EU RegCORE Client Alert

Financial Services

August 2026

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

Dr. Hagen Weiss
Tel: +49 1511 5708446
hagen.weiss@pwc.com

Fabian Joshua Schmidt, LL.M.
Tel: +49 151 41490437
fabian.joshua.schmidt@pwc.com

EU RegCORE Team
de_regcore@pwc.com

Following the money: the Commission maps the next phase of EU financial-intelligence access

QuickTake

On 29 July 2026, the European Commission published its first report on Directive (EU) 2019/1153, which facilitates law-enforcement access to bank-account information and financial intelligence. The Council circulated the Report and its annex identifying Member State designated authorities on 26 August 2026.[1]

The Report arrived 726 days after the statutory deadline of 2 August 2024. It does not propose materially wider access to information held by banks, crypto-asset service providers (**CASPs**) or other obliged entities. Instead, the Commission concludes that it is too early to determine whether extending the

[1] Available here along with its annex here. NB: The Commission adopted the Report and accompanying Annex on 29 July 2026. The Council Secretariat subsequently circulated them to Member State delegations on 26 August 2026 as documents ST 12326/26 and ST 12326/26 ADD 1. The 26 August date does not indicate a second adoption or substantive amendment and does not make the Report another four weeks late.

definition of financial information would be necessary and proportionate. This is a deferral, not a rejection.

What this means for firms. Firms should expect requests to move more quickly through a broader range of cross-border channels as the EU connects account registers and standardises covered transaction records. Once Article 6a has been implemented nationally, covered records will have to be supplied in the prescribed electronic structured format. The same data may be requested on different legal bases and will need to reconcile across FIU, supervisory, criminal, sanctions and judicial proceedings. The principal challenge is therefore one of data, governance and process rather than a new reporting policy.

Why it matters if you get it wrong. Late, incomplete or inconsistent production can prompt scrutiny of systems and controls, senior-management governance and the institution's ability to identify its own customers and accounts. A fast, coherent and legally controlled response is more likely to narrow an inquiry than to expand it.

The Commission's caution reflects reforms that are still being implemented. The emerging architecture connects record creation and retention, FIU analysis, national registers and the future Bank Account Registers Interconnection System (**BARIS**), structured transaction production, Europol and AMLA cooperation, and asset tracing and recovery.[2]

Two distinctions matter. Directive 2019/1153 connects the AML system with criminal enforcement, but the developing regime separates account identification, production format and the legal power to compel records.

1. BARIS and Article 6a perform different functions. BARIS will help authorised authorities identify bank, payment, securities and crypto-asset accounts and safe-deposit boxes across the EU. Article 6a concerns the structured format for specified payment-account and IBAN-based bank-account operations and crypto-asset transfers requested during a criminal investigation; it does not presently cover securities or custody transactions generally.

2. Article 6a standardises how covered records are produced; it does not create an EU-wide power to demand them. National law continues to determine the requesting authority, threshold, authorisation, deadline, grounds of challenge and evidential use.

The Report itself imposes no new production obligation. It nevertheless points towards faster, more consistent and machine-readable production, subject to national procedural law, privilege, proportionality and data-protection safeguards.

Who is affected? Article 6a is directly relevant to credit institutions and financial institutions, expressly including payment and electronic money institutions and CASPs. The wider account-identification architecture also reaches securities accounts, while technology, cloud, payment-processing and data providers may hold records needed by regulated firms.

[2] BARIS is the EU-level system, provided for in Article 16 of Regulation (EU) 2024/1624 and Article 14 et seq. of Directive (EU) 2024/1640, that is to interconnect the national centralised automated mechanisms (bank account registers and data retrieval systems) that Member States must maintain, so as to enable competent authorities to identify in which Member State a natural or legal person holds bank, payment, securities or crypto-asset accounts, without giving direct access to the underlying transaction data.

What should firms do now?

- Map which authorities may request which information from each relevant legal entity and jurisdiction.
- Test whether covered account and transaction records can be produced completely, accurately and within realistic investigative deadlines.
- Establish a central protocol for parallel FIU, supervisory, law-enforcement, sanctions, tax and judicial requests.
- Review privilege, confidentiality, tipping-off, data-protection and cross-border production controls.
- Ensure third-party and legacy-system arrangements support timely, structured and auditable production.

Bottom line: the data architecture is becoming more integrated while the governing law remains fragmented across instruments, authorities and national procedures. Firms need interoperable data without assuming that the legal bases for obtaining and using it are equally harmonised.

Background and context

Directive (EU) 2019/1153 closes a gap between the EU AML framework and criminal enforcement. AML rules require obliged entities to conduct due diligence, monitor transactions, retain records and report suspicion to FIUs. The Directive helps designated authorities establish where accounts are held, obtain FIU information and cooperate across borders, subject to specific safeguards.[3][4][5][6][7]

Directive 2019/1153 therefore requires participating Member States to designate authorities empowered to:

1. access and search national centralised bank-account registers directly and immediately;
2. request financial information or financial analysis from the national FIU;
3. exchange relevant information with corresponding authorities in other Member States; and
4. provide bank-account and financial information to Europol in appropriate cases.

---

[3] The term "obliged entities" is used in the sense of Article 2(1) of Directive (EU) 2015/849 (as amended), and now Article 3 of Regulation (EU) 2024/1624, (the **AMLR**) i.e. those persons and undertakings that are subject to EU anti-money laundering and counter-terrorist financing requirements, including credit institutions, financial institutions, CASPs, auditors, external accountants and tax advisers, notaries and other independent legal professionals when participating in specified transactions, trust or company service providers, estate agents and certain traders in high-value goods.

[4] Europol is the European Union Agency for Law Enforcement Cooperation, established by Regulation (EU) 2016/794 (as amended by Regulation (EU) 2022/991), which supports and strengthens action by national law enforcement authorities in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime affecting a common Union interest, including by processing and analysing information such as financial data.

[5] Eurojust is the European Union Agency for Criminal Justice Cooperation, established by Regulation (EU) 2018/1727, which supports and coordinates national investigating and prosecuting authorities in cases of serious cross-border crime, including by facilitating the execution of requests for judicial cooperation and mutual legal assistance.

[6] The European Public Prosecutor's Office (**EPPO**) is the independent Union body established by Council Regulation (EU) 2017/1939 under enhanced cooperation, which is competent to investigate, prosecute and bring to judgment offences affecting the financial interests of the Union, including certain VAT fraud and related money laundering, in the participating Member States.

[7] The European Anti-Fraud Office (**OLAF**) is the Commission service that, under Regulation (EU, Euratom) No 883/2013 (as amended by Regulation (EU, Euratom) 2020/2223), conducts administrative investigations into fraud, corruption and any other illegal activity affecting the financial interests of the Union, and cooperates with the EPPO and national authorities without itself exercising criminal prosecution powers.

The Directive applies to all EU Member States other than Denmark. It was adopted on 20 June 2019, entered into force on 31 July 2019 and was due to be transposed by 1 August 2021.

The annex accompanying the Commission's report lists the authorities designated under Article 3. It does not grant new powers or confirm that every element of the relevant national framework complies with the Directive.

For Germany, the annex identifies:

- the *Bundeskriminalamt*[8] (Federal Criminal Police Office) and *Bundesamt für Justiz*[9] (Federal Office of Justice) as authorities entitled to access bank-account-register information; and
- the *Bundeskriminalamt* as the authority entitled to request and receive financial information or financial analysis from the FIU.

For the specific purposes of Directive 2019/1153, Germany's designation is comparatively narrow. Several Member States designate broader groups of police, prosecutorial, judicial, tax, customs, anti-corruption and asset-recovery authorities. Spain, for example, includes EPPO in Spain (the *Fiscalía Europea*) within its competences.[10]

Why this matters for German institutions. The narrow Article 3 designation does not insulate German institutions from requests made under other domestic or cross-border powers. As BARIS develops, authorities in other Member States should be better able to identify relevant German-held accounts and then pursue the underlying records through the applicable cooperation or evidential channel.

Cross-border groups therefore need an authority-access map by legal entity, jurisdiction, requesting authority, investigative stage, information type and legal basis.

1. A late report—but a more important architectural shift

Article 21 required three assessments by 2 August 2024:[11]

1. Article 21(1) required the Commission to report on implementation of the Directive and repeat that exercise every three years.

2. Article 21(3) required the Commission to assess whether "financial information" should be extended beyond information already held by FIUs. The assessment was to cover information held by public authorities or obliged entities and available to FIUs without coercive measures under national law. If appropriate, it was to be accompanied by a legislative proposal.

3. Article 21(4) required an assessment of the opportunities and challenges involved in extending FIU-to-FIU exchanges beyond exceptional and urgent cases involving terrorism or organised crime associated with terrorism.

---

[8] The *Bundeskriminalamt* is Germany's central federal criminal-police authority and a recipient of FIU financial analysis; the German FIU sits within the *Generalzolldirektion* (General Directorate Customs).

[9] The *Bundesamt für Justiz* performs federal central-authority, register and administrative-enforcement functions relevant to criminal-justice cooperation.

[10] *Fiscalía Europea* is Spain's designation for EPPO. EPPO's competence is confined to offences affecting the EU's financial interests and inextricably linked offences.

[11] Directive (EU) 2019/1153, art 21(1), (3) and (4).

COM(2026) 408 is dated 29 July 2026. It was therefore published 726 days after the deadline.

The Commission does not provide a formal explanation. Its methodology confirms that important elements of the assessment occurred after the deadline. A meeting with Member State law-enforcement experts was held in November 2024, while the results of the Commission's questionnaire were discussed with the EU FIUs' Platform in June 2025.

The evidential basis is limited. The Article 21(3) assessment draws on 16 FIUs, 19 law-enforcement agencies and 13 Member States, rather than all 26 Member States bound by the Directive. It does not provide a comprehensive comparison of response times, refusals, investigative outcomes, prosecutions, costs or the frequency with which FIU information had to be reacquired as evidence.

Article 19 requires annual statistics on searches, requests, response times and, where available, outcomes and costs. Their absence from a consolidated presentation makes it difficult to assess how representative the conclusions are.[12]

The Commission's caution may be substantively justified. The evidence presented is not, however, sufficiently comprehensive to close the policy question.

Two different future reviews

The next periodic implementation report under Article 21(1) falls due by 2 August 2027. That should be distinguished from Article 21(5), which requires a fuller evaluation of the Directive—including how Charter rights and principles have been respected—"no sooner than" 2 August 2027. Article 21(5) establishes the earliest date for that evaluation rather than an express deadline by which it must be completed.

The Commission will need to decide whether to publish the 2027 periodic report separately, combine it with the broader Article 21(5) evaluation or rationalise the overlapping exercises.

How this plays out in practice: a worked example

The scenario. A prosecutor in one Member State is investigating an alleged fraud network. Using the interconnected registers, the authority establishes that the suspect holds a payment account with the German subsidiary of a group headquartered outside the EU, a securities account with an affiliate in a second Member State, and a crypto-asset account with a group CASP in a third. Three requests follow within a fortnight: a register enquiry, a request through the German FIU, and a European Investigation Order served on the German entity seeking eighteen months of transaction records.

Where it breaks. The payment-account data sits in one platform and the crypto-asset records in another, with no common customer identifier, so the firm cannot confirm that all three relationships belong to the same person without manual reconciliation. The eighteen-month period reaches into an archived system from which extraction takes weeks rather than days. The securities account falls outside the Article 6a format, so that entity produces spreadsheets while the German entity produces structured data. Privilege review of internal investigation material has not begun. The group's non-EU parent holds some of the relevant records, raising a conflict between the production order and local secrecy rules. Each response is drafted by a different team, and the transaction populations do not match.

[12]Directive (EU) 2019/1153, art 19(3)-(4).

The consequence. None of these difficulties necessarily establishes a breach in isolation. Together, however, they can produce a slow and inconsistent response that invites broader scrutiny of the group's systems and controls. The remainder of this alert explains how to close those gaps before a request arrives.

2. The emerging EU financial-crime data architecture

The principal significance of the report lies in how Directive 2019/1153 fits into a wider system. That system can be understood as five connected layers.

- **Layer 1: creation and retention of information:** The AML Regulation and related sectoral legislation determine what information obliged entities must collect, verify, monitor and retain. This includes customer identity, beneficial ownership, account relationships, transaction information and suspicious activity.

- **Layer 2: financial intelligence:** National FIUs receive suspicious transaction reports and other information, conduct operational and strategic analysis and exchange information with domestic and foreign counterparts. AMLA will support FIU cooperation, joint analysis and convergence without replacing national FIUs.

- **Layer 3: account discovery and transaction tracing:** National centralised registers allow authorised authorities to identify where relevant accounts are held. BARIS will interconnect national mechanisms. Article 6a will establish a common structured format for specified payment-account and IBAN-based bank-account operations and transfers of crypto-assets when requested during criminal investigations.

- **Layer 4: investigation and evidence:** National law-enforcement authorities, prosecutors, Europol and judicial-cooperation mechanisms use financial intelligence to identify suspects, build cases and obtain evidence. EPPO, Eurojust and OLAF may also become involved within their respective criminal, judicial-coordination and administrative-investigation mandates.

- **Layer 5: asset recovery:** Asset Recovery Offices[13] and judicial authorities trace, freeze, manage and confiscate criminal proceeds and other relevant property.

The architecture therefore follows a connected sequence: *create the data → identify suspicion → locate the account → reconstruct the transactions → establish the network → preserve the evidence → trace and recover the assets.*

The EU has historically regulated these stages through separate instruments and institutions. The direction of travel is towards greater technical and operational interconnection. That may improve enforcement. It also increases the importance of access controls, data quality, purpose limitation and remedies. Errors or unsupported associations can travel further and faster through an interconnected system than through isolated national processes.

[13] AROs are the national authorities that each Member State must establish under Article 5 of Directive (EU) 2024/1260 on asset recovery and confiscation (replacing Council Decision 2007/845/EC) to trace and identify criminal proceeds and instrumentalities, and to cooperate and exchange information with their counterparts in other Member States and with Union bodies.

3. What the Commission found—and what it deferred

The Commission concludes that Directive 2019/1153 has materially improved the ability of law-enforcement authorities to identify accounts and obtain financial intelligence. Direct access to national bank-account registers is particularly valuable. It avoids the need to approach multiple institutions merely to determine whether a person holds an account.

Account-identification information must be distinguished from transaction data. A central register identifies matters such as the holder, representative, beneficial owner, account or IBAN, maintaining institution and opening or closing date. Detailed transactions must still be obtained through the applicable FIU, law-enforcement, prosecutorial or judicial channel.

Europol made more than 160 requests under the Directive in 2023 and 2024, with an approximately 75% response rate. The information helped identify suspects, connections, financial circuits and assets, but an average response delay of around 50 days impaired some cross-border investigations.

Uneven implementation

The Commission identifies deficiencies in national implementation, including: (i) incomplete requirements concerning staff confidentiality, integrity, skills and training; (ii) inadequate technical and organisational safeguards; (iii) incomplete logging of access and searches; (iv) incorrect retention periods; (v) insufficient controls for processing sensitive personal data; and (vi) incomplete records of exchanges between FIUs and competent authorities.

In some Member States, safeguards were followed in practice without being stated expressly in national law. The Commission reserves the possibility of enforcement action but does not identify individual Member States against particular shortcomings.

Wider access remains unresolved

Article 21(3) asked whether law-enforcement authorities should gain access to a broader category of information held by public authorities or obliged entities. More than two-thirds of consulted law-enforcement authorities favoured earlier direct exchanges, particularly at the pre-investigative stage when information may be needed to establish whether a formal investigation is justified.

Cross-border procedures add delay: recognition of a European Investigation Order may take up to 30 days, while funds can move in seconds. Other authorities preferred to preserve the FIU's role in protecting confidentiality, filtering information, limiting unnecessary disclosure and maintaining the distinction between intelligence and evidence.

The Commission consequently concludes that it is too early to determine whether extending the definition of financial information is necessary and proportionate. This is a deferral rather than a rejection. If BARIS, common formats, AMLA and the strengthened asset-recovery framework do not resolve the identified delays, pressure for broader access is likely to return.

4. Faster access, fragmented law: why one response process will not work

The report reveals a second and less obvious development. The EU is seeking to accelerate financial-information exchange by layering newer instruments over rules that it has not yet consolidated. Directive

2019/1153 now interacts with: (i) the new AML Directive[14]; (ii) Directive (EU) 2023/977 on exchanges of information between Member State law-enforcement authorities[15]; (iii) the Asset Recovery and Confiscation Directive[16]; (iv) the Europol framework; (v) the European Investigation Order regime[17]; (vi) the GDPR i.e., the General Data Protection Regulation; (vii) the Law Enforcement Directive[18]; and (viii) national criminal-procedure and professional-secrecy rules. These instruments do not always use the same authorities, channels, time limits, logging duties or safeguards.

Directive 2023/977 and separate information channels

Directive 2023/977 establishes organisational and procedural rules for exchanges between Member State law-enforcement authorities, including single points of contact, secure electronic case-management systems and response deadlines.

Financial information and FIU analysis exchanged under the specialist financial-intelligence regime remain subject to a different set of rules. Directive 2019/1153 does not impose equivalent time limits for all cross-border exchanges or ensure consistently that Member State single points of contact are aware of them.

An investigative file often combines financial information with other intelligence and evidence. Splitting one case across different legal and communications channels may therefore recreate the delay that the framework is intended to remove.

Newer AML rules overtake parts of the 2019 framework

The new AML Directive goes further than Directive 2019/1153 in several respects. It provides for: (a) direct or indirect FIU access to law-enforcement information, with direct access encouraged where possible; (b) FIU responses to a broader range of relevant public authorities; (c) FIU powers to obtain information from obliged entities even where no prior suspicious transaction report has been filed; (d) feedback by competent authorities; (e) more developed cross-border cooperation; (f) clearer consent rules for further dissemination; and (g) one-working-day responses between FIUs in exceptional and urgent cases.

The one-working-day FIU response rule in exceptional and urgent cases addresses much of the issue assessed under Article 21(4) and is not confined in the same way to terrorism or associated organised crime.

The newer framework may therefore solve some of the deficiencies of the 2019 Directive. It may also produce uncertainty about which instrument should govern a particular exchange.

More specific is not always more protective

Directive 2019/1153 contains detailed requirements concerning staff training, logging, record-keeping and sensitive personal data. Some newer EU instruments governing comparable information exchanges are less prescriptive or rely on different case-management controls.

The Commission presents this as an opportunity to “stress test” the acquis and reduce unnecessary administrative burdens. Care is needed. Removing duplicated records may be simplification. Removing the record

---

[14]Directive (EU) 2024/1640 [2024] OJ L 2024/1640 (**AMLD6**), generally to be transposed by 10 July 2027.
[15]Directive (EU) 2023/977 [2023] OJ L 134/1 establishes single points of contact, secure case-management systems and deadlines for police-to-police exchanges.
[16]Directive (EU) 2024/1260 [2024] OJ L 2024/1260, to be transposed by 23 November 2026, strengthens tracing, freezing, asset management and confiscation.
[17]Directive 2014/41/EU [2014] OJ L 130/1 provides the judicial-cooperation route for obtaining evidence, including banking and financial records, through another Member State.
[18]Directive (EU) 2016/680 [2016] OJ L 119/89 governs law-enforcement processing; a firm's own disclosure generally remains subject to the GDPR and applicable confidentiality rules.

that allows an individual or supervisory authority to establish who accessed sensitive financial information, when and why would be a reduction in accountability.

The appropriate objective is therefore not simply fewer requirements. It is a coherent allocation of controls across the complete information lifecycle. However, ***the emerging paradox is clear*****:** the data architecture is becoming more integrated while the legal architecture risks becoming more fragmented.

5. Article 6a and the common transaction-record format

The Report states that the Commission plans to adopt an Article 6a implementing act during 2026. As at 29 August 2026, that act remains planned rather than adopted. The Article 6a amendments are generally to be transposed by 10 July 2027.

What Article 6a covers

Article 6a requires Member States to ensure that credit institutions and financial institutions, expressly including CASPs, comply with the prescribed technical specifications when responding under national law to requests: (i) issued by competent authorities; (ii) as part of a criminal investigation; and (iii) including investigations concerning the identification, tracing and freezing of related assets.

For these purposes, “transaction records” comprise: (a) operations carried out during a defined period through a specified payment account; (b) operations through a bank account identified by IBAN; and (c) details of transfers of crypto-assets. The definition does not presently extend to securities or custody transactions generally.

What Article 6a does not do

Article 6a does not harmonise the substantive or procedural power to request the records. National law continues to determine: (1) the authority entitled to issue the request; (2) the threshold for doing so; (3) whether judicial or prosecutorial authorisation is required; (4) the relevant production period; (5) available protections and grounds of challenge; and (6) how the material may be used in proceedings.

The implementing act should therefore harmonise technical production without creating an EU-wide production order.

Why the format matters

- **The problem today.** Authorities currently receive combinations of account statements, spreadsheets, PDFs, payment messages, institution-specific exports and scanned documents. Different field definitions and formats make it difficult to combine information from multiple institutions and jurisdictions.

- **What a common format may deliver.** Structured records should allow authorities to ingest and combine data, identify counterparties, map payment networks, trace layering, compare fiat and crypto-asset flows and reduce manual reconciliation. Any automated validation will depend on the final technical specifications.

- **What this requires of firms' data.** Structured production is likely to require reliable links among customers, beneficial owners, accounts, transactions, payment messages, counterparties, wallet addresses, monitoring alerts and supporting documents.

- **What to do before the specifications are final.** Firms can already map likely fields and authoritative systems, test historical retrieval, reconcile identifiers, validate timestamps and currencies, assess

virtual-IBAN and correspondent-banking data, document transformations and allocate remediation ownership.

6. BARIS, AMLA and the expanding asset-recovery chain

The 2024 AML package changes both the information available to authorities and the institutional structure through which it is exchanged.[19] The new AML Directive requires Member States to maintain centralised automated mechanisms capable of identifying holders or controllers of: (i) bank accounts; (ii) payment accounts, including virtual IBANs; (iii) securities accounts; (iv) crypto-asset accounts; and (v) safe-deposit boxes.

Those national systems are to be interconnected through BARIS by 10 July 2029. BARIS is intended to allow authorised authorities to identify whether a person holds or controls a relevant account in another Member State. It is not designed as a central EU database of every transaction. Once an account relationship is identified, detailed records must still be obtained through an appropriate legal channel.

Directive (EU) 2024/1654 amended Directive 2019/1153 to facilitate use of transaction records and access through BARIS. Article 6a is generally subject to the 10 July 2027 transposition deadline; the BARIS access provisions follow the 10 July 2029 timetable.[20]

AMLA adds an EU-level coordinating layer. It will support FIU cooperation and joint analysis and, from 2028, begin direct supervision of selected high-risk cross-border financial-sector entities. National FIUs and supervisors remain central to the system; AMLA supplements rather than replaces them.

The Asset Recovery and Confiscation Directive completes the enforcement chain by strengthening arrangements for tracing, freezing, managing and confiscating criminal property. Member States are required to transpose it by 23 November 2026.

The architecture also interacts increasingly with enforcement of EU restrictive measures. Directive (EU) 2024/1226 establishes minimum criminal offences and penalties for violations of Union restrictive measures, including certain circumvention conduct. Financial information may therefore be used not only to identify proceeds of conventional predicate offences, but also to trace frozen assets, ownership structures and payment arrangements relevant to sanctions investigations.

The wider EU enforcement network

Europol is the principal EU law-enforcement body addressed directly by Directive 2019/1153. Other EU bodies may also become involved:

- **EPPO** investigates and prosecutes offences affecting the EU's financial interests within its mandate;
- **Eurojust** supports coordination between national judicial authorities, including the resolution of conflicts and execution of judicial-cooperation measures; and
- **OLAF** conducts administrative investigations into fraud, corruption and misconduct affecting EU financial interests.

[19]Regulation (EU) 2024/1624; Directive (EU) 2024/1640; and Regulation (EU) 2024/1620. On the powers of FIUs and cooperation between them, see in particular Directive (EU) 2024/1640, arts 21, 22, 31 and 34.
[20]Directive (EU) 2019/1153, as amended by Directive (EU) 2024/1654, arts 2(7a) and 6a.

Their legal powers and access routes differ. Firms should avoid treating an inquiry from an EU institution or body as if it followed a single standard EU process.

7. Crypto-assets remain the weakest cross-border link

The report expressly identifies difficulties obtaining information from third-country virtual asset service providers offering services into the EU. Several Member States reported failures or delays in responding to law-enforcement requests. This matters because crypto-assets are used not only in cybercrime but increasingly in fraud, drug trafficking, migrant smuggling, sanctions evasion, ransomware, terrorist financing and wider laundering structures.

The EU response combines MiCAR authorisation, the crypto-asset travel rule, AML obligations for CASPs, crypto-asset account identification, FIU and AMLA cooperation, the Article 6a format and stronger tracing and seizure powers.

These measures should improve information available from authorised EU CASPs. They do not fully resolve the problem of an offshore provider that operates without effective EU authorisation, lacks a meaningful EU establishment or refuses to cooperate with EU authorities. The enforcement perimeter consequently remains wider than the regulatory perimeter.

CASPs and other firms should be able to produce wallet addresses, transaction hashes, network information, hosted or unhosted wallet status, originator and beneficiary information, travel-rule data, fiat conversion records and relevant attribution analysis. The methodology and limitations of blockchain-analytics tools should be recorded.

Blockchain activity may be visible, but attribution is not always conclusive. Firms should distinguish verified customer and account information from probabilistic inferences generated by analytics providers.

8. Faster access must remain legally defensible

The case for faster information exchange does not remove the need for legal safeguards. Financial transaction information can reveal political, religious and trade-union affiliations, medical treatment, family relationships, travel, professional advisers, commercial strategy and other sensitive aspects of private life.

A defensible framework must distinguish between:

- establishing whether an account exists;
- accessing account-holder and beneficial-owner information;
- obtaining transaction histories;
- conducting network analysis;
- receiving FIU intelligence; and
- using information as evidence.

Intelligence does not automatically become evidence

FIUs analyse suspicious facts and financial patterns. They do not ordinarily determine whether a criminal offence has been committed. Information disseminated by an FIU does not automatically become admissible evidence. Limitations may arise from:

- national procedural law;
- restrictions imposed by the supplying FIU;
- consent conditions attached to a cross-border exchange;
- the provenance and verification of the information; or
- the need to obtain the underlying primary records separately.

Investigators may therefore need to reacquire information through an evidential procedure. This adds time but protects the distinction between an analytical lead and proof capable of being tested in court.

Privilege and professional secrecy

Authority requests may capture communications with counsel, internal-investigation material and documents created for litigation or regulatory defence. The policy question also extends beyond financial institutions because obliged entities include lawyers, notaries, auditors, accountants, tax advisers and trust or company service providers, subject to applicable conditions and exemptions.

Any future extension of access to information held by obliged entities would need to preserve legal professional privilege, professional secrecy and protections applicable where professionals ascertain a client's legal position or represent a client in proceedings.

Institutions should identify and segregate potentially privileged material, apply the relevant national rules, record any withholding or redaction, manage jurisdictional differences and prevent inadvertent waiver through parallel production.

What firms can and cannot be required to produce

Firms should not obstruct lawful investigations. They should nevertheless be able to seek clarification or challenge a request where: (1) the requesting authority lacks jurisdiction; (2) the legal basis is unclear; (3) the requested period or population is excessive; (4) the information is not relevant to the stated purpose; (5) production would breach another applicable legal obligation; (6) privilege has not been addressed; (7) the requested deadline is technically impossible; or (8) secure transmission arrangements are inadequate.

Any challenge should be prompt, evidence-based and directed towards agreeing a lawful and workable production rather than delaying the investigation.

Public-private partnerships

Public-private financial-information partnerships can help banks, CASPs, FIUs and law-enforcement authorities identify networks that no participant sees alone. Their governance should address legal basis, permitted information, purpose limitation, tipping-off, onward use, data quality, retention, correction and the boundary between typology sharing and operational case information.

The EU has not yet created a fully harmonised legal framework for operational public-private information sharing. Cross-border groups must therefore account for differing national models.

9. One customer, many proceedings: why you need a single matter file

A single transaction pattern can generate parallel: (i) FIU analysis; (ii) AML supervisory review; (iii) prudential investigation; (iv) criminal proceedings; (v) sanctions inquiry; (vi) tax or customs investigation; (vii) EPPO or OLAF involvement; (viii) internal investigation; and (ix) civil litigation.

The principal institutional risk is inconsistent production: different teams may use different datasets, transaction populations, factual descriptions, counterparty attributions or privilege decisions, leaving one submission irreconcilable with another.

Institutions should establish a central matter architecture comprising:

1. **a verified factual chronology** recording events, decisions and communications;
2. **a source-of-truth dataset** identifying the authoritative account, customer and transaction records;
3. **a legal-basis and jurisdiction map** recording the power, purpose and scope of each request;
4. **a privilege and confidentiality protocol** distinguishing producible, restricted and review-pending material;
5. **a production log** showing what was supplied, to whom, when and in which format;
6. **jurisdiction-specific disclosure streams** recognising differences in procedural law and onward use; and
7. **governance over inconsistencies** requiring differences between submissions to be identified, explained and approved.

This structure supports both cooperation with authorities and defensible challenge where requests overlap, conflict or exceed the applicable legal basis.

10. Implementation timeline

Date	Development	Practical relevance
During 2026	Commission plans Article 6a implementing act	Electronic structured format and technical means for specified bank/payment-account operations and crypto-asset transfers
23 November 2026	Asset Recovery and Confiscation Directive transposition deadline	Stronger tracing, freezing, management and confiscation framework
10 July 2027	Article 6a transposition deadline	National implementation of structured production requirements
10 July 2027	General AMLD6 transposition and AMLR application	New AML rulebook, expanded FIU powers and cross-border cooperation
From 2028	AMLA direct supervision expected to begin	Direct supervision of selected high-risk cross-border financial-sector firms
10 July 2029	BARIS access provisions and interconnection	Cross-border identification of covered bank, payment, securities and crypto-asset accounts and safe-deposit boxes

What firms should consider

The actions set out below fall into three distinct categories and it is worth separating them before turning to the detail. Some are obligations that already apply today and require no change. Others are existing obligations that will come under materially greater time and format pressure. A smaller number are capabilities that most firms do not currently have at all. The Commission's report imposes no new production obligations on regulated firms, so this section is not a compliance gap analysis; it identifies where the operating environment, rather than the legal duty, is changing.

Area	Position today	What changes	Category	Owning function(s)	Documentation to revisit
Suspicious transaction reporting	Established duty under the existing AML framework, with procedures already in place.	No change to the reporting duty itself. The AML package expands FIU powers to access, suspend and exchange information based on those reports from 10 July 2027.	No change	MLRO and Compliance	None required; reporting procedures remain fit for purpose.
Tipping-off, privilege and professional secrecy	Existing confidentiality, tipping-off and privilege controls, generally applied on a per-request basis.	The controls remain the same, but information supplied to one authority may be transmitted onward through channels with different safeguards and onward-use limits, raising the consequence of each notification decision.	No change	General Counsel and Legal; MLRO and Compliance	Privilege and confidentiality guidance, to address onward transmission and notification decisions.
Retention, privacy and records management	Existing retention schedules, privacy documentation and records policies, often untested against retrieval of older records.	The obligations are unchanged, but retrievability and reconstruction of historic data become operationally critical rather than a documentary compliance matter.	Greater pressure	CIO, CDO and Data Functions; Operations	Data-retention schedules and records-management policies, tested for retrieval rather than revised.
Responding to FIU and law-enforcement requests	Existing obligation, handled request by request and predominantly involving a narrow set of domestic designated authorities.	A wider requesting population, more cross-border requests and shorter effective timescales, with the same underlying data potentially sought more than once on different legal bases.	Greater pressure	Operations; MLRO and Compliance	Authority-request and production procedures.
Deadline and escalation management	Existing intake, verification and allocation processes, operating against relatively tolerant response timetables.	The Commission identifies average response delays of approximately 50 days as having undermined cross-border investigations, and the direction of travel is towards faster access.	Greater pressure	Operations; Board and senior management	Authority-request and production procedures, including escalation and governance reporting.

		Escalation of unrealistic deadlines and incomplete data becomes a governance matter.			
Structured electronic production	Largely absent. Responses are frequently assembled manually and produced in unstructured or inconsistent formats.	The Commission plans an Article 6a implementing act during 2026 prescribing an electronic structured format and technical means for specified bank and payment-account operations and crypto-asset transfers, together with automated validation.	New capability	CIO, CDO and Data Functions; Procurement and Outsourcing	Regulatory data inventories; outsourcing and data-provider contracts.
Identifier reconciliation across platforms	Partial at best. Identifiers are commonly siloed across customer, account, payment and crypto-asset platforms, with transformation and export logic undocumented.	Structured production and automated validation cannot operate without reconciled identifiers and documented authoritative data fields, converting this from good practice into a technical prerequisite.	New capability	CIO, CDO and Data Functions	Regulatory data inventories, recording authoritative fields and export logic.
Cross-jurisdictional access mapping	Typically mapped only against domestic designated authorities. In Germany the designation is comparatively narrow, covering the Federal Criminal Police Office and the Federal Office of Justice.	BARIS interconnection from 10 July 2029 will allow authorities to identify accounts across borders, and designations in other Member States are considerably broader. There is no single operational answer to who can request the information.	New capability	General Counsel and Legal	Authority-request and production procedures, mapped by entity and jurisdiction.
Reconciliation across parallel proceedings	Requests generally answered on their own terms, with no single verified chronology or source-of-truth dataset spanning matters.	Authorities will expect information to be complete, consistent and reconcilable across FIU, supervisory, criminal, sanctions and judicial proceedings, requiring governance over inconsistencies between submissions.	New capability	Investigations and Forensics; General Counsel and Legal	Internal-investigation protocols; sanctions-investigation procedures.

What this may mean for each function:

- **General Counsel and Legal.** Map authority access and challenge rights by entity and jurisdiction; govern parallel investigations, privilege and cross-border production; identify legal conflicts; and test contractual access to third-party data.

- **MLRO and Compliance.** Reconcile STR, FIU and law-enforcement procedures; record dissemination restrictions; identify notification triggers; govern public-private information sharing; and link monitoring alerts to source records.

- **Investigations and Forensics.** Maintain the central matter file, preserve evidence and chain of custody, validate transaction populations and counterparties, and record the limits of analytical attribution.

- **CIO, CDO and Data Functions.** Map authoritative fields, test historical retrieval, reconcile identifiers, document transformations and prepare for structured production.

- **Operations.** Test intake, verification, allocation, deadline management, four-eyes review, secure transmission and escalation of incomplete data or unrealistic deadlines.

- **Procurement and Outsourcing.** Review access, audit, portability, preservation and assistance clauses; confirm access to archived and sub-processor data; and allocate responsibility for late or incomplete records.

- **Board and senior management.** Monitor request volumes, overdue productions and material data gaps; oversee remediation; and ensure sufficient legal, compliance, forensic and technology resources.

Distinguishing request types

Whichever documents are revisited, authority-request and production procedures should distinguish clearly between (i) an FIU request; (ii) a supervisory request; (iii) a law-enforcement inquiry; (iv) a prosecutorial or judicial order; (v) a cross-border request; (vi) an EPPO, Eurojust or OLAF interaction; (vii) a public-private information exchange; and (viii) a voluntary disclosure.

As set out above, these categories may concern the same underlying transaction while engaging different legal bases, safeguards, deadlines and permitted uses, and the basis relied on should be recorded in each case.

Non-EU headquartered groups: four questions to resolve early

- **Which entity is in scope?** Article 6a applies to the EU-established credit institution, financial institution or CASP rather than the group as such. Groups should identify the entity receiving the request and the systems it can lawfully and practically access.

- **Where does the data actually sit?** Where records are held outside the EU or by a group service company, the EU entity needs timely legal and operational access. Intra-group agreements, access rights and retention arrangements should be tested rather than assumed.

- **What happens when laws conflict?** EU production duties may conflict with third-country secrecy, localisation or blocking rules. Foreseeable conflicts should be analysed with local counsel before a request arrives.

- **Who coordinates the response?** Groups should allocate ownership of the group response, establish one verified dataset and require approval of differences between entity-level submissions.

- **A note on outsourcing and ICT arrangements.** DORA contract reviews should also test whether cloud, platform, processor, archive and analytics providers can extract complete, structured and historic data, including from sub-processors, on short notice.

Outlook

The Report is formally an implementation review but substantively a holding position while the EU completes a more integrated financial-intelligence and asset-recovery architecture.

The Commission accepts that the existing framework remains slow and fragmented and that authorities do not always have the technical capacity to process the information they receive.

Rather than widening direct access now, the EU is first connecting account registers, standardising covered transaction records, strengthening FIUs and AMLA cooperation, and improving asset tracing and recovery.

That sequencing is defensible: the EU should determine whether existing information can be accessed and used effectively before opening wider categories of sensitive data to law enforcement.

The delay remains significant. After taking almost two additional years, the Commission has deferred the Article 21(3) question on evidence from only half of the affected Member States.

For firms, the direction is clearer. Account and transaction data should become more standardised, interconnected and operationally important, increasing the need for rapid and reconcilable production across products, systems and jurisdictions.

The technology may integrate faster than the law. Account discovery, production, FIU analysis, police exchange, judicial evidence and asset recovery remain governed by overlapping instruments and national procedures.

The next phase of EU financial-crime policy will turn on how quickly authorities can follow the money and convert intelligence into effective action while preserving privilege, proportionality, data protection and the safeguards separating investigation from surveillance.

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 multiple thousands of 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

Dr. Hagen Weiss
Tel: +49 1511 5708446
hagen.weiss@pwc.com

Fabian Joshua Schmidt, LL.M.
Tel: +49 151 41490437
fabian.joshua.schmidt@pwc.com

EU RegCORE Team
de_regcore@pwc.com

www.pwc.de