# Sanction screening changes due to the Instant Payment Regulation

**Technical challenges of sanction screening**

**-**

**Specialized article**

## What changes will result from the Instant Payment Regulation in the area of sanctions screening?

Instant payments offer great potential to speed up and modernize payment transactions. However, Article 5d of the EU Regulation on Instant Payments (2024/886) also makes it clear that efficiency and speed must not come at the expense of compliance with EU sanctions law.

In order for the payment service provider to fulfill its obligation to the customer to process and post instant payments within ten seconds, the Instant Payment Regulation (IP Regulation) provides for the payment service provider (PSP) to check its own customer master data against EU financial sanctions lists in accordance with Article 215 TFEU on a regular and ad hoc basis. This means that the customer master data is checked against EU financial sanctions lists in advance of the transaction, so that the transaction is already approved with regard to sanctions at the time of initiation by the customer. This has a significant difference to common practice prior to the publication of the IP Regulation, which focused on transaction-based sanctions screening to check individual transactions for EU sanctions violations.

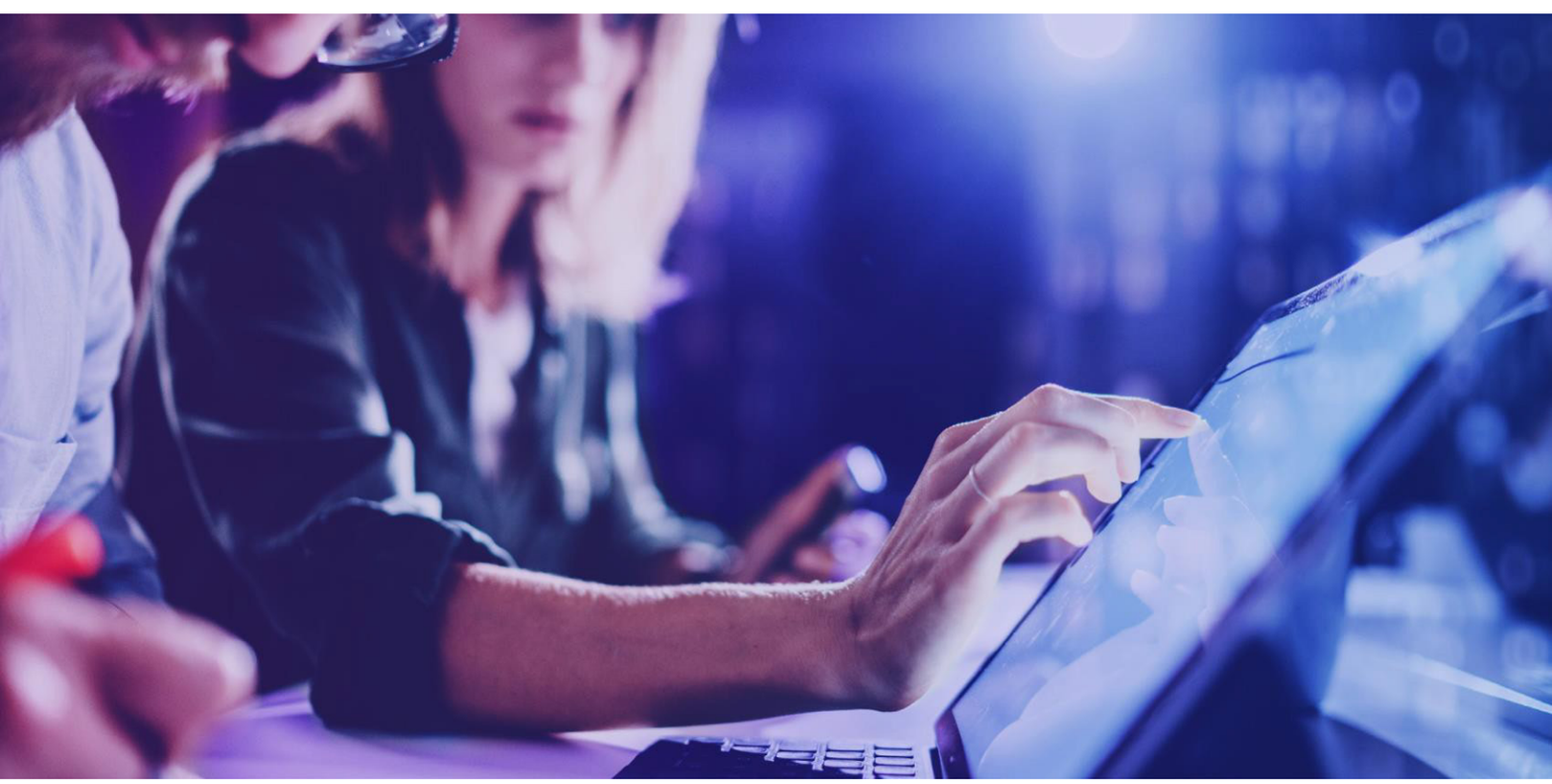
With the entry into force of the IP Regulation, payment service providers are therefore obliged to check their own customer master data record against the valid EU financial sanctions lists on a regular basis, i.e. at specified intervals, as well as on an ad hoc basis review.

This is intended to prevent economic resources from being made available to those persons or organizations that are subject to direct or indirect targeted financial restrictive measures (e.g. freezing of assets).

For PSPs, this means that their own customer data must be checked for EU financial sanctions violations at least once a day, which requires continuous checking 365 days a year. Secondly, every time the valid EU financial sanctions lists are updated or changed, all own customer master data must be checked against the new EU financial sanctions lists immediately to ensure that the requirements of the IP Regulation are met and payments to sanctioned persons are prevented.

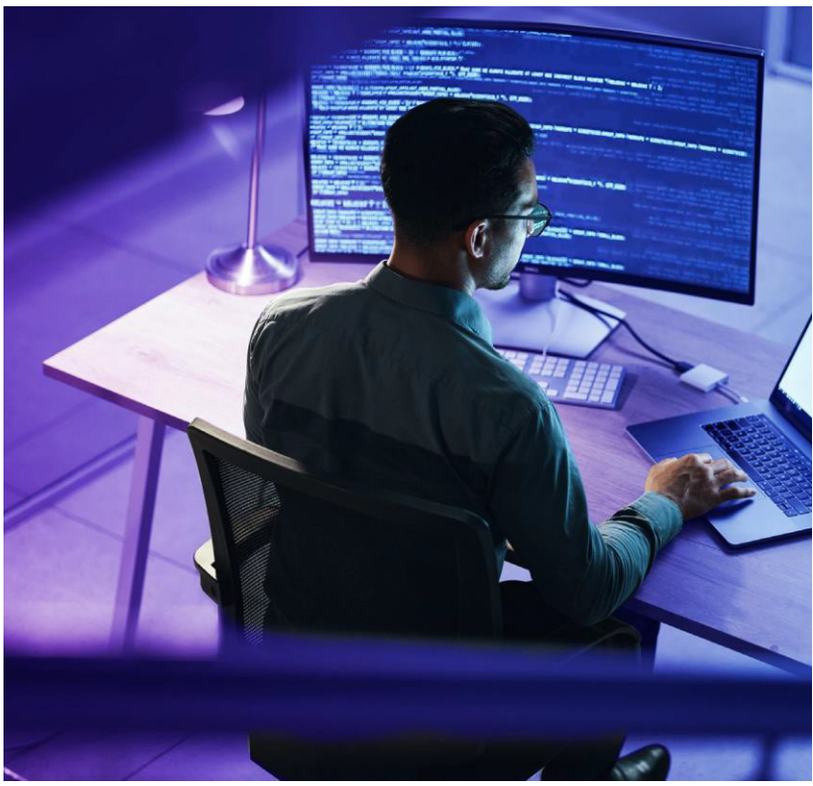
If a hit is identified in its own customer base as part of the sanctions list check, the payment service provider must check this immediately. As long as the hit cannot be clearly identified as "False Positive", the Instant Payment function will be suspended for the customer concerned.

The risks and consequences of non-compliance with the financial sanctions audit under the IP Regulation can be serious and have legal, financial, economic and reputational implications.
is therefore crucial that payment service providers ensure that they implement the relevant regulations appropriately and effectively.



It is important to emphasize that the check against non-EU financial sanctions lists is excluded from this regulation. The payment service provider remains obliged to check each individual IP transaction and the transaction details contained therein (e.g. customer, counterparty, purpose of use, etc.) against non- EU financial sanctions list in real time and, in the event of a hit, to take appropriate measures such as temporarily halting transactions. To implement this requirement, the payment service provider needs an appropriate and effective transaction- based sanctions screening system with corresponding connections to the core banking systems.

Although transaction-based screening against non-EU financial sanctions lists continues to be of great importance, this article focuses mainly on client-based sanctions screening with regard to EU financial sanctions lists. This is where the most significant regulatory changes are expected in the future.



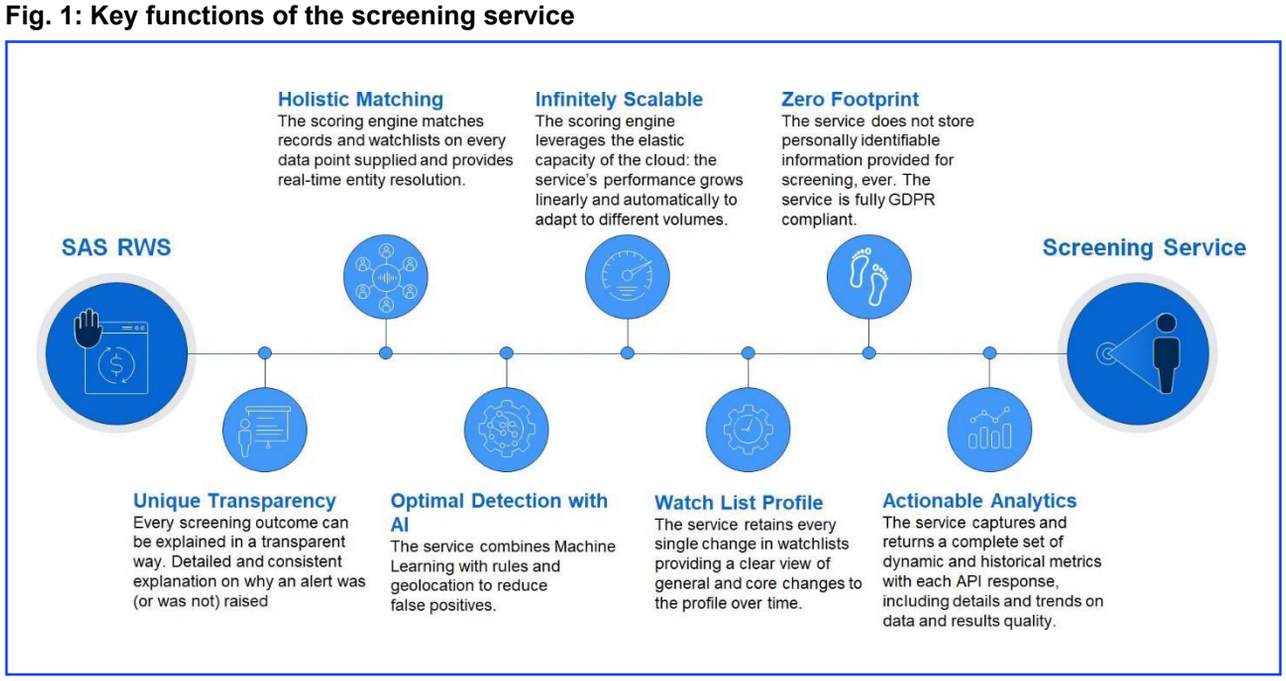
## How does SAS support the technical implementation of customer-based sanction screening in compliance with the requirements of the Instant Payment Regulation?

SAS (Statistical Analysis System) is a leading company in the field of data analysis and business intelligence. In the area of compliance, it also offers a variety of solutions that help companies to fulfill regulatory requirements and effectively counteract risks. In the area of sanctions in particular, SAS provides advanced tools to help companies comply with international sanctions regulations and identify potential violations at an early stage.

SAS uses innovative technologies such as artificial intelligence and machine learning provide accurate and efficient solutions. These advanced technologies help companies analyze complex data sets and make informed decisions, significantly increasing the effectiveness of their compliance measures.

SAS also offers a suitable and effective solution for the technical implementation of regulatory requirement in accordance with the IP Regulation to immediately conduct a screening of your customer data screening against EU financial sanctions lists.

**Fig. 1: Key functions of the screening service**




*Source: SAS, 2025*

In this context, KPMG and SAS have initiated a dialog to intensify their cooperation and develop innovative solutions in the area of compliance. The aim of this cooperation to the strengths of both companies and offer comprehensive, customized solutions that meet the growing requirements of the regulatory authorities.

By combining the in-depth technical expertise of KPMG with the advanced technological capabilities of SAS, companies can benefit from a holistic approach. This alliance partnership makes it possible to effectively address both strategic and technical challenges in the area of compliance.

Another critical aspect of the SAS solution is to ensure that changes to the EU financial sanctions lists are made available to the PSP immediately in order to perform the required screening of its own customer master data against EU financial sanctions lists. The so-called SAS-RWS solution supports real-time, batch or ad-hoc screening against multiple lists, provided that the organization has a subscription or license for the sanctions lists with a third party provider. The available lists are updated regularly according to the schedules defined in the SAS- RWS configuration plan. This schedule allows for automatic downloads and updates to ensure the most current sanctions information is available in the system without the need for manual intervention.

The exact duration required by SAS for the customer-based check of customer master data against the EU financial sanctions lists can vary and, in addition to the maturity level of the existing IT architecture, depends largely on the PSP's customer data volume.

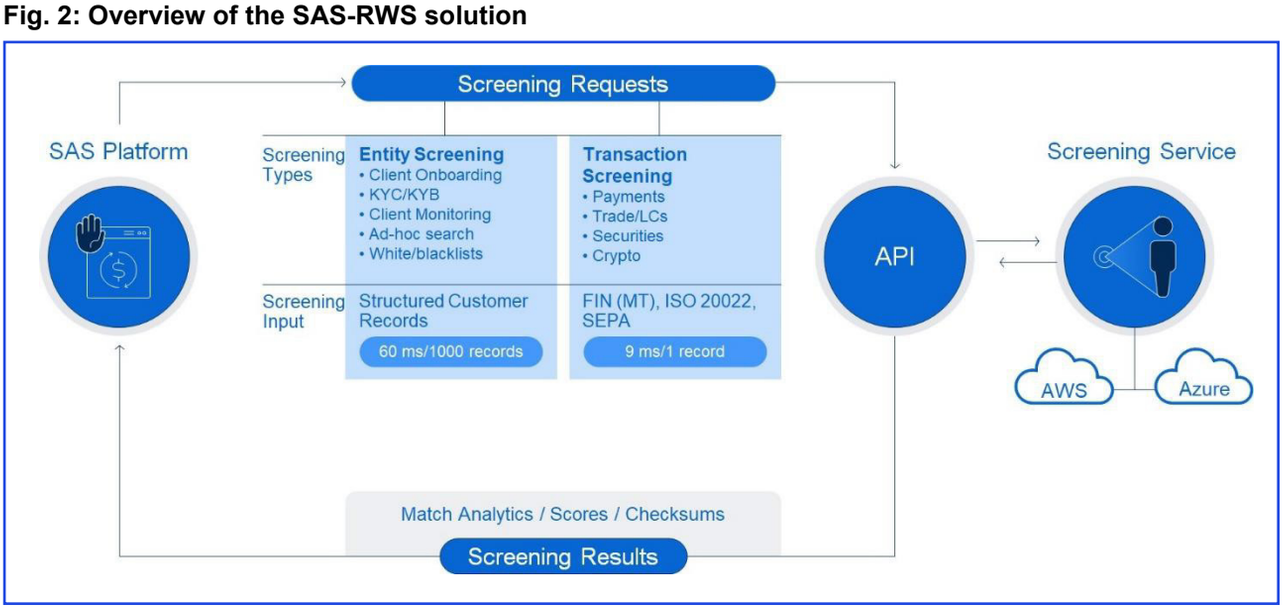
SAS is designed to carry out these processes efficiently and automatically, which usually results in considerable time savings. SAS can guarantee that the processing of 1000 customer data can be completed within a maximum time of
60 milliseconds

Several measures are being implemented to enablethese results. These include:

- High-performance architecture that uses in-memory processing, parallelization and optimized indexing for fast data retrieval and calculation.
- Efficient matching algorithms that use holistic matching methods (fuzzy, semantic, AI- based) and adaptive thresholds minimize processing time while ensuring accuracy.
- Scalable technology stack that includes cloud- based elastic solutions and high-throughput frameworks such as load balancing supports seamless processing.
- Intelligent pre-processing techniques such as sorting, duplicate detection and reference data optimization to reduce complexity.
- SAS' high-performance analytics and hybrid fraud detection methods that safeguard low latency and compliance.

These strategies support optimized and accurate processing within the required timeframe.

**Fig. 2: Overview of the SAS-RWS solution**

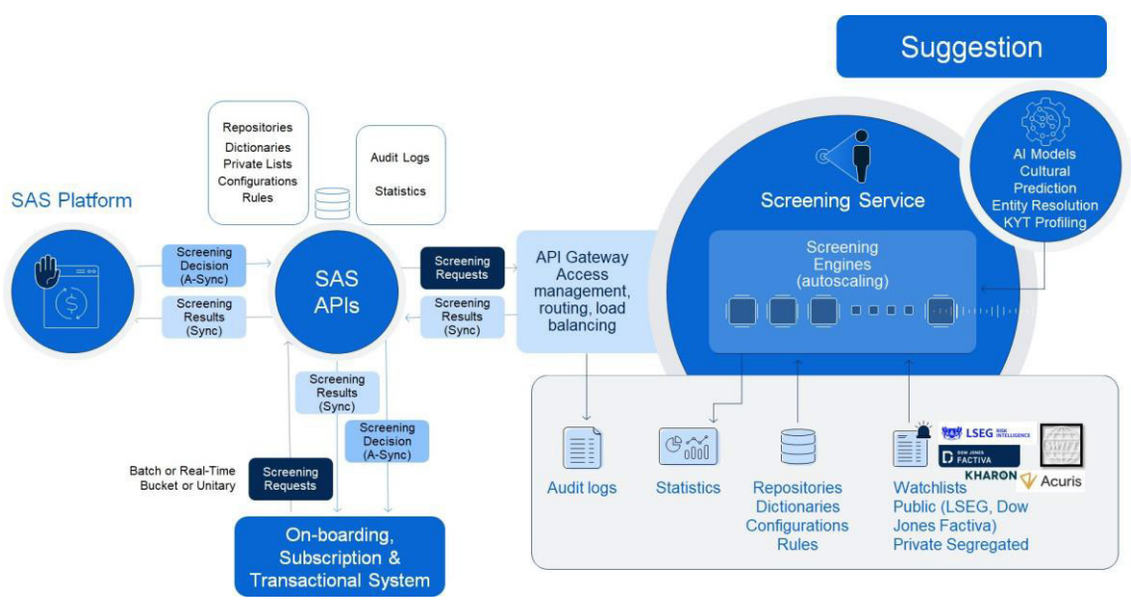



*Source: SAS, 2025*

**With the SAS solution, the payment service provider should be able to take advantage of the following benefits:**

1. Combine AI-driven matching algorithms with real-time decisions: SAS' holistic matching algorithms, combined with composite scores and parameter adjustments, allow customers to assign composite scores and adjust parameters to meet their organization's needs in real-time via customizable presets.
2. Configurable, flexible data orchestration and enrichment: An extensible and flexible message specification enables the mapping of any data into the incoming data schema and provides an external messaging API.
2. Creation of private blacklists and clearance lists: Confidential information can be protected by creating ephemeral blacklists without leaving a permanent trace. At the same time, organizational policies can be enforced through explicit approvals based on predefined criteria to streamline the screening process.
3. Leverage an end-to-end, scalable, secure and accessible cloud-native platform: The fully cloud-native architecture is fully scalable to support business growth and captures fully auditable actions.
   It includes industry-standard encryption algorithms.

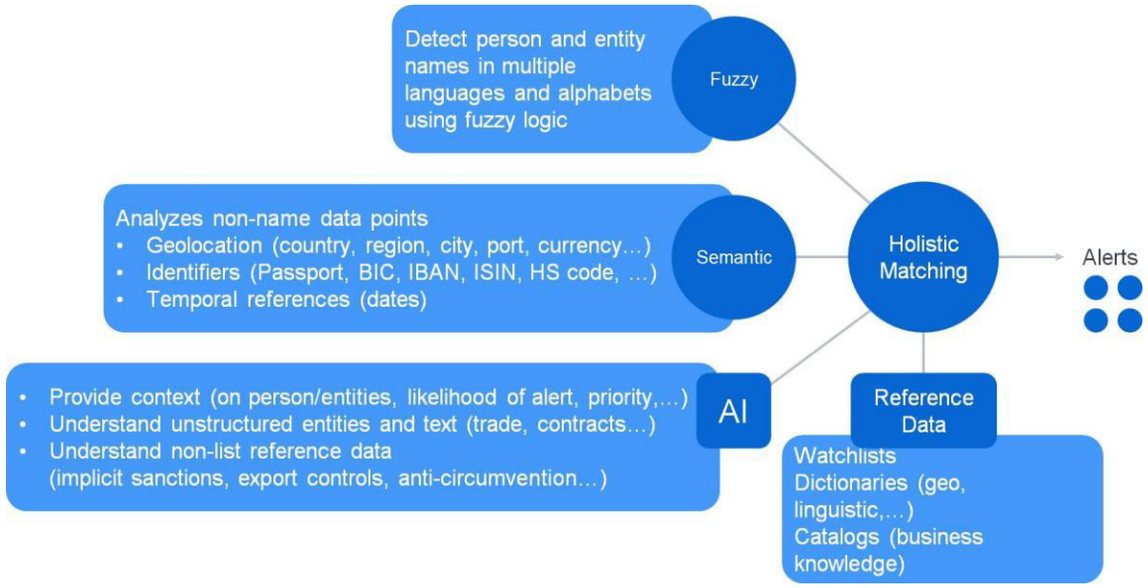
**Fig. 3: API architecture of the screening service**




*Source: SAS, 2025*

The SAS solution uses the holistic matching approach to check customer master data against the EU financial sanctions lists. The holistic-matching approach is an effective and accurate method checking data matches, in which all relevant data , information and its context are taken into account. This leads to better results and helps PSPs achieve their goals for timely, appropriate and effective screening of their own client master data against EU financial sanctions lists.

**Fig. 4: Functions of the "holistic matching approach"**



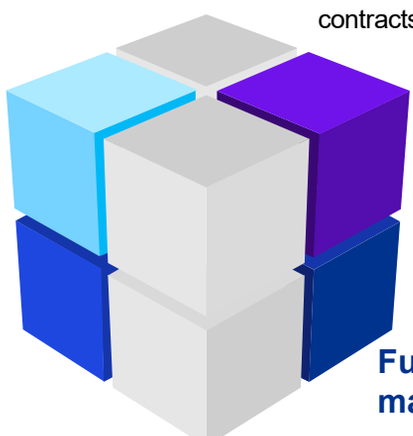

*Source: SAS, 2025*

## Function 1: Fuzzy matching

- Recognition of names, persons and entities in different languages and alphabets
- Reduction of errors due to transliteration, abbreviations or typos

## Function 3: AI matching

- Application of advanced machine learning models contextualize matches, for example:
  - relationships in unstructured data such as contracts or commercial documents
  - Identification of entities implicitly linked to sanctions (for example through export controls or circumvention rules)
  - Evaluation of the probability and priority of hits



## Function 2: Semantic matching

- Analysis of the following non-name-related data points to improve matching accuracy:
  - Geolocalization: country, city, port, currency, etc.
  - temporal reference data: Important data (e.g. dates of birth, transaction data, etc.)
  - Other identifiers: passport numbers, BICs, IBANs, ISINs and HS codes, etc.

## Function 4: Reference data matching

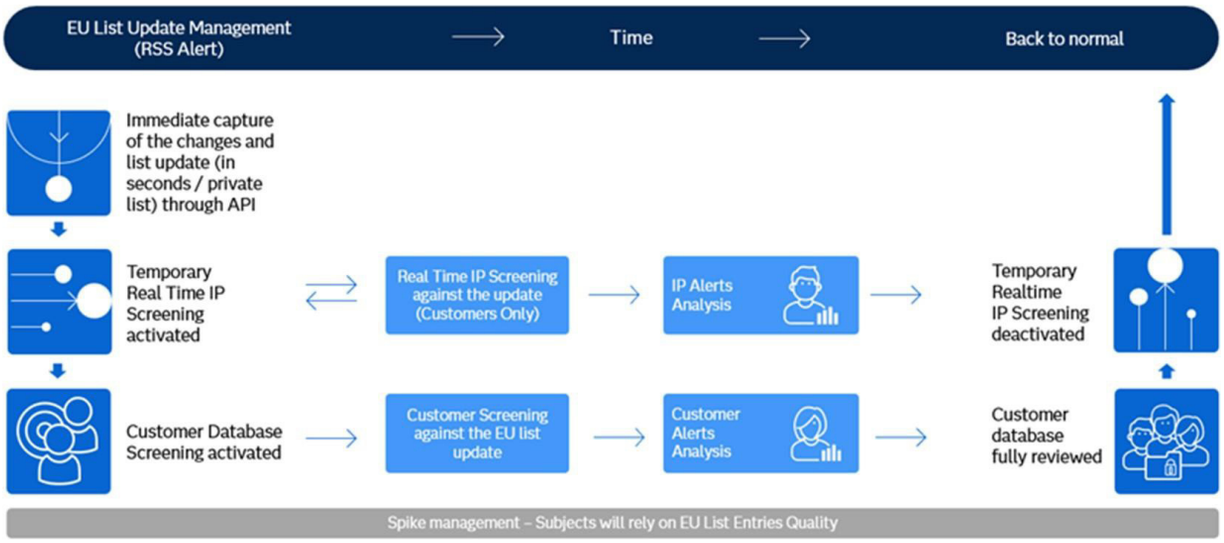
- Use of curated reference data sets suchas:
  - Watchlists: Ensures compliance with global and regional lists
  - Dictionaries: Geo-linguistic references to improve accuracy
  - Catalogs: embedding domain-specific expertise

These functions reduce the dependency on exact name matches and significantly reduce the rate of false positives.

A hit is immediately forwarded to the case management workflow for further processing and evaluation ("false positive" vs. "true positive"). The final assessment is fed back into the system to improve the matching algorithms and reduce the number of false positives.

Instant transfers can be filtered in real time while customer master data is being checked. The time taken to check your own customer master data against the EU financial sanctions lists can be significantly reduced as only the changes in the EU financial sanctions lists are checked instead of considering the entire list. SAS offers a configurable option for carrying delta screenings, in which only newly added or changed entries in the EU financial sanctions lists are checked.

**Fig. 5: Process flow of the SAS sanction screening approach**




*Source: SAS, 2025*

## What are the implications and challenges associated with the new requirement for sanction screening, both technically and procedurally?

Payment service providers face the following technical and procedural implications and challenges in the course of implementing the IP Regulation with regard to the daily and event-driven sanctions screening of their own customer master data against EU financial sanctions lists:

- **Data management:**
  - Management and updating of large amounts of data, especially when processing delta screenings.
  - Ensuring data quality and
  - -integrity to ensure accurate screening results.
- **Performance:**
  - Ensuring system performance and scalability to process large amounts of data in real time.
  - Minimization of latency times to enable immediate decisions and actions.
- **Real-time integration with external systems:**
  - Ensure seamless integration with external sanctions list providers and core banking systems to retrieve updated data in real time.
  - Managing API connectivity and ensuring robustness to avoid interruptions.
- **Scalability with high transaction volumes:**
  - Scaling of the system to cope with peak transaction times or sudden increases in sanctions list updates without any loss of performance.
  - Supporting the growth of customer data as the payment service provider expands its business.

**With regard to the procedural implications and challenges, PSPs should note the following:**

- **Process customization:**
  - Definition and implementation of efficient workflows to carry out checks of generated hits promptly and without delays.
  - Adaptation of existing business processes to meet the new sanctions screening requirements.
- **Risk management:**
  - Identification and assessment of risks associated with non-compliance with the new EU sanctions regulation.
  - Definition and implementation of measures mitigate risks and deal with potential breaches.
- **Documentation:**
  - Documentation of all checks and measures in order to be able to prove compliance with the regulation in the event of audits or other checks.
- **Resource management:**
  - Provision of sufficient human resources to carry out continuous and ad hoc reviews.
  - Training and awareness of employees to the importance and the requirements of sanction screening.

These technical and procedural implications and challenges require careful planning and implementation to ensure the requirements for daily and event-driven customer-based sanctions screening are effectively met.

## KPMG supports you with the implementation

Payment service providers face the following technical and procedural implications and challenges in the course of implementing the IP Regulation with regard to the daily and event-driven sanctions screening of their own customer master data against EU financial sanctions lists:

The expansion of the customer-based sanction check to include daily and event-driven sanction screening of the company's own customer base in the existing IT infrastructures of payment service providers (PSPs) requires the fulfillment of several technical requirements.

KPMG acts as a technical specialist partner and offers comprehensive support in implementing these specific requirements and regulatory specifications - whether through a new technical solution or as an integration into existing solutions.

KPMG has extensive experience and numerous references in the area of sanctions lists and their review at financial services institutions. KPMG's expertise covers various aspects of the regulatory requirements and technical implementations necessary for effective sanctions screening. In addition, KPMG provides comprehensive project management support to ensure that the implementation runs smoothly and on time.

In addition to regulatory and technical advisory expertise in developing sanctions screening requirements, KPMG has experience in automating processes and implementing systems to comply with EU sanctions regulations. Advisory services can focus on various aspects of sanctions screening, such as the integration of real-time notifications and delta screening, or on the implementation and optimization of sanctions screening processes. KPMG supports the adaptation of processes and systems to meet the new requirements of the Instant Payment Regulation.

- **Customization and integration:** KPMG supports payment service providers in the customization and integration of sanctions screening solutions into their existing IT infrastructures. This ensures that the specific requirements and regulatory specifications are met efficiently.
- **Process automation:** KPMG brings extensive experience in the automation of compliance processes, which significantly improves the efficiency and accuracy of sanctions screening. This helps to minimize errors and ensure compliance with EU sanctions regulations.
- **Support and optimization:** KPMG not only offers support during the implementation phase, but also long-term support and optimization of the sanctions screening processes. This includes regular training, updates and adjustments to ensure that the systems always comply with the latest regulatory requirements.

## Open points for discussion

The current wording in the EU Regulation on Instant Payments (2024/886) for daily and event-driven customer-based sanctions screening against the current EU financial sanctions lists currently leaves room for interpretation about the continuation of transaction-based sanctions screening against EU financial sanctions lists.

If transaction-based sanctions screening is completely disabled, the question arises as to how the payment service provider ensures that no transactions that violate EU sanctions law are initiated by the customer during the check of their own customer master data against EU financial sanctions lists (so-called batch run).

The European Banking Authority (EBA) has also not issued a clear statement in the Guideline (EBA/GL/2024/24) regarding the issue of ensuring the conformity of transactions during the batch run. In this regard, the guideline only confirms that transaction-based sanctions screening against EU financial sanctions lists is generally notpermitted.

This uncertainty poses a significant challenge, as payment service providers must ensure that all transactions are compliant with the applicable regulations, even though customer-based screening is the main focus.

Depending on the regulator's final statement in this regard, the corresponding processes must be adapted and technologically implemented. In this matter, payment service providers must react flexibly and agilely to ensure that they both meet the regulatory requirements and maintain the integrity of their transactions.

For a detailed look at the specific requirements and solutions, please refer to other **specialist articles on this topic:**

- Fast payments, strong alliance partnerships: The future of instant payments with KPMG and SAS
- Reporting obligations in the context of the Instant Payment Regulation
- Fraud and Verification of Payee (VoP)

We will be happy to continue to inform you about the Instant Payment Regulation on our website: Instant Payment Regulation - KPMG Germany

## Contact us


KPMG AG Wirtschaftsprüfungsgesellschaft

**Danic Seiwert**
Senior Manager,
Financial Services
M +49 151 46259053
dseiwert@kpmg.com

SAS

**Katarina Garai**
Fraud & FinCrime Partnerships
& Strategic Initiatives Lead,
Western, Central and
Southern Europe
T +43 664 106 2543
katarina.garai@sas.com

This article was written in collaboration with Anja Apfel, Financial Services

**Anna Lykourina**
Head of Fraud & Security Intelligence
Customer advisory,
South-East Europe
T +30 6947 377
960
anna.lykourina@sas.com




**www.kpmg.de**

**www.kpmg.de/socialmedia**