



EU GEOPOLITICAL RISK UPDATE KEY POLICY & REGULATORY DEVELOPMENTS

No. 128 | 22 September 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, Middle East conflict, health threats, and cyber threats. It does not purport to provide an exhaustive overview of developments.

This regular update expands from the previous EU Emergency Response Update (last issue [No. 115](#)), and COVID-19 Key EU Developments (last issue [No. 99](#)).

LATEST KEY DEVELOPMENTS

Competition & State Aid

- European Commission approves €400 million German State aid to enhance insulin supply resilience
- European Commission publishes first review of Foreign Subsidies Regulation
- Recovery and Resilience Facility reaches implementation deadline
- European Commission approves schemes under Middle East Crisis Temporary State Aid Framework (METSAF)
- European Commission approves schemes under Clean Industrial Deal State Aid Framework (CISAF)

Trade / Export Controls

- New landmark European Union Customs Code enters into force
- European Union receives €1.4 billion in revenue from immobilized Russian assets to be used to support Ukraine
- Council of the European Union discusses and extends sanctions against Russia
- EU publishes report on monitoring EU agri-food trade

Medicines and Medical Devices

- European Commission introduces new EU framework to secure Europe's supply of medical radioisotopes
- European Commission launches pilot initiative on medical countermeasure manufacturing and health preparedness
- Updated EU guidance and new eligibility tracker released for joint clinical assessments

Cybersecurity, Privacy & Data Protection

- ENISA publishes Threat Landscape Report 2026
- EU Cyber Resilience Act – Mandatory vulnerability and incident reporting obligations become applicable
- Council of the EU adopts new sanctions in response to Russia's cyberattacks and malicious activities
- European Commission presents EU Action Plan on Cybersecurity and Artificial Intelligence

COMPETITION & STATE AID

European Commission approves €400 million German State aid to enhance insulin supply resilience (see [here](#))

On 8 September 2026, the Commission approved, under EU State aid rules, a €400 million German measure in favor of Sanofi-Aventis Deutschland GmbH ("Sanofi") to strengthen the resilience of the supply of human insulin and insulin analogues ("insulins"). Under the measure, Germany will pay Sanofi a public service compensation to provide a service of general economic interest ("SGEI", i.e., an essential public service such as postal delivery, transportation, or energy).

Backdrop. To recall, the 2012 SGEI Framework of specific State aid rules for SGEIs entered into force (see [here](#)), which set out the conditions for allowing State aid in the form of public service compensation.

In 2025, the Commission amended the 2012 [SGEI Decision](#) (a component of the SGEI Framework) to clarify that Member States can entrust specific public service obligations to operators to enhance the security of supply of critical medicines when market failure is identified and thereby compensate these operators (i) up to €20 million per year without being subject to notification; (ii) over €20 million per year, subject to notification and approval under the SGEI rules.

German measure. Germany's €400 million measure for pharmaceutical manufacturer Sanofi will compensate for the company's net costs for the provision of an SGEI to strengthen the resilience of the supply of insulins for German patients against production and supply bottlenecks (including other manufacturers' decisions to divert production capacity to GLP-1-RA products).. Sanofi's public service obligation includes, in particular:

- building a new insulin factory at its site at Industriepark Frankfurt-Höchst by 31 December 2032;
- ensuring an annual production of at least 1.1 tonnes of insulins at its Frankfurt-Höchst site and stockpiling 1 tonne of insulin active pharmaceutical ingredients until 31 December 2042; and
- prioritizing the European Economic Area (EEA) markets in case of insulins shortages.

According to the Commission's press release, Sanofi would close its insulin active ingredient production on its German site without the State aid. This would weaken the security of supply of insulins in the EEA markets, leaving only one production site in the EEA.

Commission assessment. In assessing the German measure under EU State aid rules (in particular, the SGEI Framework and Article 106(2) Treaty on the Functioning of the EU (TFEU)*), the Commission notably determined that:

- Germany properly considered the public service needs;
- the compensation does not exceed the net costs of the provision of the public service obligation; and
- the entrustment complies with EU public procurement rules.

Next steps. The non-confidential version of the Commission decision will be available under case number SA.115239 in the [State aid register](#) on the Commission's competition website, upon resolving any confidentiality issues.

* Under [Article 106\(2\) TFEU](#), companies that run SGEIs are subject to EU competition rules, except if adhering to such rules prevents the company from doing its essential public service.

European Commission publishes first review of Foreign Subsidies Regulation (see [here](#))

On 14 July 2026, the Commission published its first review of the [Foreign Subsidies Regulation](#) (FSR) of December 2022, covering the first three years of FSR enforcement.

To recall, under the FSR, the Commission can investigate subsidies granted by third countries to companies operating in the EU, in the context of participation in public procurement procedures, concentrations (mergers/acquisitions), or other economic activities taking place in the internal market. The FSR requires mandatory notifications for public tenders and mergers and acquisitions (M&A) above certain thresholds. It has led to a very significant number of filings being made to the Commission, notably in the area of public tenders.

The review is based on an in-depth analysis, including over 100 stakeholder contributions received from two consultations and an independent study conducted by an external party (*for further details on consultation results, see [Jones Day EU Geopolitical Risk Update No. 126 of 19 March 2026](#)*).

According to the Commission's review, the FSR is working well in practice. The Commission's view is that FSR procedures for reviewing M&A transactions and tender bids in public procurement procedures are important to enabling it to identify and address potentially distortive foreign subsidies before an M&A transaction is concluded or a high-value public contract is awarded.

Furthermore, the Commission considers that its "ex officio" powers provide an effective complementary framework to investigate and address potential distortive foreign subsidies in the internal market.

Room for improvement. The review notes certain concerns raised about the FSR's complexity and burdensome requirements, e.g.:

- Administrative burdens in collecting/reporting data on so-called foreign financial contributions (FFC) which could entail subsidies;
- Length and complexity of certain procedures linked to investigations;
- Uncertainty over the Commission's call-in powers for below-threshold M&A transactions; and
- Need for increased clarity regarding certain reporting obligations and greater transparency in enforcement practice.

The Commission indicates that it is examining potential simplification and plans to initiate targeted adjustments to the FSR procedural framework, such as the following:

- Under the chapter for M&A transactions:
 - Increasing the turnover notification threshold;
 - Introducing a simplified notification possibility for specific cases or FFCs;
 - Moderately increasing the reporting thresholds for FFCs; and

- Introducing additional exemptions from reporting requirements for FFCs not categorized as foreign subsidies most likely to distort the internal market.
- Under the public procurement chapter:
 - Simplifying and clarifying the forms used for notifications and declarations;
 - Revising the framework for companies to request waivers to limit information disclosure for certain FFCs; and
 - Clarifying the rights and obligations of companies and the contracting authority, including for processing confidential information, in the context of access to files.

In the Commission's view, these adjustments would ease administrative burdens related to the number of submissions, streamline reporting requirements, and better focus on cases more likely to raise concerns under the FSR.

Several business associations urged the Commission to propose legislative amendments to the FSR so as to ease the burden on companies active in Europe; however, the Commission has declined to come forward with changes to the FSR itself, suggesting it will instead make adjustments in the Commission's implementing rules and guidelines.

Looking ahead. The Commission aims to release draft targeted adjustments in Fall 2026 for stakeholder feedback and to adopt targeted adjustments in 2027 in light of such feedback and additional evidence.

Recovery and Resilience Facility reaches implementation deadline (see [here](#))

On 31 August 2026, the Recovery and Resilience Facility (RRF)* reached a major milestone, marking the final implementation deadline for the reforms and investments presented in Member States' national recovery and resilience plans.

To recall, the RRF is the cornerstone of the unprecedented €723.8 billion [NextGenerationEU](#) package, created in December 2020 to support Europe's pandemic recovery and to respond to geopolitical and energy challenges, towards strengthening Member State's long-term resilience, economic growth and competitiveness.

On reaching this milestone, President of the European Commission, Ursula von der Leyen, remarked:

"NextGenerationEU helped protect our citizens and economies at a time of great uncertainty. It accelerated the clean and digital transitions, cutting Europe's reliance on imported energy. The reforms and the resilience will benefit Europe for generations to come."

Final payment requests. Access to RRF funding is performance-based and thereby conditional on Member States implementing agreed reforms and investments from their national recovery and resilience plans. As of 31 August 2026, €440 billion had been disbursed, with up to a further €133 billion to be paid by end-2026. Notably:

- On 31 August, the Commission approved [Sweden's](#) final payment request of €332.8 million, following its successful completion of 100% of the investments and reforms linked to its recovery and resilience

plan. This final payment brought the total funds paid out to Sweden under the RRF to €3.45 billion.

- On 31 July 2026, [Denmark](#) received its final payment request of €359 million, becoming the first Member State to receive all the grants linked to its RRF plan, for a total €1.63 billion allocation under the RRF.

Next steps. Following the 30 September 2026 deadline for Member States to submit their final payment requests under the RRF, together with all supporting evidence, the Commission will complete all payments by 31 December 2026. No payments will be made in 2027.

For an overview of implementation of the RRF and national recovery plans, see the [RRF Scoreboard](#).

** [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')*

European Commission approves schemes under Middle East Crisis Temporary State Aid Framework (METSAF) (see [here](#))

The Commission approved additional measures under the Middle East Crisis Temporary State Aid Framework ([METSAF](#)) of 5 May 2026 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, below-referred), 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 22 September 2026):

- €52 million Romanian State aid for cattle farmers facing increased fuel and fertiliser prices.
- €30 million Portuguese State aid for agricultural, fishery and aquaculture companies facing increased fuel and fertiliser prices.

- €285 million Italian State aid scheme to support agricultural, fishing and aquaculture companies facing increased fuel and fertiliser prices.
- €4.5 million German State aid scheme for fishing and aquaculture companies facing increased fuel prices.
- €20 million State aid scheme for agricultural and fishing companies in the Italian region of Friuli Venezia Giulia that are facing increased fuel and fertiliser prices.
- €149 million Swedish State aid for agricultural, fishing and aquaculture companies facing increased fuel and fertiliser prices.
- Prolongation and modification of a previously approved Spanish State aid scheme to support road transport companies facing increased fuel prices, with an estimated budget increased to €703 million.
- €300 million Italian State aid scheme to support road transport companies facing increased fuel prices due to the Middle East crisis.
- €74 million Spanish State aid scheme to support maritime transport companies affected by increased fuel prices.
- €54 million Luxembourgish State aid for road and rail transport firms facing increased fuel prices.
- €212 million French State aid scheme to support agricultural and aquaculture companies facing increased fuel prices.

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 CISA allows further flexibility and higher aid intensities to address electricity price spikes.

Among the most recently approved State aid schemes under the CISA and deemed in line with the objectives of the Clean Industrial Deal (up to 22 September 2026):

- €84 million (DKK 629 million) Danish scheme to support clean technology (cleantech) manufacturing capacity.
- €780 million Dutch scheme to support the production of renewable hydrogen.
- €59 million Slovenian State aid scheme to promote battery energy storage systems.
- €300 million Irish State aid scheme for temporary electricity price relief for energy-intensive companies.
- €63 billion French scheme to support offshore wind energy.
- Approval of Czechia's market-wide capacity mechanism to ensure sufficient capacity to produce or store electricity, or to reduce electricity consumption so that production meets demand in the long term. It is the first capacity mechanism approved under the CISA. Aid will be granted through competitive bidding processes.

The capacity mechanism will be financed through consumer charges, with an estimated overall budget ranging from €3.1 billion to €6.2 billion, the exact amount depending on auction outcomes and system needs over time.

Looking ahead. The CISA, 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).

TRADE / EXPORT CONTROLS

New landmark European Union Customs Code enters into force (see [here](#))

On 22 September 2026, the new Union Customs Code entered into force, overhauling the EU customs framework in a landmark reform to provide the EU with a modernized toolbox to facilitate global trade, collect customs duties more efficiently, and tighten controls on non-compliant or unsafe goods. The EU Customs Union manages trade worth over €4.3 trillion, around 14% of global trade.

Crises in recent years have highlighted the “*indisputable need*” for a “*structural modernization*” to make EU customs a strategic capability of the EU, as stated in the [Commission Communication on Customs reform: Taking the Customs Union to the next level](#) of 17 May 2023. In particular, EU customs faces the challenge of the war in Ukraine at the European border, including the implementation of sanctions while supporting humanitarian

efforts. The COVID-19 pandemic also confronted EU customs with a massive increase of traffic of sub-standard and dangerous goods in the health area, from personal protective equipment to medicines and medical devices (see also [EU Emergency Response Update No. 103 of 23 June 2023](#)).

The new EU customs framework notably includes the following:

- Managing rising e-commerce, e.g.:
 - Non-EU e-commerce platforms will be treated as the importer of goods sold into the EU, making them responsible for ensuring that customs formalities and duty payments are handled (rather than the final EU consumer).
 - A new penalty system applies to e-commerce operators that fail to fulfil customs obligations. The most serious cases may incur fines of up to 6% of the company's annual import value in the preceding year, removal of customs privileges and access restrictions to online platforms.
 - An EU-wide handling fee on small parcels will be introduced by 1 November 2026, with the Commission to set the level before Member States apply it. The fee is separate from the removal of the historical customs-duty exemption for imports valued below €150.*
- New EU Customs Authority and Data Hub, e.g.:
 - A new decentralized EU Customs Authority, located in Lille, France, will coordinate governance of the EU Customs Union and will establish priority control areas and risk criteria, as well as coordinate EU-level crisis management for customs.
 - The EU Customs Data Hub will provide a central platform for importers and exporters to interact with customs and will analyze constantly updated import and export data, helping Member States to identify the riskiest cargo for inspection.
- New category of Trust and Check traders, e.g.:
 - The new category of Trust and Check traders will cover transparent businesses that provide comprehensive information on the movement and compliance of their goods and meet other stringent criteria.
 - Trust and Check traders will benefit from simplified customs procedures, and the most reliable companies may release goods into circulation without active customs intervention.

Next steps. Implementation will occur on a rolling basis. Member States will have 12 months to implement the new rules in full.

The EU Customs Authority is expected to initiate operations in 2027. The EU Customs Data Hub will become mandatory for e-commerce consignments as of 1 July 2028 and will expand to all traders as a single mandatory EU customs entry point as from 1 March 2034.

** From 1 July 2026, the EU has applied a temporary €3 customs duty per item on low-value consignments (up to €150) imported from outside the EU, abolishing the previous duty exemption. The €3 temporary customs duty is a flat fee, which will apply until 1 July 2028, after which normal customs duties will apply (for more details, see [here](#)).*

European Union receives €1.4 billion in revenue from immobilized Russian assets to be used to support Ukraine (see [here](#))

On 3 August 2026, the EU received €1.4 billion in windfall profits generated by interest on cash balances originating from immobilized assets of the Central Bank of Russia (CBR) held by Central Securities Depositories (CSDs) in the EU.*

This was the fifth transfer of its kind, covering revenues accumulated during the first half of 2026. The CBR assets themselves remain immobilized under EU sanctions against Russia for its war on Ukraine (*see below item for more details on EU sanctions*). The prohibition on transactions involving those assets and reserves has resulted in cash and deposits accumulating on CSD balance sheets as financial instruments mature, generating significant revenues.**

Allocation of proceeds: Of the €1.4 billion in windfall profits:

- 95% will support Ukraine through the [Ukraine Loan Cooperation Mechanism](#) (ULCM), which provides non-repayable support to assist Ukraine in repaying (i) the EU macro-financial assistance loan disbursed throughout 2025; in addition to (ii) loans from G7 bilateral lenders under the [Extraordinary Revenue Acceleration \(ERA\) Loans](#), which total €45 billion; and
- 5% will be channelled through the [European Peace Facility](#) (EPF), which addresses Ukraine's pressing military and defence needs.

* *CSDs operate the infrastructure that enables the settlement of securities (such as shares or bonds) in financial markets, such as by tracking each change in the ownership of securities and allowing the settlement of securities in exchange for cash (see [here](#)).*

** *Since launching in 2024, the immobilization of Russian assets has generated a total of €8 billion in windfall profits. In December 2025, the Council of the European Union prohibited transfers of immobilized CBR assets back to Russia in a more sustained way under Regulation 2025/2600 (see [here](#)).*

Council of the European Union discusses and extends sanctions against Russia

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 22 September 2026, the Council decided to prolong the restrictive measures targeting those responsible for undermining or threatening the territorial integrity, sovereignty and independence of Ukraine for another 36 months, until 22 September 2029 (see [here](#)).

The current restrictive measures apply to more than 3,000 individuals and entities and 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.

- On 7 August 2026, the Council adopted additional restrictive measures against five individuals responsible for supporting Russia's military and industrial complex in the context of its ongoing war against Ukraine and its intensified strikes deliberately targeting civilians and civilian infrastructure (see [here](#)).
- On 23 July 2026, the Council adopted a **21st package of restrictive measures** (see [here](#)) in response to Russia's war against Ukraine and follows Russia's recent brutal military strikes targeting civilian infrastructure. The package totals 218 individual listings, comprising 48 individuals and 170 entities (the largest set of individual listings in the last four years) and economic sanctions targeting key sectors that sustain Russia's war against Ukraine, and notably:
 - Intensified financial services and crypto-asset measures, e.g.:
 - Imposing asset freezes and a prohibition on making funds available to 94 banks and major financial institutions, and extending the transaction ban to 33 additional Russian credit and financial institutions.
 - Introducing, for the first time, the possibility of a full third-country ban for crypto-asset services, which is intended to serve as an important deterrent to countries hosting platforms that help Russia evade EU sanctions. This new instrument enables the EU to ban any transaction between an EU operator and any crypto provider used by Russia.
 - Widening transaction bans to 14 crypto-related service platforms located in countries such as the UAE (United Arab Emirates), Panama, the Marshall Islands, and Belarus.
 - Sustained pressure on energy revenues, e.g.:
 - Suspending the automatic adjustment of the oil price cap mechanism* until 15 July 2027, with an interim review to ensure that the suspension remains necessary and proportionate.
 - Targeting three Russian oil refineries and a major Belarusian refinery, and creating the possibility of prohibiting transactions with listed refineries processing Russian crude oil or petroleum products.
 - Russia's military industrial complex, e.g.:
 - Introducing 56 individual listings of persons and companies involved in the Russian military industrial complex, including 37 linked to long-range drones.
 - Adding 51 new entities to tighter export restrictions on dual-use goods and technologies, including entities in, e.g., China (including Hong Kong), India, Turkey, and the UAE.
 - Trade and other measures, e.g.:
 - Expanding export bans to items and technologies used by Russia's military industry, including materials and equipment for aerospace, defence, unmanned aerial vehicles and drones.
 - Introducing further import restrictions on goods generating significant revenues for Russia, worth over €60 million.

Furthermore, the 21st package also strengthens legal protection for EU operators in litigation arising from EU restrictive measures by allowing EU courts and Member States not to recognize or enforce any court decision obtained in legal proceedings before the Russian courts.

- On 13 July 2026, the Council imposed restrictive measures on nine Russian individuals and four entities forming part of Russia's cyber ecosystem, responsible for and involved in carrying out, enabling and facilitating cyber-attacks against the EU, its Member States and international partners (see [here](#)). *For further details on these sanctions of 13 July 2026, see also below Cybersecurity, Privacy & Data Protection section.*

Altogether, EU restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine now apply to over 3,000 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 21st package of sanctions.^{**}

** The G7 Oil Price Cap Coalition established an oil price cap mechanism on Russian seaborne crude oil and petroleum products in 2022. EU operators are only allowed to provide maritime transport and related services for Russian crude oil and petroleum products if sold at or below the relevant price caps. This mechanism was specifically designed to put further pressure on Russia's oil revenues, while keeping global energy markets stable through continued supplies (for further details, see [here](#)).*

*** An in-depth analysis of the 21st 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)).*

EU publishes report on monitoring EU agri-food trade (see [here](#))

On 30 July 2026, the European Commission published its recurring report on monitoring EU agri-food trade, covering January-May 2026.

The EU's agri-food sector recorded a stronger trade surplus in the first five months of 2026 (despite lower export and import values compared with the same period last year), reaching €19.4 billion between January-May 2026, i.e., €1 billion higher than a year earlier.

In this respect, cumulative exports reached €96.9 billion (down 3% compared to the same period in 2025), while cumulative imports amounted to €77.5 billion (down 5% compared to the previous year).

These cumulative figures reflect lower export and import values across several major product categories, as reflected below:

- Exports:
 - The main export reduction was to the U.S. (-13%, - EUR 1.6 billion). This follows high export levels in the first months of 2025 with potential frontloading ahead of anticipated US tariffs. The most significant reductions were in drinks (primarily due to lower prices),

olive oil (lower volumes and prices) and cocoa products (mainly due to lower volumes).

- The closure of the Strait of Hormuz from March 2026 diminished exports to the United Arab Emirates (-28%, - EUR 371 million) and to other Gulf countries with smaller flows. Exports to Bahrain, Kuwait, Qatar together fell by 29% (- EUR 186 million).
- Imports:
 - The main declines in imports were in coffee, tea, cocoa and spices, down EUR 2.9 billion (-16%). This was primarily due to the falling prices of cocoa products (-24%), which reduced import value by EUR 2.6 billion, while volumes also fell by 6%.
 - The largest import increases were in fruit and nuts, up 4% (+€465 million), and beef and veal, up 28% (+€330 million). Beef and veal imports increased from all main trading partners, supported by short supply and high EU prices.

The Commission stated that EU agri-food trade performance remained resilient from January to May 2026. The continued increase in the EU trade surplus highlighted the agri-food sector's ability to adapt to changing market conditions and maintain a strong position in global trade.

MEDICINES AND MEDICAL DEVICES

European Commission introduces new EU framework to secure Europe's supply of medical radioisotopes (see [here](#))

On 10 September 2026, the European Commission published the European Radioisotope Valley Initiative ("ERVI") (C/2026/6132), a new strategic framework designed to consolidate Europe's leading position in the production of medical radioisotopes.

Overview / objectives. Global demand for medical radioisotopes, as well as the pace of innovation in this field, only continue to accelerate. In the EU, each year, over 10 million medical examinations using radioisotopes are performed—mainly for oncology and cardiology. As a result, a substantial European production and distribution network has developed to supply patients with radioisotopes on a daily basis: The EU is now the global-leading producer of medical radioisotopes and exports half of its production abroad.

Nevertheless, certain key links in Europe's supply chain are vulnerable and exposed to dependence on foreign suppliers, ageing production facilities, and competition from alternative suppliers, which create risks of security of radioisotope supply and investment relocation, as well as rising costs.

ERVI seeks to address these challenges by setting out a coordinated approach to securing the EU's radioisotope supply, steering investment in the sector, and curbing strategic dependencies on third countries; especially targeting Russia. It also makes a direct contribution to the [REPowerEU](#) roadmap aimed at ending Russian energy imports.

Strategic priorities. ERVI is structured, in particular, around five strategic priorities:

- (1) Advancing research and innovation in next-generation radioisotopes, radiopharmaceuticals and production technologies, to be underpinned by a dedicated Strategic Research and Innovation Agenda ("SRIA") to outline common strategic goals, key research priorities, and funding

strategies to better unify fragmented EU research and innovation efforts;

- (2) Directing investment toward production infrastructure, notably by developing EU-based High Assay Low Enriched Uranium ("HALEU")* capacity and stable isotopes, which are presently sourced from Russia, alongside reactor upgrades and new facility construction;
- (3) Strengthening market monitoring and demand forecasting, leveraging the [European Observatory on the Supply of Medical Radioisotopes](#);
- (4) Forging strategic international partnerships, particularly with the UK and US, to diversify supply routes and bolster the supply chain for HALEU;
- (5) Modernizing the regulatory framework through cooperation with the International Atomic Energy Agency ("IAEA") on reliable transport rules medical radioisotopes and the simplification of EU and national procedures governing radiation protection and waste management to support patients' access to innovative treatments.

Looking ahead. As a first step under above priority (1) on advancing research and innovation, in the 2026-2027 period, the Commission plans to launch a funding call for the development of an SRIA for medical radioisotopes. In a next step, in the 2028-2034 period, the Commission aims to support the implementation of the SRIA (through a PPP (Public-Private Partnership) or other appropriate mechanism).

While concrete timelines are not yet provided for the other strategic priorities, the Commission has indicated that it will pursue these priorities in cooperation with, in particular, the Member States, industry, and end-users.

* *HALEU is used to produce medical radioisotopes in research reactors.*

European Commission launches pilot initiative on medical countermeasure manufacturing and health preparedness. (see [here](#))

On 2 July 2026, the European Commission launched the pilot phase of the "Rapid Agile Manufacturing Partnerships for Union Protection" ("RAMP UP").

Overview. RAMP UP is a voluntary preparedness network established by DG HERA (European Union (EU) Health Emergency Preparedness and Response Authority). The aim of RAMP UP is to accelerate the scale-up of the production and supply of medical countermeasures ("MCM") across the EU/EEA in the event of a health emergency. MCMs include products such as medicines, vaccines, diagnostics, medical devices, personal protective equipment, and the materials, technologies and services needed to manufacture and deliver them.

The program is built on cooperation established with industry and relevant supply chain actors ahead of emergencies and operates through four pillars:

1. Secure cooperation framework to exchange information with HERA;
2. Strategic data sharing on manufacturing and supply chain capacities;
3. Strengthened supply readiness to better inform HERA's internal emergency procurement procedures; and
4. Facilitating partnerships between actors across the MCM ecosystem.

Eligibility. RAMP UP is open to legal entities established in the EU/EEA or in countries with close trade and procurement links with the EU, with a proven role in ensuring access to medical countermeasures in a health emergency.

On eligible categories of organizations, these include marketing authorizations holders, manufacturers of medicines and medical devices, contract organizations and suppliers of active pharmaceutical ingredients (“APIs”).

Membership is voluntary, free of charge and open on a rolling basis to eligible organizations (for more information on eligibility requirements or the application process, see [here](#)).

Pilot phase / Next steps. The initial pilot phase of RAMP UP focuses on engaging pharmaceutical companies with portfolios covering pharmacological classes identified for the purpose of this RAMP UP pilot phase (see [here](#)). Such companies are encouraged to apply and participate in building the practical arrangements of the RAMP UP initiative, including data submission templates, data-sharing procedures and operational workflows.

In light of experience gained during this pilot phase, RAMP UP will progressively broaden its scope to other medical countermeasure categories, such as medical devices, in vitro diagnostics and personal protective equipment.

Updated EU guidance and new eligibility tracker released for joint clinical assessments (see [here](#))

On 19 August 2026, updated guidance and a new eligibility tool were issued for Joint Clinical Assessments (“JCAs”):

- The European Medicines Agency (“EMA”) updated pre-authorization guidance for applicants of the centralized procedure in light of the Health Technology Assessment (“HTA”) Regulation (Regulation (EU) 2021/2282)) concerning JCAs (see [here](#)).
- A new JCA eligibility tracker was released on the European Commission’s HTA webpage (see [here](#)).

To recall, the HTA Regulation provides for EU-level JCAs of certain health technologies, with the scope for medicinal products currently covering new active substances for cancer and advanced therapy medicinal products (“ATMPs”) and expanding to orphan medicinal products in 2028 and other medicinal products in 2030.

The above-referred updated guidance and new tracker introduce two notable developments:

- First, the updated guidance (Section 2.4.1.2) specifies the procedure by which applicants and health technology developers must declare whether their application falls within the scope of the HTA Regulation and is subject to JCAs.
- Second, by introducing a new JCA eligibility tracker, the Commission aims to enable health technology developers to assess at an early stage whether a medicinal product falls within the scope of a JCA. The tracker is intended to facilitate early preparation but does not replace the formal declaration through [IRIS](#), a secure online platform for handling product-related scientific and regulatory procedures with EMA.

The updated guidance reinforces the need for health technology developers to integrate JCA planning into the marketing authorization application (“MAA”) process at an early stage, in view of facilitating the regulatory and HTA timelines to be coordinated from the outset. The new JCA eligibility tracker supports enabling such early integration.

CYBERSECURITY, PRIVACY & DATA PROTECTION

ENISA publishes Threat Landscape Report 2026 (see [here](#))

On 22 September 2026, ENISA published its annual Report assessing the cybersecurity threat environment affecting the EU, covering 8,257 incidents recorded from 1 January 2025 to 31 December 2025 (*for last year's Report, see [Jones Day EU Geopolitical Update No. 123 of 8 October 2025](#)*).

Main findings. The Report indicates that the EU cyber threat landscape in 2025 remained heavily influenced by geopolitical tensions, cybercrime, and the increasing interconnection of digital ecosystems. Notably:

- Primary targets. The most targeted sector remained public administration (32% of cases), followed by business services (8%), transport (8%), manufacturing (7%), and finance/banking (6%).
- Tactics and techniques:
 - Ransomware, phishing, DDoS attacks* and vulnerability exploitation remained among the most frequently observed attack vectors affecting organizations across the EU.
 - Supply chain compromises and incidents involving cloud service providers and other digital dependencies continued to grow in impact, demonstrating how disruptions affecting a single provider can have cascading consequences across multiple sectors.
- Continued impact of geopolitical developments:
 - The war in Ukraine and the escalation of conflicts in the Middle East continued to drive cyber activity in the EU, with ideology-driven operations accounting for 57.3% of observed incidents.
 - State-sponsored cyberespionage activity continued, notably by Russia-nexus intrusions targeting governmental and diplomatic entities and by China-nexus intrusions showing continued interest in the transport sector, including maritime related entities.

Outlook. ENISA expects the main trends observed in 2025 to remain ongoing. EU organizations are likely to remain exposed to a combination of cybercrime, cyberespionage and hacktivist activity, increasingly driven by geopolitical developments.

In particular, the growing use of AI in cyber operations is expected to continue to enhance the speed, scale and sophistication of attacks, lower barriers to entry for malicious actors and create new cybersecurity risks for organizations, in particular as integrating AI systems into business environments creates a broadened attack surface.

* “DDoS (Distributed Denial-of-Service) attacks” are cyber-attacks designed to make a website, online service or network unavailable by overwhelming it with an extremely large volume of internet traffic. By flooding the target with more

requests than it can handle, attackers can slow down or completely disrupt access for legitimate users.

EU Cyber Resilience Act – Mandatory vulnerability and incident reporting obligations become applicable (see [here](#))

On 11 September 2026, mandatory vulnerability and incident reporting obligations under the EU Cyber Resilience Act ("[CRA](#)") started to apply.

To recall, the CRA is a first-of-its-kind regulation establishing comprehensive cybersecurity requirements for economic operators placing products with digital elements* on the EU market.

Extensive reporting duties are among the CRA's key obligations for manufacturers – which must notify both (i) the European Union Agency for Cybersecurity ("ENISA") and (ii) the relevant Computer Security Incident Response Team ("CSIRT") designated as coordinator* -- of any actively exploited vulnerability* in their product and any severe incident* affecting the security of their product (see also [Jones Day Alert: EU Cyber Resilience Act: 24-Hour Reporting Duties Start September 11, 2026](#)).

Reporting timelines run from the moment the manufacturer becomes aware:

- Early warning notification: within 24 hours;
- Vulnerability notification: within 72 hours;
- Final report on vulnerability: within 14 days after a corrective or mitigating measure becomes available (for actively exploited vulnerabilities), or within one month of the 72-hour notification (for severe incidents).

All notifications must be submitted via ENISA's [CRA Single Reporting Platform](#) ("SRP"). The SRP allows manufacturers to report only once, rather than notifying multiple national authorities separately. Manufacturers submit a single electronic notification through the SRP to the CSIRT designated as coordinator, regardless of whether they have multiple branches or subsidiaries within the EU or whether their parent company is headquartered outside the EU.

To facilitate compliance with these new reporting obligations, ENISA has published a range of supporting resources for manufacturers using the SRP, including [Frequently Asked Questions \(FAQs\)](#), a [Factsheet](#), a [Glossary](#), and detailed [User Manual](#).

Looking ahead. The next deadline under the CRA is 11 December 2027, when all remaining obligations will start to apply for manufacturers (including the requirement to ensure "cybersecurity by design" for products with digital elements), as well as obligations applicable to importers and distributors.

* *The CRA defines:*

a "product with digital elements" as a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network.

a "CSIRT designated as coordinator" as the national CSIRT of the Member State where the manufacturer has its main establishment in the EU, understood as the Member State where the decisions related to the cybersecurity of the products with digital elements are predominantly taken.

an “actively exploited vulnerability” as a vulnerability for which there is reliable evidence that a malicious actor has exploited it in a system without permission of the system owner.

a “severe incident” as an incident that negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of data or functions, and which either (i) affects sensitive or important data or functions; or (ii) has led or is capable of leading to the introduction or execution of malicious code in a product with digital elements or in the network and information systems of a user of the product with digital elements.

Council of the EU adopts new sanctions in response to Russia’s cyberattacks and malicious activities (see [here](#))

On 13 July 2026, the Council of the EU imposed sanctions on nine Russian individuals and four entities (see [here](#)) or their involvement in malicious cyber activities and other destabilizing actions targeting the EU, its Member States and international partners.

The sanctions were adopted under the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (“[EU Cyber Diplomacy Toolbox](#)”), a political framework to enable the EU and its Member States to deploy the full range of measures under the Common Foreign and Security Policy (CFSP), including restrictive measures, to prevent, discourage, deter, and respond to malicious cyber activities.

Backdrop. Since adopting the EU Cyber Diplomacy Toolbox on 19 June 2017, the Council has further built this framework by adopting Decision 2019/797* and Regulation 2019/796** on 17 May 2019, which together established a dedicated sanctions regime allowing the EU to impose travel bans and asset freezes on persons and entities responsible for cyber-attacks with a significant effect constituting an external threat to the EU or its Member States.

On 8 October 2024, the Council established a broader sanctions framework under Decision 2024/2643,*** targeting those engaged in actions by the Russian government that undermine EU values, security, and integrity, and also covering hybrid threats such as cyber-attacks, disinformation, sabotage of critical infrastructure, and the instrumentalization of migrants.

New sanctions. The sanctions imposed in July 2026 target key actors within Russia’s cyber ecosystem involved in enabling, facilitating, or carrying out cyber-attacks against the EU and its partners. Notably, they mark the first time the EU and the UK adopted sanctions simultaneously under their respective cyber sanctions regimes.

Those targeted under the sanctions include providers of cybercriminal infrastructure, pro-Russian hacktivist groups, individuals involved in the development and deployment of malicious software, and persons linked to Russian military intelligence operations and broader destabilization activities.

The sanctions impose asset freezes, prohibit EU persons and companies from making funds available to the listed persons and entities, and subject the sanctioned individuals to EU travel bans.

For further details on EU sanctions against Russia, see above Trade / Export Controls section.

* [Council Decision \(CFSP\) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States](#)

**** [Council Regulation \(EU\) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States](#)**

***** [Council Decision \(CFSP\) 2024/2643 concerning restrictive measures in view of Russia's destabilising activities](#)**

European Commission presents EU Action Plan on Cybersecurity and Artificial Intelligence (see [here](#))

On 7 July 2026, the European Commission presented the [EU Action Plan on Cybersecurity and Artificial Intelligence](#) ("Action Plan"), which aims to provide a structured response to the risks and opportunities arising from the use of advanced AI models in cybersecurity.

The Action Plan forms part of a broader and ongoing EU effort to strengthen cybersecurity in the age of AI. In particular, it builds on the EU's existing legal framework (including the [AI Act](#), the [Cyber Resilience Act](#) (CRA), the [NIS 2 Directive](#), the [Digital Operational Resilience Act](#) (DORA), and the [Cyber Solidarity Act](#)).

The Action Plan sets out a coordinated approach to help Member States, businesses and public authorities harness the benefits of AI while addressing the cybersecurity risks it may create. It is built around three pillars:

- Making frontier AI safe, accessible and deployable for European cybersecurity by strengthening AI risk evaluation, testing capabilities, and secure access to advanced AI systems for legitimate cybersecurity purposes. This includes developing a [European Blueprint guidance document](#) for enabling secure access to advanced AI systems, as well as establishing a secure testing platform to support the safe deployment of AI solutions in critical sectors.
- Preparing the EU cyber ecosystem for the AI age by integrating AI into cybersecurity operations, supporting critical sectors, accelerating vulnerability management, and reinforcing cyber resilience through ENISA's expertise. This includes promoting the implementation of existing EU cybersecurity legislation.
- Scaling European AI capabilities for cybersecurity by fostering innovation, investment, deployment, and skills development to strengthen cyber resilience and enhance Europe's digital sovereignty. This includes, notably:
 - launching an [EU Grand Challenge on AI for Cybersecurity](#) to accelerate the development of innovative AI-powered security solutions, bringing together European cybersecurity and AI companies, research organizations, critical infrastructure operators and open source communities around this common mission;
 - investing in sovereign AI capabilities through initiatives such as [leveraging existing AI Factories](#) (e.g., relevant cyber-focused AI Factories should facilitate access to high-quality AI-ready datasets, from public data to sensitive industrial and cybersecurity data, and support the development and validation of AI models in a controlled and accountable environment through their data labs); and
 - [fostering private investment to scale European AI technologies](#), notably through an envisaged [new European equity capacity](#) managing a portfolio of large-scale equity investments key for the EU's technological sovereignty (e.g., digital technologies such as frontier AI, as well as clean energy technologies, biotech, and

potentially defence tech), in consultation with the Member States, the EIB (European Investment Bank) Group and other key stakeholders.

Outlook. Recognizing that AI capabilities will continue to evolve rapidly, bringing both new opportunities and emerging risks, the European Commission will regularly monitor implementation of the Action Plan and adapt its measures as necessary.

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.