EU GEOPOLITICAL RISK UPDATE KEY POLICY & REGULATORY DEVELOPMENTS

No. 127 | 21 June 2026

This regular alert covers key policy and regulatory developments related to EU geopolitical risks, including in particular, economic security, Russia's war against Ukraine, the Middle East crisis, 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 2025 Report on Competition Policy
- European Commission publishes Middle East Crisis Temporary State Aid Framework
- European Commission approves schemes under Clean Industrial Deal State Aid Framework (CISAF)
- European Commission publishes Guidelines on closure of Recovery and Resilience Facility

Trade / Export Controls

- Adoption of regulation revising EU framework for screening foreign direct investments (FDI)
- Council of the European Union discusses and extends sanctions against Russia and Iran
- Internal Market Emergency and Resilience Act (IMERA) becomes applicable and European Commission holds first IMERA Board meeting

Medicines and Medical Devices

- Political agreement reached on proposed Critical Medicines Act
- Updated Frequently Asked Questions on the European Health Data Space
- European Commission announces global health commitments at One Health Summit

Cybersecurity, Privacy & Data Protection

- European Commission presents new Tech Sovereignty Package
- ENISA releases updated framework to assess national cybersecurity maturity
- EDPB publishes draft guidelines on the processing of personal data for scientific research purposes

- EU AI Act – Recent developments

COMPETITION & STATE AID

European Commission publishes 2025 Report on Competition Policy (see here)

On 5 May 2026, the Commission published the 2025 Report on Competition Policy, setting out main legislative initiatives, policy developments, and enforcement actions in the competition field. The Report opens by highlighting the challenges and deep uncertainties the EU claims to face, driven by what it describes as sudden geopolitical shifts, significant technology shifts, and climate change.

The Report, in particular, sets out the Commission's stated efforts to protect competition and the innovative capacity of EU companies, while contributing to EU resilience and meeting the objectives of the green and digital transitions through initiatives such as the following:

- The Commission adopted the Clean Industrial Deal State Aid Framework (CISAF) in June 2025, designed to facilitate the EU's clean transition in view of making the EU a key global player in state-of-the-art clean technologies, while avoiding fragmenting the Single Market.

  CISAF sets out to simplify the State aid rules across targeted areas (e.g., roll-out of clean energy and low-carbon fuels; temporary electricity price relief for energy-intensive users; decarbonization of existing production facilities; development of clean tech manufacturing capacity in the EU; measures to stimulate demand for clean technology products; and de-risking of investments related to the objectives of the Commission's Clean Industrial Deal of February 2025).

  By end-2025, the Commission had adopted eight decisions approving nine national measures notified by five Member States with a total amount of €18.4 billion (e.g., authorizing France to invest €11 billion to accelerate the use of renewable energy; and approving national schemes totalling €6.7 billion toward building sufficient manufacturing capacity in clean technologies).

- The Foreign Subsidies Regulation of December 2022 is stated as having contributed to countering anti-competitive and market-distortive activities by firms active in the EU that receive subsidies from outside the EU. In 2025, the Commission consulted stakeholders on the then-draft FSR Guidelines, on improving predictability and transparency for companies by clarifying key concepts, such as how the Commission concludes whether a foreign subsidy has caused a distortion of competition and when a transaction that falls below the FSR's mandatory filing thresholds should be called in (subsequently, on 9 January 2026, the Commission published FSR Guidelines (*see Jones Day EU Geopolitical Update No. 126 of 19 March 2026).*

  On FSR enforcement in 2025, the Commission notably made ADNOC's offered commitments legally binding in its acquisition of Covestro; conducted one unannounced inspection under the FSR at the premises of a company active in the e-commerce sector; and continued work on its preliminary review in the wind energy sector.

- The Commission's other enforcement activities in 2025 also notably included cartels, with a settlement involving fines of €329 million for Delivery Hero and Glovo in online food and grocery deliveries and €72 million in a cartel decision for three automotive starter battery manufacturers and the trade association Eurobat.

	The accompanying Staff Working Document provides a comprehensive account of policy developments and enforcement, including by sector, in the competition field. The Commission also released an infographic, which traces the year's key competition developments.
European Commission publishes Middle East Crisis Temporary State Aid Framework (see here)	On 5 May 2026, the Commission published its Communication on a Middle East Crisis Temporary State Aid Framework (METSAF) to enable targeted support to the EU economy in response to the impact of the Middle East crisis. The METSAF seeks to allow Member States to act swiftly to shield the most exposed companies in key sectors by providing for, e.g.: – Aid based on actual consumption in agriculture, fishery, land transport, and intra-EU short sea shipping, enabling Member States to compensate up to 70% of a beneficiary's extra costs due to the price increase of fuel and fertilizer caused by the crisis. – A simplified approach for small amounts of aid, allowing Member States to calibrate individual aid amounts on elements such as the size and type of beneficiaries' activities, a general estimate of fuel consumption in the sector (or other relevant proxies), with each beneficiary able to receive up to €50,000. – For eligible energy-intensive industries, a temporary adjustment to the Clean Industrial Deal State Aid Framework (CISAF, as also discussed above / below), allowing further flexibility and higher aid intensities to address electricity price spikes. Aid intensity can increase from 50% to up to 70% for the electricity cost of eligible consumption. Measures under the METSAF must be notified to the Commission, and the framework aims to allow for a rapid approval process. Among the most recently approved State aid schemes under the METSAF (up to 21 June 2026): – €85 million Irish State aid for agricultural companies facing increased fuel prices due to the Middle East crisis. – €8 million Croatian State aid for fishing companies facing increased fuel prices due to the Middle East crisis. – €25 million Spanish State aid for fishing companies facing increased fuel prices due to the Middle East crisis. – €54 million Spanish State aid for agricultural companies facing increased fuel prices due to the Middle East crisis. – €500 million Spanish State aid for agricultural companies facing increased fertilizer prices due to the Middle East crisis. – €15 million French State aid for agricultural and aquaculture companies facing increased fuel prices due to the Middle East crisis. – €13 million French State aid for fishing companies facing increased fuel prices due to the Middle East crisis.

	Looking ahead. The METSAF will be in place until 31 December 2026, and the Commission will keep the content, scope and duration under review in the light of developments in the Middle East and in the general economic situation. Additionally, in responding to the Middle East crisis, Member States can continue relying on specific State aid rules applicable to sectors covered by the METSAF, e.g., for agriculture, Guidelines for State aid in the agricultural and forestry sectors and in rural areas; for fishery, Guidelines for State aid in the fishery and aquaculture sector; for road and maritime transport, Guidelines on State aid to maritime transport.
European Commission approves schemes under Clean Industrial Deal State Aid Framework (CISAF) (see here)	The Commission approved additional measures under the Clean Industrial Deal State Aid Framework (CISAF) of 25 June 2025 (*see also Jones Day EU Geopolitical Update No. 122 of 31 August 2025*). The CISAF is a key component of the Commission's Clean Industrial Deal: A joint roadmap for competitiveness and decarbonization of 26 February 2025, which aims to support the EU manufacturing industry's competitiveness and resilience, while accelerating decarbonization. The CISAF replaced the Temporary Crisis and Transition Framework (TCTF)* and sets out streamlined rules aimed at the simplified and swifter approval of priority State aid measures that seek to accelerate Europe's competitiveness and green transition goals (e.g., accelerating renewable energy rollout; facilitating industrial decarbonization and energy-efficiency projects; ensuring sufficient EU manufacturing capacity for net-zero technologies; and easing private investment risk). Additionally, the METSAF regime (above-referred) provides that for eligible energy-intensive industries, a temporary adjustment to CISAF allows further flexibility and higher aid intensities to address electricity price spikes. Among the most recently approved State aid schemes under the CISAF and deemed in line with the objectives of the Clean Industrial Deal (up to 21 June 2026): – €1 billion Slovak State aid scheme to support clean technology (cleantech) manufacturing capacity. – €10 million Austrian scheme to support cleantech manufacturing capacity. – €23 billion Italian State aid scheme to support renewable electricity production. – €100 million Austrian State aid scheme to support cleantech manufacturing capacity. – €300 million Irish scheme to support the production of renewable heat. – €380 million French scheme to support cleantech manufacturing capacity. – €334 million State aid scheme in Bulgaria Germany and Slovenia to provide temporary electricity price relief for energy-intensive companies

	– €3.8 billion State aid scheme in Germany to provide temporary electricity price relief for energy-intensive companies – €90 million State aid scheme in Slovenia to provide temporary electricity price relief for energy-intensive companies – €3.7 billion Czech State aid scheme for sustainable biomethane production. – €500 million Luxembourgish scheme to support strategic investments that add (cleantech manufacturing capacity. – €50 million scheme set up by the Spanish region of Catalonia to support manufacturing capacity in line with the Clean Industrial Deal objectives. – €5 billion Danish State aid scheme to support offshore wind energy. Looking ahead. The CISAF, applicable since 25 June 2025, will remain in force until 31 December 2030. * *The TCTF was established in 2022 to support the EU economy in the context of Russia's invasion of Ukraine and in sectors key to accelerating the green transition and reducing fuel dependencies*. *From 2022 to 2024, €103.18 billion was disbursed under measures addressing the Russian invasion of Ukraine (see European Commission State Aid Scoreboard 2025, covering data up to 31 December 2024, published on 15 January 2026).*
European Commission publishes Guidelines on closure of Recovery and Resilience Facility (see here)	On 30 April 2026, the Commission published Guidelines for Member States on operational aspects related to the final phase and closure of the Recovery and Resilience Facility (RRF),* the cornerstone of the unprecedented €723.8 billion NextGenerationEU package created in December 2020 to support Europe's pandemic recovery and strengthen Member State's long-term resilience, economic growth and competitiveness. Backdrop. Access to RRF funding is conditional on Member States implementing agreed reforms and investments from their Recovery and Resilience Plans. The final deadline for meeting milestones and targets is 31 August 2026, as provided in the RRF Regulation. On 5 May 2026, the Commission disbursed a combined total of €5.85 (€4.6 billion to Germany and €1.25 billion Slovakia) under the RRF, bringing the total RRF funds disbursed across the EU to over €400 billion (see here). The Commission indicated that this "landmark figure" reflected the RRF's signficant role in driving reforms and investments to ramp up Europe's energy independence, the green and digital transitions, and long-term resilience and competitiveness. Key features. The Guidelines set out, in particular: – Further technical guidance to Member States on the operational handling of final payment requests in view of applicable deadlines. – Addressing cases where milestones and targets have not been satisfactorily fulfilled or where reversals – when a milestone or target

is initially deemed fulfilled but is subsequently found to be unmet – may occur in the RRF's final phase.

- Details on certain post-2026 obligations, including reporting, monitoring, control, audit, and data retention, to ensure continued protection of the EU's financial interests. While the RRF's funding phase will conclude in 2026, Member States must maintain robust oversight to ensure accountability and compliance with EU financial rules.

Next steps. Member States need to submit final payment requests under the RRF by September 2026, and all payments by the Commission must be executed 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.**

* *RRF Regulation (EU) 2021/2411 establishing the RRF entered into force in February 2021 and was amended twice by (i) Regulation (EU) 2023/435 incorporating REPowerEU objectives; and (ii) Regulation (EU) 2024/795 establishing the Strategic Technologies for Europe Platform ('STEP')*

* *See also the Fourth Annual Report on the Implementation of the RRF of October 2025 (Jones Day EU Geopolitical Risk Update No. 123 of 8 October 2025).*

TRADE / EXPORT CONTROLS

Adoption of regulation revising EU framework for screening foreign direct investments (FDI) (see here)

On 8 June 2026, the Council of the European Union adopted a regulation revising the EU foreign direct investment (FDI) screening framework under FDI Regulation 2019/452, which had become fully applicable in October 2020.

Background. To recall, the EU FDI framework addresses concerns over foreign investors seeking to invest in European firms implicating technologies, infrastructure, inputs, or sensitive information critical for more than one EU Member State or on a project of EU interest. It also covers greenfield investments, which typically involve the creation of a new company or establishment of facilities.

The EU FDI framework is intended to identify risks related to investments in strategic assets that could threaten security or public order. It also established a cooperation framework between the Commission and EU Member States for the exchange of information and for raising concerns in notified cases from the Member States that have screening mechanisms.

This cooperation framework between Commission and the Member States underpins Member States' FDI assessments and facilitates a Member State's ultimate decision where the FDI is planned or completed.

Amended rules. The revised regulation will replace the existing FDI screening framework, towards ensuring a more coordinated and effective approach across the EU to safeguard security and public order.

The amended rules will require all EU Member States to establish screening mechanisms covering a common minimum scope of sensitive sectors, technologies and infrastructure, e.g.:

	– dual-use items and military equipment, – critical raw materials, – artificial intelligence, – energy, – transport; and – digital infrastructure. The revised regulation, furthermore, is intended to reinforce cooperation between Member States and the European Commission; improve transparency and consistency across national screening systems; and streamline procedures for investors and public authorities. It also introduces new tools to ease information exchange and impede circumvention of the rules. Looking ahead. The revised regulation will be published in the Official Journal and enter into force 20 days after publication. The new rules will start applying 18 months after entry into force.
Council of the European Union discusses and extends sanctions against Russia and Iran	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: • On 21 June 2026, Commission President Ursula von der Leyen issued a statement on the **forthcoming 21st sanctions package against Russia** (see here). She indicated that this package focuses on the most impactful sectors, including energy, financial services and crypto, and trade. In this respect, the package would, for instance: – For the first time, target vessels that assist the shadow fleet, by providing bunkering and other services, for example; and restrict the sale of LNG tankers to Russia (as is already the case for oil tankers). – For the first time, introduce the possibility of a full third-country ban for crypto-asset services; and expand transaction bans to 31 more Russian banks; and – Impose new export restrictions on items and technologies used by Russia's military industry (e.g., for drones, ground support equipment, and jamming and launch systems); and new import bans on a number of goods worth €60 million, covering certain metals, metal ores, and car parts.

- Address one of the last major unsanctioned sectors: fisheries (e.g., substantial restrictions on imports on some fish products, and a total ban on others, including cod).

- On 15 June 2026, the Council adopted a set of **restrictive measures to combat Russia's war of aggression against Ukraine** (see here), with additional listings consisting of 34 individuals and 47 entities in total, in particular with respect to:
  - Supporting Russia's military and industrial complex and its enablers in third countries (e.g., manufacturers and suppliers of drones and other military equipment to the Russian armed forces);
  - The shipment and export of crude oil or petroleum products from Russia, including through Russia's shadow fleet, a tool devised to circumvent EU sanctions; and
  - Direct malicious activities against the EU, its Member States and third countries (e.g., spreading disinformation aimed at justifying, promoting or legitimizing Russia's war against Ukraine).

- The Council adopted a **20th package of restrictive measures** on 23 April 2026 (see here), comprising 120 further individual listings (the largest package of listings in two years) and economic sanctions targeting key sectors that sustain Russia's war against Ukraine, and notably:
  - Further constricting Russia's energy revenues, e.g.:
    - Foreseeing a future prohibition on transporting Russian oil and petroleum products, in full coordination with the G7. The Council will decide when such maritime services ban is to enter into force, considering an appropriate wind-down period.
    - A new prohibition on maintenance services for Russian LNG tankers and icebreakers. .
  - Intensifying financial sector measures , e.g.:
    - Extending the transaction ban to four banks in Kyrgyzstan, Laos, and Azerbaijan that assist the Russian war effort by significantly frustrating sanctions or connecting to the Russian System for Transfer of Financial Messages, the Russian banking messaging network.
    - A total sectorial ban on carrying out exchanges with any Russian crypto-asset service provider as well as any decentralized platforms enabling crypto trading because of their use in circumvention.
  - New export and imports restrictions and bans, e.g.:
    - New export bans to Russia on goods, such as rubber and tractors, worth over €365 million.
    - New import bans on metals, chemicals and minerals, not yet under sanctions, worth over €530 million.
    - New restriction on provision of cybersecurity services to Russia.

Altogether, EU restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine now apply to some 2,700 individuals and entities, who were targeted in response to Russia's ongoing unjustified military aggression against Ukraine. The current restrictive measures include travel restrictions for natural persons,

	the freezing of assets, and a ban on making funds or other economic resources available to the listed 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) and up to the present 20th package of sanctions.* * *An in-depth analysis of the 20th 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)).* **Iran:** Among recent developments: • On 22 May 2026, the Council broadened the scope of EU's restrictive measures originally established to address Iran's military support for Russia's war against Ukraine and various armed groups in the Middle East and the Red Sea region (see here). The modified sanctions framework now also targets individuals and entities involved in Iran's actions threatening the freedom of navigation in the Middle East. Iran's actions against vessels transiting through the Strait of Hormuz are contrary to international law and infringe upon established rights of transit through international straits. The EU may now introduce additional restrictive measures in response to Iran's actions undermining the freedom of navigation in the Strait of Hormuz (e.g., travel restrictions to prohibit listed individual and entities from entering or transiting through EU territories and asset freezing). Furthermore, EU citizens and companies are prohibited from making funds, financial assets or economic resources available to the listed individual and entities. • On 8 June 2026, the Council approved restrictive measures against two individuals and one entity (see here) under the above-referred extended legal framework targeting those involved in Iran's actions and policies threatening the freedom of navigation in the Middle East. These actions are contrary to international law and infringe upon established rights of transit through international straits. With these latest listings, restrictive measures under the amended sanctions framework now apply to 26 natural and legal persons and 27 entities from a range of countries. The Council's overview of EU sanctions against Iran for its military support of Russia's war against Ukraine (since 2023) is also available here.
Internal Market Emergency and Resilience Act (IMERA) becomes applicable and	On recent developments concerning the EU Internal Market Emergency and Resilience Act (IMERA)*: (i) On 29 May 2026, IMERA became applicable.

European Commission holds first IMERA Board meeting (see here and here)

To recall, IMERA aims at ensuring the free movement of persons, goods and services, as well as greater transparency and coordination, in times of crisis. These goals are notably to safeguard the stability of supply chains for critical goods and services. IMERA builds on lessons learned during recent emergencies such as COVID-19, Russia's war against Ukraine, and the energy supply crisis.

IMERA framework. Complementing other EU legislative measures for crisis management, IMERA sets out a crisis management framework to identify threats to the internal market and to preserve its smooth functioning, in particular by:

- Establishing an Internal Market Emergency and Resilience Board, a crisis governance mechanism chaired by the European Commission and composed of Member State representatives to monitor the internal market, identify different levels of risk, and coordinate appropriate responses. This crisis governance provides for a three-tier approach:
  - Contingency mode enables the Commission to undertake measures to prepare for possible crises (e.g., cooperation and exchange of information with Member States; consultation with economic operators on their initiatives to mitigate/respond to potential internal market crises; and training and stress tests for Member States);
  - Vigilance mode can be activated to address the threat of a crisis with the potential to escalate into an internal market emergency that disrupts the free movement of goods and services or disrupts supply chains. Vigilance mode measures include, e.g., Member State monitoring of supply chains of strategically important goods and services, as well as establishing and maintaining a confidential inventory in these areas; and
  - Emergency mode is to be activated in the event of a crisis of significant impact on the internal market that severely disrupts free movement or the functioning of critical supply chains. Emergency mode measures include, e.g., a blacklist of prohibited restrictions such that Member States cannot impose measures such as banning the transit of crisis-relevant goods.

    Additionally, and only when the emergency mode has already been activated, the Commission may also make use of last-resort measures under extraordinary circumstances, e.g., the Commission may issue requests to economic operators established in the EU to accept priority-rated orders to produce or supply crisis-relevant products. Economic operators remain free to refuse such requests.
- IMERA also provides for a stakeholder platform to facilitate sector-specific dialogue and partnerships by gathering key stakeholders from industry, researchers and civil society (e.g., to indicate voluntary actions needed to successfully respond to an internal market emergency and to provide scientific advice, opinions or reports on crisis-related issues).

(ii) On 4 June 2026, the Commission held the first formal IMERA Board meeting, convening Member States and other stakeholders to discuss risks facing the internal market, supply chain resilience (notably, the supply chain

implications of the evolving Middle East situation, particularly in vital sectors such as fertilizers and aluminium), and preparedness for future crises.

During this Board meeting, industry representatives from key impacted sectors shared their views. The Commission noted that companies are the first to identify and face supply shocks, emphasizing IMERA's central need for public-private cooperation.

The Commission provides further details on IMERA (here) and in a factsheet for companies (here).

* *Regulation 2024/2747 of 9 October 2024 establishing a framework of measures related to an internal market emergency and to the resilience of the internal market and amending Council Regulation (EC) No 2679/98 (Internal Market Emergency and Resilience Act)*

Additionally, IMERA is accompanied by a package of measures (so-called "IMERA omnibus," see below) concerning current legislation in areas related to the internal market (e.g., General Product Safety Regulation), which require amendments setting out emergency response procedures:

Regulation (EU) 2024/2748 and Directive (EU) 2024/2749, both of 9 October 2024, which amend harmonized EU product legislation to ensure that strategic goods can be rapidly brought to the market to address shortages in case of a market crisis.

MEDICINES AND MEDICAL DEVICES

Political agreement reached on proposed Critical Medicines Act (see here)

On 11 May 2026, the European Parliament and the Council of the EU reached a political agreement on the proposed Regulation on Critical Medicines ("Critical Medicines Act" or "CMA"), which the Commission released in March 2025 (see here).

Key elements of the agreed proposed CMA include, among other things:

- **Supply chain diversification and EU preference in public procurement.** Member States will be required to diversify and incentivize resilience in medicine supply chains during public procurement procedures. For critical medicines, procurers must support the diversification and reliability of supply sources -- in cases of high dependency on a single or limited number of third countries, the proposed CMA goes further, foreseeing an obligation for contracting authorities to favor manufacturing within the EU.
- **Facilitating Strategic Projects**. The creation of Strategic Projects (i.e., to boost, increase, or modernize EU manufacturing capacity for critical medicines or their active substances) will be facilitated through easier access to Member State and EU funding, as well as fast-tracked administrative support. Projects for manufacturing of orphan medicines will also benefit from faster permitting procedures.
- **Contingency stocks safeguards and solidarity**. Where Member States require companies to hold contingency stocks, they will have to ensure that such requirements do not negatively affect the supply of critical medicines in other Member States. In this respect, any contingency stock requirements should be transparent and adhere to the principles of solidarity and proportionality.

	• **Enabling collaborative procurement**. Member States may join forces when procuring critical medicines, orphan medicines, and other medicines of common interest, thereby bolstering their collective leverage and addressing availability and access disparities with respect to such medicines. • **Strategic partnerships.** The Commission will explore strategic partnerships with international partners to broaden the supply chain and reduce dependencies on single or limited numbers of suppliers. The CMA is proposed in the context of the European Health Union and complements the ongoing reform of EU pharmaceutical legislation (see "Pharma Package") (*see also* *Jones Day Commentary "The EU Pharma Package Is a Done Deal: a Holiday Gift, or Not?"* of December 2025). The political agreement is now subject to formal endorsement by both the Council and the European Parliament.
Updated Frequently Asked Questions on the European Health Data Space (see here)	On 26 March 2026, the European Commission updated its set of "Frequently Asked Questions on the European Health Data Space" ("FAQs"), which was first published in March 2025. The COVID-19 pandemic highlighted the imperative of timely access to quality electronic health data (both for health threats preparedness and response and for secondary use) to contribute to more effective management of future pandemics and ultimately helping to save more lives. Against this backdrop, the European Union adopted the European Health Data Space ("EHDS") Regulation (EU) 2025/327, which entered into force on 26 March 2025 (*see also* *Jones Day Vital Signs: Digital Health Law Update, Spring 2025*). The EHDS is the first sector-specific common EU data space. Its core objectives are three-fold: (1) empowering individuals to access, control, and share their personal electronic health data across borders for healthcare delivery ("primary use"); (2) enabling the secure and trustworthy reuse of health data for research, innovation, policymaking, and regulatory activities ("secondary use"); and (3) fostering a single market for electronic health record ("EHR") systems through harmonized interoperability, security, and certification requirements. One year after the EHDS Regulation entered into force, the Commission's updated FAQs address practical questions that emerged during the first year of the transition period. Among the most significant new and revised questions are the following: • **Medical devices, IVDs, and high-risk AI systems**: Manufacturers of medical devices, in vitro diagnostic ("IVD") medical devices, and high-risk AI systems that claim interoperability with EHR systems must comply with the essential requirements in Annex II of the EHDS Regulation (interoperability and logging software components), though they are not required to use the European digital testing environment reserved for EHR system manufacturers. The FAQs also note that the

MDR ("Medical Device Regulation") and IVDR are currently undergoing a targeted revision, meaning the relevant cross-references in the EHDS may need to be adapted in due course.

- **Cyber Resilience Act**:The FAQs address the interplay between the EHDS and the Cyber Resilience Act, which is relevant for manufacturers of EHR systems that also qualify as products with digital elements.

The updated FAQs also add important guidance on secondary use and other cross-cutting topics:

- **Future data extractions under data permits**: Only public sector bodies and EU institutions may obtain permits providing for recurring access to future data, while all other data users must apply for a new permit each time. This is particularly relevant for pharma and medtech companies conducting longitudinal real-world evidence studies or post-market surveillance.

- **Right to lodge complaints and contest HDAB decisions**: Both natural and legal persons, including corporate data holders and data users, may challenge decisions of Health Data Access Bodies ("HDABs") by way of complaints concerning opt-out rights being transmitted to the relevant Data Protection Authority.

- **Definition of an EHR system**: The Commission now provides more granular examples of what qualifies as an EHR system, which is critical for manufacturers assessing whether their products fall within scope.

- **Territorial scope and data holder obligations**: The FAQs clarify the conditions under which non-EU-based entities, such as sponsors of clinical trials conducted in the EU, may be subject to health data holder obligations under the EHDS Regulation.

The updated FAQs serve as an early but authoritative signal of how the Commission interprets the EHDS Regulation's interplay with existing regulatory frameworks, including the GDPR, the MDR, the IVDR, the AI Act, and the Cyber Resilience Act.

Looking ahead. The EHDS Regulation's key provisions on primary and secondary use and on EHR systems will apply from 26 March 2029. Other provisions, including those on governance, will apply by 26 March 2027. The Commission is currently working on various implementing acts, which should be adopted by March 2027.

Companies should use the updated guidance to begin mapping their data holdings, assessing whether their products qualify as EHR systems or claim interoperability with them, and preparing for the new data-permit regime.

European Commission announces global health commitments at One Health Summit (see here)	On 7 April 2026, at the One Health Summit, the European Commission announced a series of major global health commitments totaling nearly €800 million. The centerpiece is the Commission's planned €700 million pledge to the eighth replenishment of the Global Fund – the worldwide partnership working to defeat HIV, tuberculosis, and malaria. The Commission, together with the EU Member States ("Team Europe") has committed a total of more than €3

billion to the Global Fund's eighth replenishment, reinforcing Europe's position as one of the Fund's strongest supporters since its creation in 2002.

Alongside the Global Fund pledge, the Commission announced its additional initiatives:

- €46.5 million in new programs to strengthen One Health cooperation between Europe and Africa, with a particular focus on combating antimicrobial resistance (AMR).
- €50 million in research and development, comprising (i) €30 million for new antibiotics and AMR countermeasures; and (ii) €20 million for the development of dengue treatments in anticipation of growing vector-borne disease risks driven by climate change.

These initiatives fall within the scope of the EU's forthcoming Global Health Resilience Initiative, which had been expected to launch before the summer of 2026 (see here).

CYBERSECURITY, PRIVACY & DATA PROTECTION

European Commission presents new Tech Sovereignty Package (see here)

On 3 June 2026, the European Commission presented the Tech Sovereignty Package ("Package"), as set out in its Communication on European Tech Sovereignty, accompanied by an EU Open Source Strategy.

The Package introduces significant measures across semiconductors, cloud, AI, open source, and data centers that will reshape the regulatory landscape for technology companies operating in Europe (*see* also *Jones Day Alert, EU Proposes Tech Sovereignty Package with Major Implications for Digital Markets*, June 2026).

The Package comprises four interconnected initiatives:

- The proposed Chips Act 2.0 would introduce new measures aimed at strengthening the European semiconductor ecosystem, reducing strategic dependencies, and supporting advanced semiconductor production within the EU. The proposal is structured around four key objectives:
  - Improving conditions for investment and competitiveness by strengthening research, innovation, and skills development, accelerating permitting procedures, and supporting strategically important technologies, including AI chips, through dedicated "Grand Challenges."
  - Stimulating demand and industrial uptake, notably by strengthening links between chips manufacturers and demand from user industries, and by establishing "Demand Accelerators" to ensure that new semiconductor products align with industry needs and reach the market more rapidly.
  - Reinforcing supply-side measures, in particular by enabling State aid funding for "First-of-a-Kind" projects that are not yet present in the EU.
  - Increasing resilience and reducing dependencies through measures such as a new Business-to-Business Semiconductor

Supply Chain Platform, designed to facilitate information sharing and proactive risk management across the semiconductor chain.

- The proposed Cloud and AI Development Act ("CADA") would introduce a harmonized EU-wide sovereignty framework for cloud services based on four assurance levels, subject to certain requirements as follows:
  - Level 1: data processing and storage must occur within an EU infrastructure.
  - Level 2: demonstrated independence from third countries and transparency over the software supply chain.
  - Level 3: mandatory EU ownership and control, with additional citizenship criteria for personnel, although the Commission can recognize third-country providers.
  - Level 4: full transparency and control over the software supply chain, with no interference from a third country.

  Under the proposal, for instance, cloud providers seeking to offer services to the public sector would (subject to limited exceptions) be required to meet at least Level 1 requirements. Member States would also be permitted, based on risk assessments, to require higher assurance levels for specific cases.

  The proposal also seeks to triple EU data center capacity within five to seven years by requiring Member States to designate at least one "acceleration zone," where data center projects would benefit from streamlined permitting procedures (see also *Jones Day Commentary, European Commission's Proposed Cloud Sovereignty Framework Creates New Compliance Tiers for Software Providers*, June 2026).
- The EU Open Source Strategy identifies open source software as a key enabler of European tech sovereignty. Backed by €2 billion in funding over seven years, the Strategy adopts a full lifecycle approach encompassing research and development, market deployment, long-term maintenance, and governance of critical open source technologies. The Strategy outlines several measures to strengthen the European open source ecosystem, including:
  - Promoting the adoption of open source solutions in strategic EU initiatives, including the EU Digital Identity ecosystem.
  - Strengthening cooperation with Member States, notably through the European Digital Infrastructure Consortium for Digital Commons, to develop, adapt, and scale secure open source solutions for public services.
  - Encouraging public administrations to act as anchor users, through procurement guidance and open-source-friendly tendering practices.
- The Strategic Roadmap for Digitalisation and AI in Energy addresses the growing energy demands of digital infrastructure. It envisages, in particular:
  - Developing an EU model for tripartite agreements (between data center operators, energy stakeholders, and public authorities), in view of setting out potential actions for signatory parties to facilitate the sustainable integration of data centres in the energy system and support the twin green and digital EU transition. .

	– A proposed pan-European AI model for power grid management (see also, *Jones Day Commentary, EU Data Center Rules Combine Expansion Incentives with New Energy Obligations*, June 2026). Looking ahead. The Package's legislative proposals for the Chips Act 2.0 and CADA will now be examined by the European Parliament and the Council of the European Union. Significant changes may be made during the legislative process, and final adoption is likely to take between 18 and 24 months, given the breadth of the proposals.
ENISA releases updated framework to assess national cybersecurity maturity (see here)	On 22 April 2026, the European Union Agency for Cybersecurity (ENISA) issued the revised National Capabilities Assessment Framework (NCAF 2.0). Aims / backdrop. The NCAF 2.0 sets out the methodology designed to support national authorities in strengthening their cybersecurity capabilities and assessing the maturity of national cybersecurity strategy implementation. Its revision is accompanied by an online tool that enables policymakers to identify gaps, set priorities, and promote evidence-based decision-making. Updating the original 2020 framework, NCAF 2.0 reflects the evolving threat landscape and advancements in EU legislation, most notably the NIS 2 Directive.* To recall, the NIS 2 Directive aims to ensure a high common level of cybersecurity across the EU. To this end, Article 7 requires EU Member States to adopt a national cybersecurity strategy that sets out strategic objectives, the resources needed to achieve them, and appropriate policy and regulatory measures. Such strategies must include, among other elements, policies addressing supply chain security, vulnerability management, and cybersecurity education and awareness. NCAF 2.0 provides a structured self-assessment methodology allowing Member States to evaluate the maturity of their national cybersecurity capabilities across 20 strategic objectives (e.g., strengthening cyber-resilience and cyber hygiene of the private sector (including SMEs), addressing cybercrime, developing cyber crisis management frameworks, and protecting critical sectors). These strategic objectives are organized under four thematic clusters, addressing a Member State's abilities with respect to: – Capacity building and awareness, e.g., raising awareness of cybersecurity risks and threats, strengthening cyber-resilience and cyber hygiene, enhancing incident preparedness and response, and promoting advancements in cybersecurity research and innovation. – Cooperation and collaboration, e.g., ensuring a sufficient level of cooperation and information sharing among stakeholders at national and international levels, including mutual assistance mechanisms, as well as the capacity to prevent, detect, and respond to cybercriminal activities. – Cybersecurity governance, e.g., establishing effective governance structures and promoting sound practices in the cybersecurity domain. – Regulatory and policy frameworks, e.g., developing and implementing regulatory and policy instruments to enhance supply

	chain security, facilitate coordinated vulnerability disclosure, promote active cyber protection, and safeguard critical information infrastructure. The NCAF 2.0 framework seeks to enable national authorities to identify strengths, weaknesses, and priority areas, and to monitor progress at both strategic and operational levels. * *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union*
EDPB publishes draft guidelines on the processing of personal data for scientific research purposes (see here)	On 15 April 2026, the European Data Protection Board* (EDPB) published the draft Guidelines 1/2026 on processing of personal data for scientific research purposes for public consultation. Objective / backdrop. The draft Guidelines aim to provide greater clarity and a more consistent application of the General Data Protection Regulation (GDPR) across the EU in the research context, particularly given fragmented national approaches. The GDPR applies to the processing of personal data for scientific research purposes, while also providing specific provisions designed to facilitate such research. The draft Guidelines reflect a continuation and consolidation of the EDPB's earlier Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, which were developed in response to the pandemic. More broadly, the draft Guidelines should be understood in the context of crisis preparedness – by establishing a clear and consistent framework for the processing of personal data in scientific research, they aim to ensure that researchers and controllers across the EU are better equipped to facilitate responsible data-driven research when future public health or other risks arise. Key clarifications. The draft Guidelines introduce important clarifications in several areas, e.g.: – Concept of scientific research. The EDPB stresses that only research that is genuinely scientific should benefit from the GDPR's research-related provisions. To support this assessment, it proposes six indicative criteria (such as adherence to ethical standards, as well as verifiability and transparency) that should be considered when determining whether an activity qualifies as scientific research. Where these criteria are met, the activity may be presumed to constitute scientific research. – Further processing and storage limitation. The EDPB confirms that further processing of personal data for scientific research purposes is presumed to be compatible with the original purpose for which the data were collected, without the need to carry out a separate compatibility assessment. In addition, personal data may be stored for longer periods where they are processed for scientific research purposes, even if the initial purposes have been fulfilled, provided that appropriate safeguards are in place. – Consent as a legal basis. The EDPB acknowledges that consent may serve as an appropriate legal basis for scientific research. It accepts the use of "broad consent" whereby data subjects may consent to the processing of their personal data for future research projects within

certain areas of scientific research where the specific purposes are not fully defined at the time of collection.

- Appropriate safeguards. The EDPB emphasizes that, pursuant to Article 89(1) GDPR, controllers must implement appropriate safeguards to protect the rights and freedoms of data subjects when processing personal data for scientific research purposes (e.g., use of anonymized data where possible (or, alternatively, pseudonymized data), independent or ethical oversight, secure processing environments, privacy-enhancing technologies, measures to protect the publication of research results, and confidentiality arrangements).

Next steps. Following the public consultation for the draft Guidelines (until 25 June 2026), the EDPB will review feedback received and finalize and publish the Guidelines. It has not specified the timeline for adoption of the final version.

** The EDPB is an independent EU body established under Article 68 GDPR. Its primary role is to ensure the consistent application of data protection rules across the EU by issuing guidelines, opinions, and binding decisions on cross-border data protection matters, thereby promoting cooperation among national supervisory authorities.*

EU AI Act - Recent developments

The EU AI Act* 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*, *February 2025*).

Recent developments. Since our previous update (*see Jones Day EU Geopolitical Risk Update No. 126 of 19 March 2026*), new developments on the EU AI Act notably include:

- On 10 June 2026, the European Commission published the final version of the Code of Practice on marking and labelling AI-generated content (see also, *Jones Day Commentary, European Commission Publishes Draft Code of Practice on AI Labelling and Transparency*, January 2026). While adherence to the Code remains voluntary, providers** and deployers*** that choose to sign it may rely on the specific measures set out therein to demonstrate compliance with the specific transparency obligations under Article 50 EU AI Act on detecting and labelling AI-generated content, deep fakes****, and certain AI-generated text intended for public dissemination. The Code is accompanied by new EU icons that deployers of generative AI systems may use to label their AI-generated content.
- On 17 May 2026, the Commission issued draft guidelines on the classification of high-risk AI systems (see also *Jones Day Commentary, Draft EU Guidelines Clarify When AI Systems Are High-Risk Under the AI Act*, June 2026). The draft guidelines set out the Commission's interpretation of key concepts relevant to classifying high-risk AI systems and provide practical examples of when AI systems should be considered high-risk. The draft guidelines are presented in three main sections:
  - General principles for the classification of AI systems.
  - Classification of high-risk AI systems embedded in or constituting “regulated products.”

- Classification of high-risk AI systems falling within the high-risk use cases of Annex III of the AI Act.

- On 8 May 2026, the Commission published draft guidelines on the implementation of the transparency obligations for certain AI systems under Article 50 of the AI Act. The draft guidelines are intended to provide practical guidance to competent authorities, as well as providers and deployers of AI systems, in order to support the consistent and effective application of the EU AI Act's transparency requirements. The draft guidelines complement the Code of Practice on the marking and labelling of AI-generated content by addressing the full range of transparency obligations set out in Article 50 EU AI Act (rather than focusing solely on marking and labelling requirements relating to AI-generated content), including the obligations applicable to AI systems that interact directly with natural persons, emotion recognition systems, and biometric categorization systems.

- On 7 May 2026, the Council of the European Union and the European Parliament reached a provisional agreement on the proposed Digital Omnibus on AI. On 16 June 2026, the European Parliament approved the provisional agreement.

  The proposed Digital Omnibus on AI aims to streamline certain elements of the EU AI Act and to postpone compliance deadlines for high-risk AI systems (see also *Jones Day Commentary, EU Digital Omnibus: How EU Data, Cyber, and AI Rules Will Shift*, December 2025). Under the proposal, AI systems classified as high-risk in sensitive areas such as employment and law enforcement (Annex III) would need to comply by 2 December 2027 (instead of currently 2 August 2026). Hsigh-risk AI systems embedded in products governed by sector-specific legislation, such as medical devices (Annex I), would face a later deadline of 2 August 2028 (instead of currently 2 August 2027).

  The provisional agreement confirmed these postponements and introduced several additional amendments to the EU AI Act, such as:

  - Prohibiting the use of AI to generate non-consensual sexual and intimate content or child sexual abuse material.
  - Introducing a grace period for providers of AI systems generating synthetic audio, image, video, or text content, where such AI systems were placed on the market before 2 August 2026. The new deadline for compliance with the transparency obligations is set at 2 December 2026.
  - Extending certain regulatory exemptions, currently granted to SMEs, to small mid-cap enterprises (i.e., enterprises with fewer than 750 employees and up to €150 million in turnover or €129 million in assets).

  Next steps. The provisional agreement must now be formally endorsed by the Council of the EU before being submitted to a legal-linguistic revision with a view to the formal adoption of the legislative act by the co-legislators in the coming weeks. The agreement is particularly timely for providers and deployers of high-risk AI systems in sensitive areas (Annex III), for which the original 2 August 2026 compliance deadline is fast approaching.

  * *Regulation (EU) 2024/1689 laying down harmonized rules on artificial intelligence (entered into force on 1 August 2024).*

*** "Providers" are defined by the EU AI Act as natural or legal persons, public authorities, agencies, or other bodies that develop an AI system or a general purpose AI model or that have an AI system or a general-purpose AI model developed and place it on the market or put the AI system into service under their own name or trademark, whether for payment or free of charge.*

**** "Deployers" are defined by the EU AI Act as natural or legal persons, public authorities, agencies, or other bodies using an AI system under their authority except where the AI system is used in the course of a personal non-professional activity.*

***** "Deep fakes" are defined by the EU AI Act as AI-generated or manipulated image, audio, or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful.*

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),* ***Justine Naessens*** *(Associate), and* ***Olivier Verhasselt*** *(Associate) in the Brussels Office contributed to this Update.*