EU RegCORE Client Alert

Financial Services

August 2026

The EU's 20th and 21st Russia Sanctions Packages: A new compliance architecture for financial services firms

QuickTake

On 23 April 2026 and 23 July 2026, the Council of the European Union adopted, respectively, the 20th and 21st packages of restrictive measures against Russia.[1] Together, these packages represent what the Council describes as a structural shift in EU sanctions policy: from expanding lists of designated persons toward systematically disrupting the financial infrastructure (payment channels, banking relationships, crypto-asset ecosystems, correspondent banking, trade finance and maritime logistics) that enables Russia's war economy.

Bottom line: *For banks, investment firms, payment institutions, e-money institutions, crypto-asset service providers (**CASPs**), insurers and asset managers, these developments significantly increase operational compliance expectations. The compliance challenge is no longer simply screening customers*

Dr. Michael Huertas
Tel: +49 160 97375760
michael.huertas@pwc.com

Mariya Atanasova-Rigas
Tel: +49 151 42669964
mariya.atanasova-rigas@pwc.com

EU RegCORE Team
de_regcore@pwc.com

[1] 20th Package available here and 21st Package available here.

against sanctions lists. Firms must now identify how transactions, financing arrangements and digital assets may indirectly facilitate sanctioned economic activity.

Background and context

EU sanctions policy against Russia has evolved considerably since the initial packages adopted in 2014 and the major expansion following the full-scale invasion of Ukraine in February 2022. Earlier packages concentrated primarily on designating individuals and entities (asset freezes, travel bans), excluding specific banks from SWIFT and imposing sectoral export and import controls. This approach was effective in constraining identified actors but left significant scope for circumvention through alternative financial infrastructure.

The 20th package (adopted 23 April 2026) and, in particular, the 21st package (adopted 23 July 2026) mark a notable evolution. Rather than merely expanding the list of designated persons, these packages target the infrastructure that permits sanctions evasion:

1. Russian financial institutions and their correspondent relationships;
2. crypto-asset service providers and decentralised platforms;
3. shadow banking networks and alternative payment mechanisms (including "**SPFS**", Russia's SWIFT-equivalent);
4. shadow fleet vessels and their financing/insurance ecosystem;
5. third-country intermediaries facilitating re-export and circumvention; and
6. LNG tanker services and energy-sector financing.

This trajectory can be described as a shift toward "network-based sanctions" — that is, measures directed at the financial networks and infrastructure enabling sanctioned activity, rather than solely at designated end-users. This is our own analytical framework for describing the direction of EU sanctions policy; it is not a legal term used by the EU institutions themselves. Nevertheless, it captures a genuine trend: for financial institutions, sanctions compliance is increasingly converging with financial crime risk management rather than remaining a standalone list-screening exercise.

1. Expansion of banking and financial institution restrictions

The two packages have substantially expanded the scope of financial sector designations and transaction bans:

- **20th package**: extended the EU market access ban to 20 additional Russian banks, bringing the total of Russian banks excluded from the EU market to 70 (subject to narrow humanitarian exceptions). Transaction bans were extended to four third-country banks (in Kyrgyzstan, Laos and Azerbaijan) assisting the Russian war effort or connected to SPFS. Five third-country financial entities were delisted following commitments not to re-engage in sanctioned activity.

- **21st package**: imposed asset freezes and prohibitions on making funds available to 94 banks and major financial institutions, together with a prominent figure in Russia's banking establishment. Transaction bans were extended to 33 additional Russian credit/financial institutions. A further Kyrgyz bank connected to SPFS and two Indian branches of Russian banks. were subjected to transaction bans for circumventing sanctions. Four designations related to the cross-border "A7 network," including new links to Africa.

Taken together, these measures mean that a substantial part of significant Russian banking infrastructure is now subject to EU restrictive measures and that EU-regulated firms face heightened due diligence expectations in relation to any residual correspondent relationships that could indirectly access Russian banking networks.

2. Crypto-assets as a sanctions priority

Crypto-asset channels have been identified as a principal circumvention mechanism and the EU has responded with progressively broader measures:

- **20th package**: introduced a total sectoral ban on exchanges with any Russian CASP and any decentralised platform enabling crypto trading, on the basis of their use in circumvention. Prohibited the use of or support to RUBx (a rouble-backed stablecoin) and the digital rouble (Russia's CBDC under development), both identified as enabling sanctions circumvention.

- **21st package**: extended transaction bans to 14 crypto-related service platforms based in Georgia, Panama, the UAE, the Marshall Islands, Kyrgyzstan and Belarus. Introduced, for the first time, the possibility of a full third-country ban for crypto-asset services — a new instrument enabling the EU to ban any transaction between an EU operator and any crypto provider used by Russia, intended as a deterrent to countries hosting circumvention platforms.

The new third-country crypto ban instrument is particularly significant. It represents a jurisdictional tool allowing the EU to cut off entire national crypto ecosystems from EU market access where those ecosystems are assessed as facilitating Russian circumvention. CASPs and firms with crypto-asset exposure must now maintain dynamic monitoring of which jurisdictions and platforms fall within scope and must be prepared for rapid de-risking if a third-country ban is activated.

3. Third-country circumvention and anti-circumvention tools

As stated in the Council's press release a defining feature of the 20th package was the first-ever activation of the EU's anti-circumvention instrument, applied to the Kyrgyz Republic for systematic failure to prevent re-export to Russia of EU machine tools and telecommunications equipment used in drone and missile manufacturing. As Commissioner Albuquerque noted, this represented "another decisive step in tackling sanctions evasion, targeting financial actors and infrastructure in third countries that enable circumvention."[2]

Across both packages, the anti-circumvention measures include:

- **20th package**: 60 entities added to the circumvention list (32 in Russia, 28 in third countries including China/Hong Kong, Türkiye, UAE, Thailand). Transaction bans imposed on third-country banks connected to SPFS. Port bans extended for the first time to a third-country port (Karimun Oil Terminal, Indonesia).

- **21st package**: 51 new entities added to tighter dual-use export restrictions, located in China (including Hong Kong), India, Kazakhstan, Kyrgyzstan, Türkiye and the UAE, implicated in circumventing export restrictions on microelectronics, CNC machine tools and semiconductor processing equipment. Designation of third-country suppliers (China, UAE, Uzbekistan, Kazakhstan, Belarus) providing dual-use goods and weapons systems.

[2] See here.

For financial institutions, these measures create heightened obligations to monitor trade finance, correspondent banking and payment flows involving third-country intermediaries whose jurisdictions or sectors have been flagged for circumvention risk. Standard customer due diligence may be insufficient; enhanced transaction-level analysis of goods flows, end-use and beneficial ownership chains is increasingly expected.

4. Shadow fleet financing and maritime logistics

The shadow fleet — vessels used to transport Russian crude oil and petroleum products outside the G7/EU price cap mechanism — has been a sustained focus:

- **20th package**: 46 additional vessels listed (bringing the total to 632). A significant maritime insurer was designated. New safeguards on EU tanker sales introduced mandatory "no Russia" clauses, enhanced due diligence and a "scrapping clause" for decommissioning/exit. Port access bans imposed on Murmansk and Tuapse (Russia) and Karimun Oil Terminal (Indonesia). Basis laid for a future maritime services ban on transporting Russian crude/petroleum products, to be timed with G7/price cap coalition coordination.

- **21st package**: 41 further vessels listed. Scope extended to cover vessels providing bunkering or other services supporting the shadow fleet. Eight entities and one individual designated in the shadow fleet ecosystem, including crypto-related companies operating on behalf of Russian oil majors and, for the first time, a crewing agency. Five oil traders added to the transaction-ban list for frustrating the purchase prohibition.

For insurers, trade finance providers and banks with shipping portfolios, these measures create direct exposure. Vessel screening, insurance underwriting due diligence and trade finance documentary checks must now encompass not only sanctioned vessels themselves but also the broader ecosystem of bunkering services, crewing agencies and crypto-denominated payment flows that support the shadow fleet.

5. LNG and energy financing

Energy-sector measures have been significantly expanded:

- **20th package**: 36 listings across the upstream/downstream Russian energy sector (exploration, extraction, refining, transport). Prohibition on maintenance services for Russian LNG tankers and icebreakers. Ban allowing EU operators to terminate long-term LNG terminal services contracts with Russian operators.

- **21st package**: 18 entities and one individual designated, including three Russian refineries, a major Belarusian oil refinery and a company selling Belarusian petroleum products within Russia. New possibility to prohibit transactions with listed refineries in Russia/third countries processing Russian crude. A transaction ban (entering into force in six months) imposed on a Georgian refinery trading/processing Russian oil at Kulevi. New notification obligation for sales of LNG tankers, with the possibility of restrictions on sales to Russian citizens/companies and new contractual obligations to mitigate resale/reuse risk.

- **Oil price cap**: automatic adjustment mechanism paused until 15 July 2027 (to contain Russian oil-sale profits given market conditions following the closure of the Strait of Hormuz), with an interim review to confirm the suspension remains necessary and proportionate.

Financial institutions providing project finance, trade finance or structured lending to energy-sector clients must review their portfolios for exposure to newly designated refineries and the expanding scope of LNG-related restrictions, including contractual obligations on tanker sales.

6. Legal protections for EU operators

Both packages have introduced or expanded legal protections for EU firms facing retaliatory or abusive litigation in Russian courts:

- **20th package**: Member State courts are empowered to address litigation by Russian entities brought in Russian courts that the EU considers to lack legitimate basis. EU firms may claim damages where such judgments are enforced in third countries. The Council is empowered to impose transaction bans on third-country firms or individuals cooperating in enforcement of such judgments. Transaction bans were imposed against Russian competitors benefiting from expropriation of EU operator assets and those using EU operators' IP rights in Russia without consent.

- **21st package**: EU courts and Member States empowered not to recognise or enforce judgments obtained in Russian court proceedings.

These provisions are of immediate relevance to financial institutions with residual Russian exposures, trapped assets, or ongoing contractual disputes. They provide a legal basis for resisting enforcement of Russian court judgments and pursuing compensation for retaliatory measures.

Litigation and enforcement tools

The 20th and 21st packages introduce (or at least aim to facilitate) significant new legal tools for EU operators facing retaliatory or abusive litigation in Russian courts, as well as expanded enforcement exposure for firms whose infrastructure may be connected to circumvention networks. This annex addresses the key litigation and enforcement considerations.

1. Defence against Russian court judgments

The 21st package empowers EU courts and Member States not to recognise or enforce judgments obtained in Russian court proceedings. This represents a significant strengthening of legal protection for EU operators with trapped Russian assets or ongoing contractual disputes. Firms should consider:

- Reviewing existing Russian court proceedings and judgments for potential non-recognition under the new provisions;
- Assessing whether any pending enforcement actions in third countries may be resisted on the basis of EU non-recognition;
- Documenting the abusive or retaliatory nature of Russian proceedings for use in EU court applications; and
- Engaging with Member State courts on procedural requirements for invoking non-recognition.

2. Damages claims for abusive enforcement

The 20th package enables EU firms to claim damages where abusive Russian court judgments are enforced in third countries. This creates a potential recovery mechanism for firms that have suffered losses as a result of retaliatory litigation. Key considerations include:

- Identifying and documenting losses attributable to enforcement of abusive judgments;
- Assessing the availability of assets within the EU against which damages claims may be enforced;
- Coordinating with legal counsel in relevant third-country jurisdictions where enforcement has occurred; and
- Monitoring the Council's potential imposition of transaction bans on third-country firms or individuals cooperating in enforcement.

3. Enforcement exposure for infrastructure-connected firms

The shift toward infrastructure-focused sanctions creates new categories of enforcement risk. Firms whose payment channels, correspondent relationships, crypto-asset services or trade finance operations are connected — directly or indirectly — to circumvention networks may face:

- Regulatory enforcement action by national competent authorities for inadequate sanctions controls;
- Designation or transaction-ban listing where the firm is assessed as facilitating circumvention (as occurred with third-country banks connected to SPFS);
- Reputational consequences and potential de-risking by correspondent banks or counterparties;
- Civil liability exposure where customers or counterparties suffer losses as a result of sanctions breaches; and
- Criminal liability for directors or officers in severe cases involving wilful or reckless facilitation.

4. Third-country crypto ban: jurisdictional enforcement implications

The new third-country crypto ban instrument — enabling the EU to prohibit transactions between EU operators and any crypto provider used by Russia — introduces novel enforcement considerations. Firms should assess:

- Exposure to jurisdictions currently hosting circumvention platforms (Georgia, Panama, UAE, Marshall Islands, Kyrgyzstan, Belarus);
- Contractual termination rights and wind-down procedures in the event a third-country ban is activated;
- Documentation requirements to demonstrate that counterparty due diligence was conducted prior to any ban; and
- Escalation protocols for rapid de-risking if a jurisdiction is designated.

5. Trapped assets and contractual disputes

Many EU financial institutions continue to hold trapped Russian assets or face ongoing contractual disputes arising from sanctions-related performance failures. The new legal protection provisions provide a basis for:

- Resisting enforcement of Russian court judgments purporting to award damages for non-performance attributable to EU sanctions;
- Seeking declaratory relief in EU courts confirming the non-enforceability of such judgments;

- Pursuing claims against Russian entities that have benefited from illegitimate expropriation or IP misappropriation; and
- Coordinating multi-jurisdictional litigation strategies where assets are located across multiple EU Member States and third countries.

6. Board and senior management liability

The governance implications of infrastructure-focused sanctions extend to personal liability exposure for directors and senior managers. Boards should consider:

- Whether D&O insurance policies adequately cover sanctions-related claims;
- The adequacy of management information provided to the board on sanctions risk;
- Documentation of board-level oversight and decision-making on sanctions matters;
- Personal exposure under national implementing legislation in each relevant Member State; and
- Indemnification arrangements and legal expense coverage for sanctions-related investigations or proceedings.

Governance implications for firms

Given all of the changes discussed above and the overarching shift from entity-based sanctions to infrastructure-focused measures, this is likely to pose significant implications for board and senior management oversight for firms requiring to abide by EU sanctions:

- **Sanctions governance architecture:** sanctions compliance can no longer be treated as a standalone legal silo. It must be embedded within enterprise-wide financial crime governance frameworks, with clear reporting lines to the board or a designated board committee.

- **Risk appetite:** boards should articulate a sanctions risk appetite that addresses not only direct sanctions exposure but also the risk of indirect facilitation through payment channels, correspondent relationships and third-party networks.

- **Escalation frameworks:** given the pace of new designations (218 listings in the 21st package alone — the largest batch in four years) and the introduction of new instrument types (the third-country crypto ban), escalation protocols must enable rapid decision-making on de-risking and transaction blocking.

- **Management information (MI):** boards require structured MI that captures not only screening hit rates but also indicators of potential circumvention — unusual payment routing, third-country concentration risk, crypto-asset flow anomalies and trade finance red flags.

- **AI-assisted monitoring:** the complexity and volume of infrastructure-focused sanctions increasingly necessitate AI and machine-learning tools for transaction monitoring, network analysis and anomaly detection, subject to appropriate model governance.

- **Third-party risk:** firms must assess whether outsourced functions (payments processing, custody, trade finance operations) have adequate sanctions controls, particularly where service providers operate in or through flagged third-country jurisdictions.

What firms should consider doing now

In light of the 20th and 21st packages, financial services firms should consider the following actions as a matter of priority:

- **Sanctions screening and transaction monitoring.** Conduct a comprehensive gap analysis of current sanctions screening and transaction monitoring systems against the expanded scope of infrastructure-focused measures, including crypto-asset flows, correspondent banking chains and third-country intermediaries.

- **Network-level analysis.** Update sanctions policies and procedures to reflect the shift from entity-only screening to network-level analysis, incorporating indicators of circumvention risk (unusual payment routing, jurisdictional concentration, vessel-related anomalies).

- **Crypto-asset compliance.** Review and, where necessary, enhance crypto-asset compliance frameworks to address the total sectoral ban on Russian CASPs, the prohibition on RUBx/digital rouble and the potential activation of the third-country crypto ban instrument.

- **Correspondent banking.** Reassess correspondent banking relationships for any residual indirect exposure to designated Russian banks or SPFS-connected institutions, including through multi-hop payment chains via third-country correspondents.

- **Trade finance and shipping.** Strengthen trade finance and shipping due diligence to incorporate expanded vessel lists (673+ vessels), port bans, “no Russia” contractual clauses and enhanced scrutiny of bunkering, crewing and insurance service providers.

- **Energy-sector exposures.** Review energy-sector portfolio exposures against newly designated refineries, LNG tanker restrictions and the six-month wind-down for the Georgian refinery transaction ban.

- **Board and senior management MI.** Upgrade board and senior management MI to include sanctions-specific risk indicators, circumvention red flags and metrics on the effectiveness of infrastructure-level monitoring.

- **Third-party and outsourcing arrangements.** Assess third-party and outsourcing arrangements for sanctions adequacy, particularly where service providers operate in or through jurisdictions flagged for circumvention risk (Kyrgyzstan, UAE, Türkiye, Georgia, Panama).

- **Legal protection provisions.** Engage proactively on the new EU legal protection provisions (non-recognition of Russian court judgments, damages claims for abusive enforcement), particularly where firms hold trapped Russian assets or face contractual disputes.

- **Regulatory integration.** Integrate sanctions compliance planning with MiCAR, DORA and AML/AMLA readiness, reflecting the supervisory trend toward treating these as interconnected domains rather than separate workstreams.

Outlook

The trajectory of EU sanctions policy is clear. Since February 2022, the EU has moved through successive phases: from targeted asset freezes and travel bans, through sectoral export controls and SWIFT exclusions, to the current phase in which the financial infrastructure itself — payment rails, correspondent banking, crypto ecosystems, maritime logistics, LNG services — is the primary target. Each successive package has demonstrated greater precision in identifying and disrupting the networks that enable circumvention.

Our thesis, consistent with our work across EU sanctions, AML and financial services regulation, is this:

> *The next phase of EU sanctions enforcement will focus less on adding names to designations lists and more on ensuring that the financial infrastructure available to EU-regulated firms cannot — directly or indirectly, intentionally or inadvertently — facilitate sanctioned economic activity. This is a fundamentally different compliance challenge, requiring a fundamentally different governance and operational architecture.*

The question that boards and senior management must now confront is not simply “is this customer sanctioned?” but rather “could our financial infrastructure inadvertently facilitate sanctioned economic activity?” That is a more consequential question — and one that demands enterprise-wide visibility across payments, correspondent banking, trade finance, crypto-asset and energy exposures.

About us

PwC Legal is assisting a number of financial services firms and market participants in forward planning for changes stemming from relevant related developments. We have assembled a multi-disciplinary and multi-jurisdictional team of sector experts to support clients navigate challenges and seize opportunities as well as to proactively engage with their market stakeholders and regulators.

Moreover, we have developed a number of RegTech and SupTech tools for supervised firms, including PwC Legal's Rule Scanner tool, backed by a trusted set of managed solutions from PwC Legal Business Solutions, allowing for horizon scanning and risk mapping of all legislative and regulatory developments as well as sanctions and fines from more than 2,500 legislative and regulatory policymakers and other industry voices in over 170 jurisdictions impacting financial services firms and their business.

Equally, in leveraging our Rule Scanner technology, we offer a further solution for clients to digitise financial services firms' relevant internal policies and procedures, create a comprehensive documentation inventory with an established documentation hierarchy and embedded glossary that has version control over a defined backward plus forward looking timeline to be able to ensure changes in one policy are carried through over to other policy and procedure documents, critical path dependencies are mapped and legislative and regulatory developments are flagged where these may require actions to be taken in such policies and procedures.

The PwC Legal Team behind Rule Scanner are proud recipients of ALM Law.com's coveted "2024 Disruptive Technology of the Year Award" and the "2025 Regulatory, Governance and Compliance Technology Award in 2025".

If you would like to discuss any of the developments mentioned above, or how they may affect your business more generally, please contact any of our key contacts or PwC Legal's RegCORE Team via de_regcore@pwc.com or our website.

Contact

Dr. Michael Huertas
Tel: +49 160 97375760
michael.huertas@pwc.com

Mariya Atanasova-Rigas
Tel: +49 151 42669964
mariya.atanasova-rigas@pwc.com

EU RegCORE Team
de_regcore@pwc.com

www.pwc.de