



SEPA Instant: Balancing Speed and Compliance in Real Time

AMLYZE

**Practical Implementation
Guide**

The background of the page features a dark blue gradient with several glowing, stylized currency symbols. These include a large Euro symbol (€) in the lower left, a large Dollar symbol (\$) in the upper center, and a large Rupee symbol (₹) in the upper right. Other smaller symbols like the Pound (£), Dollar (\$), and Rupee (₹) are scattered throughout the background, creating a financial theme.

Table of Contents

1. Introduction
2. PART I. I. Verification of Payee: A Useful but Limited Tool
3. PART I. II. Sanctions Screening: Relief and New Pressures
4. PART I. III. Navigating the Compliance Twilight Zone
5. PART II. STEP 1. Approaching the Twilight Zone of SEPA Instant
6. PART II. STEP 2. Adapt to Transaction Screening Requirements
7. PART II. STEP 3. Adapt to "Immediate" Screening Requirements
8. Summary: Balancing Speed, Compliance, and Judgment

Introduction

Speed of payments has become a defining feature of the modern financial ecosystem. Consumers expect speed, convenience, and seamless execution.

Yet for financial institutions, regulators, and compliance teams, the shift to “instant” payments creates a new operational paradox: how to reconcile the promise of real-time execution with the immovable demands of financial crime prevention, sanctions compliance, and systemic resilience.

The recent amendments to the EU regulation on credit transfers in euro – commonly referred to as the **Instant Payments Regulation (IPR)** – mark a major turning point for the regulator itself that is actively nudging the penetration of speed and convenience into the market. What was once a voluntary track under SEPA Instant is now a compulsory sprint: euro transfers must clear **within 10 seconds, 24/7/365**, and at no higher cost than standard transfers. Regulators have effectively fired the starting pistol, leaving institutions to run a race where the rules of speed and the rules of compliance often point in opposite directions.

And here enters the black sheep of financial crime compliance: false positives. Each unnecessary hit consumes precious seconds, gums up operational gears, and risks eroding customer trust when legitimate transactions are blocked. In a world where every second counts, the “crying wolf” of false positives is more than an annoyance — it’s a structural flaw. The regulatory framework adds another twist.

On one hand, IPR relieves institutions of the need to screen during the SEPA Instant transaction execution the payer and payee against targeted financial sanctions. On the other hand, it leaves broad grey zones around other screening processes and financial crime controls. The result is a familiar regulatory conundrum: balancing customer convenience against financial crime prevention. Only now, the scale is tilted further — the expectations for speed and user convenience have never been stricter, while the expectations for compliance have not eased up.

This guide is structured in two parts:

- ☐ *the 1st provides a short overview of the main requirements relevant to financial crime prevention;*
- ☐ *while the 2nd offers a deeper dive into practical implementation.*

Eglė Kontautaitė

Eglė Kontautaitė, Head of Client Solutions, AMLYZE

About The Author



Eglė is an anti-money laundering expert with hands-on experience in customer supervision and money laundering risk management in the context of financial institutions inspections.

Expertise in supervision

She has more than 13 years of experience in supervising financial market participants at the Bank of Lithuania, where her last position was Head of the Money Laundering Prevention Division.

Authority in AML/CFT world

She represented the Lithuanian delegation during the Moneyval assessment of the country's AML/CFT framework.

A hand holding a smartphone, with a payment card (Visa) overlaid on the screen. The background is a blue gradient with geometric patterns and a grid of small squares and circles.

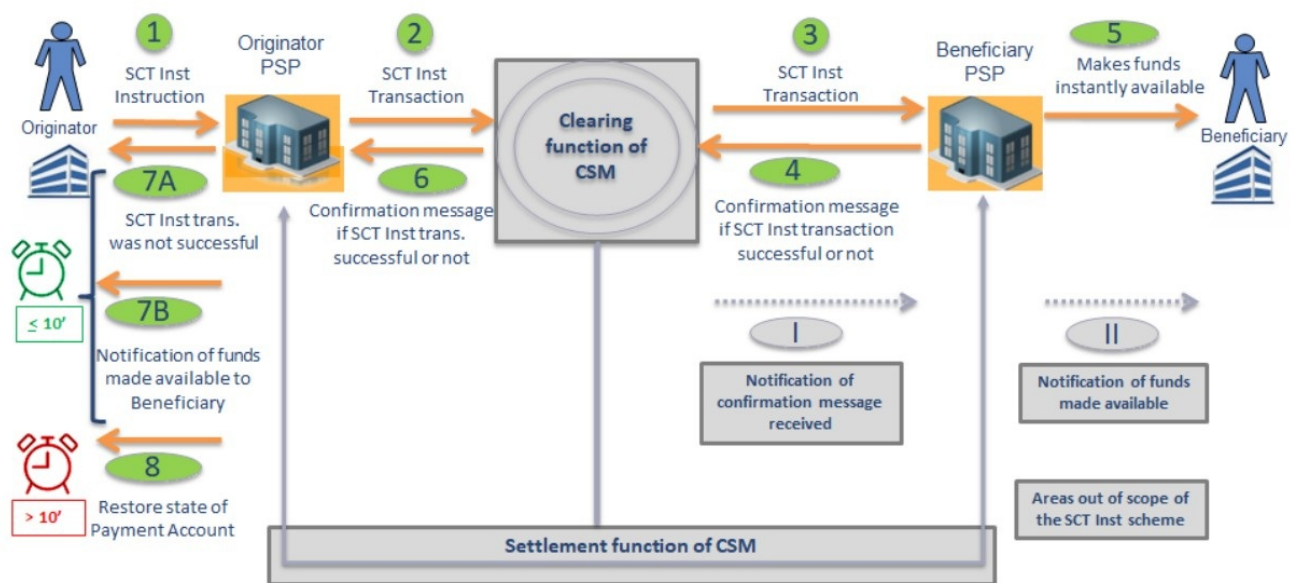
"Just as the circulatory system supplies the human body with nutrients and oxygen, an efficient, secure and moreover, highly available payment infrastructure ensures the frictionless movement of goods, services and capital throughout Europe."

European Central Bank (ECB) on payments and market infrastructure. Source: ECB

PART I: Key Regulatory Requirements and Emerging Challenges

SEPA Instant is not a newcomer to the payments landscape. For years, it operated under a self-regulatory regime shaped by the European Payments Council Rulebook. What was once voluntary, however, is now mandatory: speed (within 10 seconds) execution (24/7/365) and transactional flow.

The essential SEPA Instant flow, as defined by the Rulebook, is illustrated in the picture below. Yet while the flow itself looks straightforward on paper, the real challenge lies in what sits behind it – the compliance implications. In the sections that follow, we will shift the focus away from the technical sequence of steps and instead examine the practical consequences it creates for financial crime prevention.



Conceptual work flow of an SCT Instant. Source: European Payments Council, SEPA Instant Credit Transfer Scheme Rulebook, 2025 Version 1.0

I. Verification of Payee: A Useful but Limited Tool

Payment service providers offering SEPA Instant are now required to implement **Verification of Payee (VoP)** services, which inform the payer instantly if the beneficiary's IBAN does not match the name provided. This measure is intended to help reduce the risk of fraud. Already tested in the Netherlands, VoP reduces fraud but is no cure-all.

Fraud schemes evolve faster than regulation, and the IPR introduces no further fraud safeguards (unlike the upcoming **EU Payment Services Regulation**).

As the [EBA Opinion highlights](#):

“Instant payments, executed in 10 seconds, 24/7, present challenges for effective transaction monitoring”

EBA Opinion of the European Banking Authority on money laundering and terrorist financing risks affecting the EU’s financial sector

In other words, regulators are essentially challenging regulators: the very speed requirements meant to modernize payments can limit the ability to detect fraud or money laundering in real time. The Opinion explains that AML/CTF and fraud prevention techniques may be hindered because the speed of execution reduces the effectiveness of monitoring and complicates ex ante risk-based oversight.

This underscores that while tools like VoP are valuable, they cannot fully substitute for broader fraud detection and AML/CTF measures in a real-time payments environment.

II. Sanctions Screening: Relief and New Pressures

Two key shifts redefine sanctions compliance under IPR:

1. Immediate dataset updates

PSPs must verify users **immediately** after EU restrictive measures are adopted or amended, and at least daily.

Do not be deceived by the seemingly minor wording nuance - the insertion of the term “immediately” has caused significant turbulence in the market. As later clarified by the [European Commission in its FAQs](#), the policy intent behind this term is to set a stricter expectation regarding the permissible time gap between updates to restrictive measures and the operational execution of sanctions screening.

The choice of “immediately” - rather than “as soon as possible” or “without undue delay” - establishes a far higher compliance threshold. Payment service providers that fail to manage this gap effectively risk not only penalties under the Instant Payments Regulation, but also potential liability for financial damages claimed by a counterparty Payment service provider involved in the same transaction.

2. Removal of transaction screening obligation

Additionally, the Instant Payments Regulation introduces a major shift in payment screening practices. When executing an instant credit transfer, neither the payer's nor the payee's payment service provider is required to verify whether the parties involved are persons or entities subject to targeted financial restrictive measures.

This relief was based on three premises:

1. speed of execution of transaction;
2. poor performance of transaction screening (with **99.8% false positives**, as per the European Commission);
3. trust in institutions and supervisors to implement sanctions effectively.

When the Instant Payments Regulation was still under discussion, Eric Ducoulombier, the European Commission's Head for Retail Finance at the time, commented on the effectiveness of sanctions screening systems:



“Currently the system of transaction screening gives rise to millions of aborted or rejected instant transactions, because software has signalled that there is a possibility that one of the people involved in the transaction might be covered by the sanctions list. And of course, the bank has to verify whether it is the case. And we know (because we have all the figures) that in 99.8% of cases it turned out to be a false alarm.”

Eric Ducoulombier, the European Commission's Head for Retail Finance. Source: EU Finance Podcast

This quote clearly demonstrates the headaches surrounding SEPA Instant and the way the European Commission attempted to address them.

III. Navigating the Compliance Twilight Zone

Regulations often use the phrase “**without prejudice**” to address one area while deliberately leaving another unspoken, creating what I like to call a “twilight zone” of uncertainty. The IPR is a prime example. It relieves the market from screening instant transactions against EU targeted financial sanctions to preserve speed, yet it explicitly excludes any obligations related to other restrictive measures or AML/CFT actions.

This leaves financial institutions with several pressing questions:

- **National sanctions:** EU Member States maintain their own national restrictions, often aimed at fighting terrorism or to preserve national security (going beyond EU common foreign and security policy). How should PSPs incorporate these into instant payments?
- **Extraterritorial sanctions:** Some countries apply their sanctions policies extraterritorially, leveraging their political and economic weight. For compliance teams, this raises a difficult question: should SEPA Instant transactions also be screened against, for example, U.S. sanctions lists (SDN and non-SDN)? After all, even though SEPA Instant is an internal EU system (unlike SWIFT payments), no financial institution wants to risk falling within OFAC’s reach by opting not to screen against U.S. designated persons. Ultimately, it becomes a matter of risk appetite - but a very uncomfortable one.
- **Payment purpose screening:** Certain EU supervisors (e.g., Lithuania) along with [EBA Guidelines](#) on internal policies, procedures, and controls to ensure the implementation of both Union and national restrictive measures require payment purpose checks. Historically, these checks generate more false positives than counterparty screening. Altogether these checks consume time, creating tension with SEPA Instant’s 10-second execution mandate.
- **Sectoral sanctions and supervisory expectations:** Unlike targeted sanctions, sectoral sanctions restrict broader sectors or transaction types. PSPs are expected to enforce these, even in real time, which often conflicts with the operational demands of instant payments. In above mentioned EBA opinion SEPA Instant was explicitly mentioned as an additional challenge in “the screening of SEPA instant credit transfers, which may expose PSPs to a heightened risk of breaching restrictive measures that are not targeted financial sanctions – such as sectoral sanctions.”

As the EBA highlights - and as a few national supervisory authorities already strictly impose - financial institutions are expected to act as gatekeepers for the application of sectoral sanctions. This raises an important question: how does such an expectation align with the speed and execution requirements of EU internal market instant payments?

- **AML/CFT requirements:** AML/CFT rules require freezing funds and reporting suspicious activities to local FIUs. But how does that reconcile with the Instant Payments Regulation's strict 10-second execution requirement? If a transaction triggers a red flag, should it be rejected in order to comply with the Instant Payments Regulation? And if so, would that breach AML/CFT obligations, which require freezing the funds and filing a report instead?

If you're already feeling the stress of this compliance puzzle, don't worry — the guide that follows will provide practical recommendations for addressing each of these challenges. Stay with me, and we'll navigate this complex terrain together.

PART II: Adapting to New Regulatory Reality

By following this guide, you will gain actionable insights to implement compliant, efficient, and risk-conscious SEPA Instant operations without losing sight of customer experience. Follow the trail of thoughts, but always apply your own judgment and approach each insight with a constructive, critical eye.

STEP 1. Approaching The Twilight Zone of SEPA Instant: When AML/CFT Compliance Meets Instant Execution, What Prevails?

The SEPA Instant rulebook is not new, but its enforcement has shifted. The European Payments Council issued guidance on SEPA Instant some time ago, but this guidance was applied with a degree of flexibility across the industry. In practice, regulatory frameworks such as AML/CFT, and sanctions enforcement have always taken precedence. These frameworks are (or should I say “were”?) superior legislative acts. When their requirements clashed with SEPA Instant rules - particularly regarding speed and execution - AML/CFT considerations prevailed.

In high-risk scenarios, the strict 10-second execution requirement of SEPA Instant **Rulebook** was not always observed. Payments could be paused or frozen mid-transit to allow further examination of the origin and destination of funds. These practices were firmly grounded in EU AML/CFT regulations, which require obliged entities to refrain from executing suspicious transactions until reporting obligations are fulfilled. While the 10-second execution rule applied in most non-suspicious cases, any transaction flagged as potentially suspicious was intercepted by ex-ante monitoring rules and frozen while additional AML/CFT and fraud checks were performed. Institutions therefore had to balance adherence to instant execution requirements against the need to prioritize financial crime prevention where risks were too high.

With the entry into force of the Instant Payments **Regulation**, this balancing act has become significantly more challenging. The regulatory framework is directly applicable, with no “comply or explain” flexibility, and no allowance for short delays to complete checks. Instead, institutions must apply a binary approach: if a transaction is flagged as suspicious, the decision must be either to release it - making funds immediately available to the beneficiary- or reject it outright. While redirecting outgoing transactions to the SEPA credit transfer flow may be a practical workaround, incoming payments present a greater challenge. Here, institutions face a stark choice between acceptance and rejection- effectively placing financial crime prevention and customer convenience in opposition, rather than allowing for a balanced approach.

The SEPA Instant Regulation impacts both ex-ante and ex-post transaction monitoring for fraud and ML/TF risk prevention, shifting practices toward ex-post review. While rejecting a transaction remains an available risk management tool, under the new framework, funds cannot be frozen but remain accessible to the sender or receiver - even if the recipient is a criminal actor.

Although the Instant Payments Regulation applies “without prejudice” to PSP actions to comply with Union law on AML/CFT, it provides no clarity on whether a payment service provider may legitimately freeze or delay a transaction flagged by monitoring tools before execution. Some institutions have explored freezing entire accounts rather than individual transactions, but this approach may be more disruptive than a short delay in execution. This raises a broader policy question: did the European Commission intend for ex-ante checks to largely disappear from financial crime compliance, as occurred with the removal of sanctions screening for transactions?

A strict binary approach towards transaction flow - accept or reject - mandated by the SEPA Instant Regulation is incompatible with the AML/CFT regulatory framework, which requires suspicious transactions to be suspended or withheld. AML/CFT obligations extend beyond the immediate payment decision and include:

- Detection of suspicious activity through monitoring;
- Assessment and escalation of alerts, often requiring additional context;
- Reporting of suspicious transactions to the FIU;
- Possibility of freezing or suspending transactions where legally justified.

These steps were not designed to fit within SEPA Instant’s 10-second execution window, creating a fundamental tension: while delaying or freezing transactions is often necessary for AML/CFT compliance, this is not compatible with the SEPA Instant regulation.

To balance these compliance needs, payment service providers will need to rethink their monitoring architecture. Possible adaptations include:

1. **Layered monitoring**, where real-time rules combine ex-ante and ex-post approaches;
2. **Risk-based segmentation**, prioritizing real-time controls for higher-risk scenarios (e.g., cross-border instant transfers, high-value transactions, or known typologies);
3. **Managing transactions monitoring latency**, ensuring that the transaction monitoring system can generate alerts quickly enough to support ex-ante decision-making. In practice, this means vendors must commit to providing tools capable of flagging suspicions within a very short timeframe, giving institutions at least a narrow window to decide on the transaction flow;
4. **Close dialogue with supervisors**, as regulatory guidance is still evolving on whether AML/CFT suspicions can justify non-execution of an instant payment.

Where necessary human availability for alert resolution must be ensured 24/7/365, in line with SEPA Instant's continuous execution, including weekends and holidays.

This human oversight should be integrated into the overall real-time transaction monitoring framework, balancing ex-ante and ex-post controls. Institutions must prioritize alerts and determine which require immediate review and decision-making within the short execution window.

STEP 2. Adapt to Transaction Screening Requirements.

As previously highlighted, the SEPA Instant framework introduced an important regulatory relief by clarifying that payment service providers are not required to conduct transaction-by-transaction screening against EU targeted financial sanctions lists when executing instant credit transfers. However, this regulatory relief is not absolute - payment service providers remain fully responsible for complying with other applicable regulatory obligations.

This creates a delicate balance: on the one hand, ensuring strict adherence to legal and compliance requirements, and on the other, mitigating the risk of increased transaction rejections that may frustrate users and reduce confidence in instant payment services. Addressing the so-called regulatory “grey areas” becomes crucial, as financial institutions must reconcile compliance expectations with the operational and customer-experience challenges posed by the binary nature of SEPA Instant – where the only options are to process or reject a payment.

In order to maintain compliance while operating within this framework, payment service providers should carefully consider several key obligations.

- **Continued duty to observe financial sectoral sanctions.** Under the SEPA Instant framework, EU rules exempt payment service providers from performing payer and payee screening against **EU targeted financial restrictive measures** during the execution of instant credit transfers. The regulation also provides a **narrow, explicit definition** of targeted financial restrictive measures:

“an asset freeze imposed on a person, body or entity, or a prohibition on making funds or economic resources available to such a person, body or entity, directly or indirectly, pursuant to restrictive measures adopted under Article 215 TFEU.”

However, the SEPA Instant Regulation does not address the treatment of other EU sanctions regimes. In particular, **sectoral financial sanctions** - which impose specific restrictions (e.g., on access to capital markets, lending, or certain categories of transactions) but do not amount to asset freezes - fall outside the scope of the exemption. Consequently, these measures might remain subject to **ex-ante transaction screening obligations** for payment service providers, given the inherent risk of breaching international sanctions prohibitions.

In practice, this brings PSPs back to a **binary compliance approach** under the SEPA Instant framework: for sectoral financial sanctions designations will apply **preventive ex-ante screening** and, where a match is identified, manage the risk through outright **transaction rejection** to remain compliant with SEPA Instant regulation.

- **Continued duty to observe national sanctions lists.** A similar approach applies in relation to national sanctions lists, which some Member States maintain in addition to the EU's targeted restrictive measures. These lists often cover persons suspected of involvement in terrorism or individuals considered to pose a national security risk to that particular Member State. The practical challenge for payment service providers is determining the extent to which they should incorporate other Member States' national sanctions lists into their own screening processes.

There are a few catches when it comes to national peculiarities:

1. Some EU Member States (e.g., Lithuania, Estonia, Poland) keep their own lists of persons linked to sanctioned individuals. These aren't national sanctions designations in the strict sense, but local supervisors may treat them as such - so they can feel like an extra layer on top of the EU rules, even if technically they're not.
 2. The neat binary of SEPA Instant - either "execute" or "reject" - doesn't always hold under national sanctions regimes. Local authorities might instead ask you to freeze a transaction once a potential hit pops up (as is the case in Lithuania).
- **Duty to screen specific data fields – payment purpose.** While the SEPA Instant Regulation exempts payment service providers from real-time screening of payer and payee information, it does not relieve them from the obligation to screen other data fields. In particular, several Member States require screening of the payment purpose field, and the European Banking Authority has reinforced this expectation in [EBA Guidelines](#) on internal policies, procedures, and controls to ensure the implementation of both Union and national restrictive measures. Screening of the payment purpose field can serve as a valuable tool in identifying potential sanctions evasion schemes. At the same time, however, market experience shows that this type of screening generates a disproportionately high number of false positives - far exceeding those resulting from payer or payee screening.

Screening of payment purposes might be a good way to indicate sanctions evasion schemes, but at the same time, as market practice shows, creates a huge number of false positives, going far beyond the number of false positives created by payer and payee screening. The option on how to manage the payment purpose screening pitfalls is twofold - making very cautious judgments on parametrisation of payment purpose screening and putting payment screening under the ex-post screening options. Without such adjustments, institutions risk generating a flood of unnecessary rejections - decisions that add little value while undermining both efficiency and customer trust.

Managing these challenges requires careful consideration. Broadly, two approaches are available:

1. applying very cautious and precise judgment when calibrating the parameters of payment purpose screening, to limit unnecessary alerts;
2. tailoring screening parametrization for different payment types (e.g. applying more conservative parametrization for cross-border transactions);
3. shifting certain elements of payment purpose screening to an ex-post control framework, thereby reducing the immediate operational burden while still ensuring compliance oversight.

If you rely on an external screening provider, an additional recommendation would be to request data on the false positive ratio generated by their default parametrisation. This can serve as a valuable benchmark when comparing different vendors.

- **Managing the risks of extraterritorial sanctions application.** As noted previously, one of the challenges for payment service providers is the potential application of sanctions measures on an extraterritorial basis. A prominent example is the U.S. Office of Foreign Assets Control (OFAC), which may impose penalties on an EU-based financial institution for breaching U.S. sanctions, even where no direct legal obligation under EU law exists. To mitigate this risk, some payment service providers opt to expand their screening datasets by including sanctions lists from third countries, such as the U.S., alongside EU and national lists.

The extent to which such measures are implemented ultimately depends on the institution's risk appetite and strategic choices. Payment service providers may decide to screen SEPA Instant transactions against foreign sanctions lists on an ex-ante basis (prior to executing payments) or on an ex-post basis (after execution but subject to monitoring). Both approaches seek to balance regulatory risk management, but one with a better client satisfaction, avoiding unnecessary friction in payment flows (as mentioned previously - rejection of payments). The decision should be based on a careful assessment of the expected volume of false positives and the institution's broader approach to managing exposure to extraterritorial enforcement actions.

- **Screening against EU targeted financial sanctions – should it continue?** The regulatory philosophy of SEPA Instant, which relieves payment service providers from transaction screening obligations, was based on three main considerations:

1. a nudge towards speed,

2. the poor performance of transaction-level screening (as noted by the European Commission), and

3. trust—both in financial market participants to effectively implement EU targeted financial sanctions, and in supervisory authorities to address non-compliance.

It is precisely this third element—trust—that is now in short supply. Banks increasingly doubt the adequacy of control measures implemented by payment institutions, and financial institutions in one Member State often question whether their counterparts in other Member States apply sanctions controls effectively. This raises a Hamlet-like question for the market: to screen, or not to screen against EU targeted financial sanctions on an ex-post basis? While ex-post screening does not interrupt the payment flow, it could serve as a valuable tool to assess and hold counterparties accountable, verifying whether they have robust sanctions implementation frameworks in place.

STEP 3. Adapt to "Immediate" Screening Requirements.

As mentioned, payment service providers offering SEPA Instant must verify whether any of their payment service users are persons or entities subject to targeted financial restrictive measures **immediately** after such measures enter into force, **immediately** after any amendments to them take effect, and at least once every calendar day.

The introduction of the term "immediately" in EU regulation has created significant operational challenges for payment service providers. While batch screening of customer and counterparty datasets once per day (often overnight) has long been standard practice, regulators now expect payment service providers to reflect changes in restrictive measures in near real-time.

This shift has profound implications, of what should be done "immediately" or on an instant basis:

- datasets must be updated;
- client databases screened;
- alert resolution flows streamlined

At the same time, false positives and operational bottlenecks pose material risks, forcing payment service providers to rethink traditional compliance workflows.

Before "immediate" wording, payment service providers typically updated sanctions databases once per day (often overnight), pulling consolidated lists (EU, UN, OFAC, national) into their screening engines usually from external dataset providers. Now the regulator expects near real-time reflection of changes. This means payment service providers must ensure that dataset vendors would guarantee real-time updates across all lists.

There is an interesting constraint on the technological implementation of immediate dataset updates. Banks have highlighted a practical challenge: the **machine-readable EU consolidated list of persons, groups, and entities subject to EU financial sanctions**, provided by the European Commission, is not fully usable due to the following:

*"<...> the European Commission doesn't accept any liability for possible omissions of relevant data or mistakes <...> **Only the information published in the Official Journal of the EU is deemed authentic.**"*
Source: [DG FISMA](#)

As a result, banks rely on external providers for updated lists, which may not deliver immediate updates, particularly outside business hours, as additional efforts are needed to extract accurate data directly from the legal texts in the Official Journal. Requests for an **instant, reliable dataset straight from the source** have remained unanswered, since the Commission does not assume responsibility for the quality of EU sanctions data (an ironic regulatory paradox, in my opinion). Banks are therefore left either to perform manual or semi-automated extractions from legal texts or to rely on vendors with their inherent limitations only because the European Commission is of the opinion that:

"<...> the consolidated list published by the Commission is not envisioned to serve the purpose of PSPs' obligation referred to in Article 5d(1) ."

Another operational issue to consider is that **batch screening of all customers once every 24 hours is no longer sufficient**. While batch screening offered operational advantages - lower system load (efficient for millions of records) and manageable waves for reviewing false positives - **SEPA Instant regulation now requires real-time, or "immediate," screening**. This means that the customer base must be **re-screened automatically** whenever new measures enter into force. Such a requirement imposes **significant IT infrastructure strain** (throughput and latency issues) and an operational burden due to high volumes of alerts, often appearing in unpredictable waves.

One potential solution is the **accurate parametrisation of screening for "immediacy" side effects**, which should, among other things, include a clear **segregation of what must be screened immediately** - such as EU targeted financial and sectoral restrictive measures, and national restrictive measures - from what **can be delayed** until traditional batch screening. Examples of delayed screening include sanctions regimes monitored primarily due to risk appetite or concerns over extraterritoriality, rather than strict regulatory obligations (not mentioning other screening lists, such as politically exposed persons lists and adverse media lists).

Summary: Balancing Speed, Compliance, and Judgment

Yes, I know - it sounds like a cliché: “Compliance is not a checkbox - it’s a mindset.” But clichés exist because they’re true - constant judgment, weighing speed against risk, and recognizing that the rules on paper are never enough on their own, this is a mantra of each compliance officer.

But for me this cliché has a bit of a different flavor - applying the rules thoughtfully means asking yourself not just, “Am I compliant?” but also, “Am I being redundantly compliant?” Every unnecessary check, every over-cautious freeze, every flood of false positives and rejected payments consumes resources, frustrates customers, and - ironically - can create blind spots that clever bad actors exploit. The goal isn’t perfection on paper; it’s judgment in practice.

In SEPA Instant practice, this mindset is constantly pulled between two competing demands: delivering a seamless, instant user experience, and upholding AML/CFT and sanctions obligations. The SEPA Instant framework may shout “speed first,” but that mantra must never blind you to the real risks. At the same time, imagined risks-like obsessing over every single payment purpose of 5 EUR “for Vladimir Putin”- should not distract from the truly significant compliance challenges. Success in compliance requires discernment: separating signal from noise, understanding which risks are material, and applying judgment rather than treating every minor detail as equally critical.

By blending real-time execution with risk-conscious oversight, SEPA Instant payments can be both fast and safe. This approach allows you to deliver on the promise of instant payments while preserving trust in the financial system and safeguarding both your customers and your institution. One final - and perhaps most important - recommendation: learn from your mistakes. Analyze false positives, scrutinize inefficiencies caused by blindly following rules, and continuously adapt your control mechanisms to address the risks that truly matter.

AMLYZE screening solutions have achieved **less than 1% false positive rates** in real production environments. If you’d like to learn how we reached this milestone, you can book a [free consultation](#) with our experts.

Explore more about our [Customer Screening](#) and [Payment Screening](#) solutions, or dive into a real-world success story in our [Violet case study](#), where we helped a fintech reduce false positives by 10x.

AMLYZE

Book A Consultation

Explore more about our [Customer Screening](#) and [Payment Screening](#) solutions, or dive into a real-world success story in our [Violet case study](#), where we helped a fintech reduce false positives by 10x

BOOK NOW