect to higher-value public tenders (with monetary values exceeding certain thresholds)** and which are presumed to be of cross-border interest.

However, according to the European Court of Auditor's Special Report 28/2023 on public procurement in the EU: "*Our analysis of the data available [i.e. 2011-2021] indicates a significant increase in single bidding overall, a high level of direct contract awards in most member states and a limited level of direct cross-border procurement between member states. As several objectives of the 2014 reform remain unattained, we conclude that, the entry into force of the 2014 directives has had no demonstrable effect*." (*see also ECA Dashboard on data set used to prepare Special Report 28/2023*).

The Commission's planned revision of the Public Procurement Directives, as set out in its Political Guidelines 2024-2029 issued by Commission President Ursula von der Leyen, seeks to:

- enable giving preference to European products for certain strategic sectors in public procurement;
- ensure EU security of supply for vital technologies, products and services; and
- modernize and simplify EU public procurement rules, in particular for EU start-ups and innovators.

The Commission's plan to give preference to European products in certain strategic sectors has already raised the concerns of, *inter alia,* U.S. companies active in Europe.

Consultation. The consultation aims at collecting quality evidence providing information, data and feedback on how the Public Procurement Directives have performed. It also seeks to assess whether these Directives still suffice to address current challenges and to achieve EU policy objectives (e.g., promoting a greener and more innovative European economy).

Next steps. Interested parties can contribute to the call for evidence and public consultation until 7 March 2025. The Commission will consider these contributions in its evaluation of the Public Procurement Directives.

Within eight weeks of the close of the public consultation, the Commission will publish a factual summary report, as well as a report summarizing the

	results of the consultation activities that will be annexed to the evaluation staff working document. * *These Public Procurement Directives comprise: (i) Directive 2014/24/EU on public procurement; (ii) Directive 2014/25/EU on procurement by entities operating in the water, energy, transport and postal services sectors (Utilities Directive); and (iii) Directive 2014/23/EU on the award of concession contracts* ** *For example, for the above-referred Utilities Directive 2014/25/EU, the thresholds include, e.g., for works contracts (€5,538,000) and certain service contracts, all design contests, all supplies contracts (€443 000).*
State Aid	
European Commission approves €1.3 billion Italian State aid measure to support semiconductor advanced packaging facility (see here)	On 18 December 2024, the Commission announced the approval of a €1.3 billion Italian State aid measure to support Silicon Box in constructing a semiconductor advanced packaging* and testing facility in Novara, Italy. The aid will consist of an approximately €1.3 billion direct grant to Silicon Box to support its investment worth €3.2 billion in total. The Commission's assessment was based on Article 107(3)(c) TFEU (which enables Member States to grant aid to facilitate the development of certain economic activities subject to certain conditions) and on the principles set out in the European Chips Act, which entered into force on 21 September 2023 (*Regulation (EU) 2023/1781 of 13 September 2023 establishing a framework of measures for strengthening Europe's semiconductor ecosystem*). To recall, the Chips Act is part of the Commission's package of measures released in February 2022 (see here) aimed at ensuring the EU's security of supply and technological leadership in the field of semiconductors. (Micro-) chips or semiconductors are key building blocks for digital products, e.g., smartphones, computers, and medical equipment *(see also Jones Day EU Emergency Response Update No. 107 of 29 September 2023).* A key pillar within the Chips Act is a framework to ensure security of supply, which seeks to spur public-private investments in manufacturing facilities for chipmakers and their suppliers. In particular, "first-of-a-kind" facilities, including those producing equipment used in semiconductor manufacturing, are expected to reinforce the EU's supply security. *State aid.* In light of steep barriers to entry and the capital intensity of the chips sector, the Commission notes that private investment in chips manufacturing facilities may likely require public support. In this respect, the Commission may consider approving State aid to such facilities under Article 107(3)(c) TFEU, weighing relevant positive effects such as the following: – The chips facility is "first-of-a-kind" in Europe (as defined in the Chips Act), such that an equivalent facility does not already exist in Europe; – The public support covers a maximum of 100% of a proven funding gap, i.e., the minimum amount needed to ensure that such investments occur in Europe; and – The chips facility would enhance security of supply for European businesses using chips in their products, e.g., where such facility accepts to satisfy EU "priority-rated" orders (as provided in the Chips Act) such as orders from entities from critical sectors whose activities are disrupted or at risk of disruption due to chip shortages.

	In the present case, according to the Commission's assessment, the State aid measure to Silicon Box will reinforce Europe's security of supply, resilience, and technological autonomy in semiconductor technologies. In particular, the Silicon Box facility: – is first-of-a-kind in Europe, as there is currently no comparable advanced packaging facility for the specific technological features; and – contributes to security of supply in Europe (e.g., by committing to comply with priority-rated orders to produce in Europe in case of a supply crisis and by helping to halt overreliance on packaging services offered outside of Europe). This State aid measure is the Commission's fifth approval based on such principles set out in the Chips Act (e.g., on 5 October 2022, the Commission approved an Italian measure to support STMicroelectronics in constructing an SiC wafer plant in Sicily (*see Jones Day COVID-19 Update No. 89 of 14 October 2022*); and on 27 April 2023, the Commission approved a €2.9 billion French aid measure to support STMicroelectronics and GlobalFoundries in constructing a new microchips manufacturing facility in Crolles, France (see *Jones Day EU Emergency Response Update No. 102 of 3 May 2023*). Looking ahead. The Silicon Box plant is anticipated to reach full operating capacity in 2033. The non-confidential version of the decision will be made available under the case number SA.113264 in the State aid register on the Commission's competition website once confidentiality issues are resolved. * *Advanced packaging allows for the integration of multiple chips (often with different functions) into one package, creating a "chiplet" (multi-chip module) that functions like a single chip to enhance performance and power efficiency.*
European Commission approves €81 million Spanish State aid measure to support production of semiconductor-grade synthetic diamonds (see here)	On 16 December 2024, the Commission approved an €81 million Spanish State aid measure to support Diamond Foundry Europe in building its first factory in Europe (in Trujillo, Spain) to produce semiconductor-grade rough synthetic diamonds. The aid will consist of a direct grant of €81 million to Diamond Foundry to support its investment totaling some €675 million. The Commission assessed the measure under EU State aid rules, and in particular Article 107(3)(a) TFEU (which allows aid 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 notably contribute to the EU's strategic objectives relating to the green transition of the regional economy, regional development, and job creation. The new factory is designed to be carbon-neutral, powered through fully renewable energy generated by a solar photovoltaic plant. Using Diamond Foundry's plasma reactor technology, the plant will produce rough synthetic diamond wafers, which the semiconductor industry can use as an alternative to other resources, such as silicon. The project aims at responding to demand in key sectors, such as 5G networks and electric vehicles.

	Looking ahead. The plant's anticipated capacity is approximately 4 to 5 million carats annually. The non-confidential version of the decision will be made available under the case number SA.106799 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.*
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 31 December 2024): – €9.7 billion Italian scheme to support electricity production from renewable energy sources to foster the transition towards a net-zero economy. – €167 million Italian scheme to support the primary agricultural production sector in the context of Russia's war against Ukraine. – €400 million Finnish scheme to help companies decarbonise their production processes and to support investments in strategic sectors, to foster the transition towards a net-zero economy. – €32.5 million Irish scheme to support tillage and horticulture producers in the context of Russia's war against Ukraine. – €2.6 billion Estonian State aid scheme to support renewable offshore wind energy to foster the transition to a net-zero economy. – €590 million (BGN 1.15 billion) Bulgarian scheme to support investments in electricity storage facilities to foster the transition towards a net-zero economy.
TRADE / EXPORT CONTROLS	
Council of the European Union expands sanctions against Russia, Belarus, and Iran (see here, here, and 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; bans 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 16 December 2024, the Council adopted a 15th package of sanctions,* focusing on measures such as:

- Anti-circumvention, e.g.:
  - Targeting an additional 52 vessels from Russia's shadow fleet (now covering a total of 79 vessels), subjecting these to a port access ban and ban on provision of services These non-EU vessels are used to circumvent the EU oil price cap mechanism, support Russia's energy sector, transport military equipment for Russia, or transport stolen Ukrainian grain.
- Export restrictions, e.g.:
  - Adding 32 new companies to the list of those supporting Russia's military and industrial complex in its war against Ukraine (including 20 Russian firms, as well as others from Serbia, Iran, India, United Arab Emirates, and those under Chinese/Hong Kong jurisdiction).

    The targeted companies have been involved in circumventing trade restrictions or have engaged in the procurement of sensitive items used for Russian military operations, like UAVs and missiles. These companies will be subject to stricter export restrictions with respect to dual-use goods/technology and advanced technology items.
- Shielding European companies, e.g.:
  - The exceptional extension of divestment derogations,** which are necessary to allow EU operators to exit as rapidly as possible from the Russian market. The extended derogations will be granted on a case-by-case-basis by Member States and focus on enabling an orderly divestment process, which would be jeopardized without the extension of these deadlines.
  - Prohibiting the recognition or enforcement in the EU of rulings issued by Russian courts based on the Russian Federation Arbitration Procedure Code (Article 248). This prohibition will better protect European companies from litigation with Russian parties, since Russian court rulings under this Article 248 have prevented parties from initiating or continuing a proceeding in a jurisdiction other than Russia, which contravenes established international principles and practices, and often leads to disproportionately high financial penalties for European companies. The new measure prevents the execution in Europe of such penalties against EU operators.

The Council also added a total of 84 additional listings (54 individuals and 30 entities) responsible for actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine. In particular, these target the following:

- Russian defence companies (e.g., manufacturing aircraft parts, drones, electronics, engines, high-tech components for weapons);
- Shipping companies responsible for the sea transport of crude oil and oil products, which generate significant revenues for the Russian government; and
- Various Chinese actors, notably those supplying drone components and microelectronic components in support of Russia's war against Ukraine, are subjected for the first time to full-fledged sanctions

(asset freeze, prohibition to make economic resources available, travel ban).

Altogether, EU restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine now apply to nearly 2,400 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 14th package of sanctions was adopted by the Council on 24 June 2024 (*see also Jones Day EU Emergency Response Update No. 115 of 24 June 2024*).

* *An in-depth analysis of the 15th package of sanctions against Russia is available from the authors of the EU Emergency Update (see contact details below for Nadiya Nychay (Brussels) and Rick van 't Hullenaar (Amsterdam)).*

** *EU operators divesting from the Russian market remain bound by prohibitions on (i) importing goods subject to an import prohibition from Russia into the EU; and (ii) selling, transferring or supplying prohibited goods to a Russian buyer, as set out in Council Regulation 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine. Temporary derogations from certain of such prohibitions were introduced in Regulation 833/2014 (Art. 12b) to facilitate an expeditious exit from the Russian market (see also FAQs on divestment from Russia concerning sanctions adopted following Russia's military aggression against Ukraine, as last updated on 17 December 2024).*

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

- Belarus. On 16 December 2024, the Council imposed restrictive measures on an additional 2 entities and 26 individuals from Belarus. This includes individuals (e.g., business owners, part-owners, members of boards of directors) who have benefitted from the Lukashenka regime, including those whose companies have been awarded privileges by the regime and contributed to circumventing EU sanctions.

  Since August 2020, the EU has imposed several successive rounds of individual and sectoral sanctions in the context of Belarus' involvement in Russia's war against Ukraine and those responsible for internal repression and human rights violations in Belarus.

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

- Iran. On 18 November 2024, the Council widened the EU framework for restrictive measures in view of Iran's military support to Russia's war against Ukraine and to armed groups and entities in the Middle East and Red Sea region. In particular, the Council introduced:

  – A ban on the export, transfer, supply, or sale from the EU to Iran of components used to develop and produce missiles and UAVs.

  – A ban on any transaction with ports and locks that are owned, operated or controlled by listed individuals / entities, or are used for the transfer to Russia of Iranian UAVs (Unmanned Aerial Vehicles) or missiles or related technology and components.

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

European Commission hosts Minerals Security Partnership to advance critical raw materials projects (see here)

On 12 December 2024, the European Commission hosted key meetings of the Minerals Security Partnership (MSP),* alongside its co-chairs the Republic of Korea and the U.S., to discuss raw materials projects.

Backdrop. The MSP, launched in June 2022, is part of the EU's multilateral efforts aimed at addressing market imbalances on global raw materials markets. In particular, the MSP seeks to propel policies and projects to ensure secure and sustainable access to critical raw materials (CRMs), such as cobalt, copper, graphite, lithium, nickel, manganese, and rare earths.

In this respect, the MSP enables its members to share information on CRM developments in third countries, target investment opportunities, and co-invest in mining, refining and recycling projects that align with high environmental, social and governance (ESG) standards.

Additionally, the MSP Forum,** launched in April 2024, serves as a new platform for cooperation in the area of CRMs essential to the global green and digital transitions, bringing together resource-rich countries and countries with high demand for such resources. (*see also Jones Day EU Emergency Response Update No. 116 of 26 August 2024*).

The MSP meetings comprised the following:

- The MSP Principals' meeting focused on accelerating projects related to rare earths, a group of 17 specialty metals essential to the permanent magnets required for various high-tech applications (e.g., wind turbines, hard disk drives, electric vehicles, smartphones). Europe produces none of these rare earth elements, leading to significant dependencies, with Chinese imports meeting 98% of Europe's total rare earth magnet demand.

  The meeting discussed MSP projects in rare earths, including the HyProMag Project (UK) and the newly registered Arafura Nolans Project (Australia). MSP partner countries continue to identify new opportunities for responsible mining, processing, and recycling of critical minerals among MSP Forum members.

- The MSF Forum hosted the first in a series of workshops on public-private investment in critical minerals. This first workshop, led by the European Commission, addressed key issues such as challenges facing investors (e.g., de-risking the investment climate to facilitate investment) and government policies aimed at increasing development of the CRM sector.

These MSP meetings took place within the context of Raw Materials Week 2024 in Brussels, the largest policy event on raw materials. Held by the European Commission since 2016, the event gathers some 1,000 participants from industry, administration, civil society, research, and academia.

The MSP Forum next met on 4 February 2025 in the margin of the annual Mining Indaba event in Cape Town, South Africa, which focuses on developing mining interests in Africa.

* *The MSP consists of 15 partners (Australia, Canada, Estonia, Finland, France, Germany, India, Italy, Japan, Norway, the Republic of Korea, Sweden, the UK, the U.S., and the EU).*

** *The above-referred 15 MSP partners are also part of the MSP Forum, alongside 15 new MSP Forum members (Argentina, Democratic Republic of the Congo, Dominican Republic, Ecuador, Greenland, Kazakhstan, Mexico, Namibia, Peru, the Philippines, Serbia, Turkey, Ukraine, Uzbekistan, and Zambia).*

MEDICINES AND MEDICAL DEVICES

European Commission signs second HERA Invest agreement for €20 million against antimicrobial resistance (see here)

On 9 December 2024, the European Commission's Health Emergency Preparedness and Response Authority ("HERA") signed its second agreement under HERA Invest, the first EU financing mechanism to focus on advancing research and development of medical countermeasures and related technologies to tackle priority cross-border health threats (see here).*

This second HERA invest agreement, signed with the Danish biotech company SNIPR Biome, aims at advancing cutting-edge therapies against antimicrobial resistance ("AMR"), one of the most pressing global health threats. Through HERA Invest, the Commission and the European Investment Bank (EIB) will provide €20 million in venture debt financing to SNIPR Biome.

In particular, SNIPR Biome's CRISPR technology employs gene-editing to identify and remove harmful bacteria as a groundbreaking way to address infections resistant to conventional antibiotics (e.g., through a product designed to prevent bloodstream infections caused by E. coli).

In announcing the agreement, Hadja Lahbib, European Commissioner for Equality, Preparedness and Crisis Management, stated:

> "*Antimicrobial resistance is a silent pandemic. In the EU alone, 35,000 people die every year because of it, and resistant infections place a significant burden on our healthcare systems. Today's HERA Invest agreement is an important milestone and shows the importance of European companies' innovation in fighting this major health threat. HERA Invest is ensuring that Europe remains at the forefront of medical breakthroughs.*"

The Commission further noted that United Nation's projections anticipate that, if left unaddressed, the number of deaths attributable to AMR could rise to 10 million annually by 2050, with 390,000 of those deaths occurring in the EU/EEA.

* *In the first HERA Invest agreement (signed on 7 October 2024) HERA committed €20 million, in collaboration with the European Investment Bank, to support the French biopharmaceutical company Fabentech in developing and deploying broad-spectrum therapeutics aimed at combating biological threats to public health (see here).*

EMA launches European Shortages Monitoring Platform (see here)

On 28 November 2024, the European Medicines Agency ("EMA") announced the launch of the first version of the European Shortages Monitoring Platform ("ESMP", see here),* offering core functionalities to allow marketing authorization holders ("MAHs") to submit data to routinely report shortages of centrally authorized medicines.

The ESMP's launch is a major milestone in the effort to tackle medicine shortages and to ensure the availability of medicines. By centralizing and automating data collection on medicine shortages, this notably:

- affords regulatory authorities with access to real-time, comprehensive information to improve the prevention, monitoring, and management of medicine shortages across the European Union ("EU") and the European Economic Area ("EEA"); and

- enhances communications between the EMA, national competent authorities ("NCAs"), and industry stakeholders to ensure medicine availability for patients during public health emergencies and major events.

Following the ESMP's first version release, on 29 January 2025, ESMP's full version became available. As of 2 February 2025, MAHs must use ESMP to report data in these scenarios:

- In normal circumstances, MAHs must routinely report data on shortages of centrally authorized medicinal products**;
- During preparedness actions, led by EMA's Executive Steering Group on Shortages and Safety of Medicinal Products ("MSSG"), MAHs must provide data on centrally and nationally authorized medicinal products, as requested by the MSSG; and
- During a crisis, MAHs must report data on centrally and nationally authorized medicines which are part of a list of critical medicines created for that specific crisis.

The ESMP will also facilitate access to publicly available information on shortages of individual medicines in EMA's shortages and national shortages catalogues (available here).

** The ESMP is a deliverable of EMA's extended mandate under Regulation (EU) 2022/123 on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical device (available here).*

*** A centrally authorized medicine has a single marketing authorization issued by the European Commission and valid across the EU.*

**** A nationally authorized medicine is authorized in a Member State in accordance with its national authorization procedure.*

CYBERSECURITY, PRIVACY & DATA PROTECTION

ENISA publishes first biennial Report on the State of Cybersecurity in the EU (see here)

On 3 December 2024, the European Agency for Cybersecurity (ENISA) published its first biennial Report on the State of Cybersecurity in the EU, as mandated by the NIS 2 Directive (Article 18).*

The Report, drafted in conjunction with the NIS Cooperation Group and the European Commission, covers the period from January 2023 to July 2024.

It seeks to provide policymakers at EU level with an evidence-based overview** of the current cybersecurity landscape and capabilities in the EU. It also offers recommendations on enhancing the overall level of cybersecurity across the EU and addressing identified gaps.

The Report's main findings notably highlight:

- The cyber threat level to the EU is substantial. This indicates a high likelihood that entities are either directly targeted by threat actors or vulnerable to breaches through recently discovered vulnerabilities. In particular, the most reported forms of attack were Denial-of-Service attacks (DoS/DDoS/RDoS) and ransomware attacks (accounting for over half of all events observed), followed by threats against data;

	• Vulnerabilities in supply chains remain a significant risk, calling for enhanced EU-wide coordinated risk assessments. While Member States' cybersecurity strategies are overall aligned, only half of the Member States include the cybersecurity of supply chains in their strategies; • High criticality sectors (e.g., telecommunications, electricity, and finance) have the highest level of cybersecurity maturity, given strong regulatory frameworks, effective supervisory authority, and advanced risk management; • Moderate to high criticality sectors (e.g., healthcare, railways) face challenges due to reliance on outdated operational technology systems, which are difficult or even impossible to upgrade in order to implement cybersecurity measures; and • Member State participation in cybersecurity exercises is high at the EU-level, but is not always matched by structured national exercises, which may weaken the EU's overall capacity to deal with a cybersecurity crisis. Among the Report's policy recommendations, these address: • Strengthening the technical and financial support given to EU-level and national competent authorities, as well as to entities falling within the scope of the NIS 2 Directive, to ensure harmonized, comprehensive, and timely implementation of the evolving EU cybersecurity policy framework using existing EU structures; • Addressing supply chain security by stepping up EU-wide coordinated risk assessments and developing an EU policy framework for public and private sector supply chains; and • Enhancing the understanding of sectoral specificities and needs and improving the level of cybersecurity maturity in sectors covered by the NIS 2 Directive. Conclusions / next steps. The Report concludes that the maturity of the EU cybersecurity policy framework has reached a considerable level and that next steps should focus in particular on supporting private and public sector entities with implementing EU Member State legislation, with the support of the European Commission and ENISA. The Report also warns that emerging technologies like AI and quantum computing are growing threats (for example, AI is increasingly used in phishing and misinformation campaigns), requiring advanced risk management, including well-tested operational cooperation and raising common awareness. * *Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union. The implementation deadline for this Directive by the EU Member States was 17 October 2024.* ** *The analysis conducted is based on various sources, including the EU Cybersecurity Index, NIS Investment Report series, the Foresight 2030 and the ENISA Threat Landscape Report.*
New EU Product Liability Directive enters into force (see here)	The new EU Product Liability Directive ("PLD") entered into force on 8 December 2024.* Member States now have until 9 December 2026 to transpose the PLD into national legislation (*see also Jones Day*

Commentary "Radical Changes to Europe's Product Liability Rules Adopted" of 27 November 2024).

The PLD aims at modernizing the previous EU framework on manufacturers' liability for defective products** and enhancing the protection of injured persons. In this respect, the PLD introduces key revisions and notably:

- Broadens its scope of application to include all products placed on the EU market, regardless of their type. In particular, the PLD will now apply to all types of software, including applications, operating systems, and AI systems. As a result, manufacturers may be held liable for any defect that existed at the time their software or AI system was released, including defects that become apparent after the new release of such products due to updates;
- Identifies various circumstances in which a product is considered defective, including cases where the product does not provide the safety that a person is entitled to expect or that is required by law. For instance, the PLD specifies that a product is considered defective if it fails to meet critical cybersecurity requirements, thereby making manufacturers liable for intentional damage caused by third parties (hackers);
- Extends the right to compensation for natural persons to new types of damage. For instance, the PLD explicitly covers damage resulting from the destruction or corruption of data, provided that such data is not used for professional purposes;
- Extends liability to importers, for instance, such that an EU-based business may be held liable for damages caused by products manufactured outside the EU*;*
- Shifts the burden of proof to defendants in certain cases, such that plaintiffs could have European courts order the disclosure of evidence based on a claim being "plausible." Moreover, in certain circumstances, plaintiffs will not need to prove a defect, but may instead rely on a presumption, whereby a plaintiff need only show that a defect was "likely." (s*ee also Jones Day Commentary, "Reversal of Burden of Proof Under Proposal for a New EU Product Liability Directive" (7 November 2023*) *for further details)*; and
- The addition of a 25-year statute of limitations in the case of personal injury symptoms that are slow to emerge.

For reasons of legal certainty, the PLD will apply to products placed on the market or put into a service as of 9 December 2026. However, for products placed on the market before that date, the previous Directive on product liability will apply.

* *Directive (EU) 2024/2853 of 23 October 2024 on liability for defective products*

** *Directive (EEC) 85/374 of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products*

Cyber Resilience Act enters into force (see here)	The EU Cyber Resilience Act ("CRA") entered into force on 10 December 2024* (*see also Jones Day Commentary "EU Enacts Broad Cybersecurity Requirements for Hardware and Software Products" of 23 October 2024*). The CRA, a first-of-its-kind law, imposes a broad range of cybersecurity requirements on economic operators** providing hardware and software products with digital elements placed on the EU market. It aims at strengthening the cybersecurity of digital products by addressing inadequate cybersecurity in many products and lack of timely security updates for products and software. The CRA also introduces new requirements to better enable consumers and businesses to select and use cybersecure products. In a nutshell, the CRA: • Imposes five major categories of obligations on manufacturers (i.e., conformity assessments, product documentation, customer support, cybersecurity risk assessment, and vulnerability reporting); • Imposes requirements on importers (e.g., ensuring that manufacturers have met their obligations under the CRA, such as appropriate conformity assessment); • Imposes requirements on distributors (e.g., ensuring that the product bears a CE marking and that the manufacturer and importer have complied with certain obligations under the CRA); • Classifies products with digital components into three distinct categories: "default", "important", and "critical", in view of adapting security measures based on the level of risk and potential impact that each product category presents; • Introduces penalties for non-compliance of up to €15 million or 2.5% of global annual turnover; and • Complements existing EU cybersecurity frameworks, e.g., the NIS 2 Directive.*** Most obligations under the CRA will apply from 11 December 2027. However, certain provisions will apply at an earlier stage (e.g., manufacturers' reporting obligations (CRA, Article 14) will apply from 11 September 2026). * *Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements.* ** *Under the CRA (Article 3.12), "economic operator" includes, in particular, the manufacturer, authorized representative, importer, and distributor.* *** *Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union.*

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.*