Skadden

White Collar Defense and Investigations

February 26, 2025

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Michael Albrecht vom Kolke
Counsel / Frankfurt
49.69.74220.0
michael.albrechtvomkolke@skadden.com

Sarah Johnen
European Counsel / Frankfurt
49.69.74220.0
sarah.johnen@skadden.com

Eva Legler
European Counsel / Frankfurt
49.69.74220.158
eva.legler@skadden.com

One Manhattan West
New York, NY 10001
212.735.3000

TaunusTurm
Taunustor 1
60310 Frankfurt am Main
49.69.74220.0

Europol Published Practical Guide for Cooperation Between Financial Institutions and Investigative Authorities

Public-private partnerships across the world between financial institutions, financial intelligence units and investigative authorities have laid the foundation to advance criminal investigations. However, there is further potential for financial institutions to efficiently work with state authorities in the context of criminal investigations, to comply with national anti-money laundering acts and to reduce companies' own liability risks.

The EU has worked to harmonize the disparate Anti-Money Laundering and Combating the Financing of Terrorism framework that has been fragmented due to the varied implementation of the Anti-Money Laundering Directive across member states. In May 2020, the European Commission published an action plan for a comprehensive EU policy on preventing money laundering and terrorism financing. On that basis, the European Parliament and the European Council published the first anti-money laundering regulation with the Regulation 2024/1624 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (AMLR). The AMLR will apply starting 10 July 2027. It will, *inter alia*, establish a legal basis for "partnerships for information sharing."

On 30 January 2025, the EU Agency for Law Enforcement Cooperation (Europol) published a practical guide for public-private cooperative mechanisms that share personal data in law enforcement's sensitive investigations ("operational mechanisms"). In this guide, Europol emphasized that not only locally or operationally significant financial institutions may be members of such operational mechanisms, but also nonfinancial sector entities from the private sector such as insurance undertakings.

In this alert, we outline the guide's main takeaways for financial institutions, including objectives, intended benefits, potential methods and scenarios of cooperation, and conditions and rules for a successful cooperation. We also describe the legal context and remaining risks, especially regarding data protection laws, for financial institutions when entering into operational mechanisms.

Key Objectives and Benefits

Operational mechanisms can help identify new investigative leads and support ongoing investigations. By sharing operational information, financial institutions can improve the quality of suspicious activity reports (SARs) and develop a more precise understanding of criminal activity. Most importantly, engaging in operational mechanisms and therefore building specific, related resources will enhance financial institutions' ability to protect themselves from financial crime.

Europol Published Practical Guide for Cooperation Between Financial Institutions and Investigative Authorities

Potential Methods and Scenarios of Cooperation

Investigative authorities may seek assistance from financial institutions to identify leads or leverage an institution's specialized skills. Conversely, financial institutions can initiate cooperation to substantiate case-specific risk management, improve strategic risk management, report a crime to investigative authorities and use criminal investigations in order to detect group-wide risk. For example, a financial institution could assess whether its foreign subsidiaries are also exposed to an investigated customer. Based on the investigation results, the financial institution could reveal complex cross-border money laundering schemes to manage group-wide risks.

Conditions and Rules for a Successful Cooperation

The guide outlines fundamental conditions and general rules for effective cooperation. As essential conditions, all stakeholders should be willing to invest the necessary resources to accomplish mutually agreed upon objectives and to build mutual trust through personal relationships and confidence in each other's conduct. They should be ready to innovate and learn from successes and failures. Financial institutions should also keep in mind that **operational mechanisms may not endanger the impartiality and the operational interests of the investigative authorities or the rights of third parties and may never allow private parties to inappropriately influence the authorities' strategic or tactical decisions**.

As general rules for cooperation, the guide describes, among other rubrics, the following lessons learned from previous cooperations relevant for financial institutions:

- **Starting small and setting realistic expectations:** Beginning with smaller projects that are more likely to yield mutual beneficial outcomes will build initial successful cooperation. Setting realistic goals and clarifying the extent to which the other side can meet them enables continued improvements of the cooperation and prevents expectations from diverging.
- **Governance structure:** Establishing a governance structure aligned with the size and purpose of the envisioned cooperation will ensure suitable seniority in making key decisions.
- **Terms of reference:** Drawing up basic terms of the cooperation in writing at an early stage can establish reliability for both sides. These terms should clearly define the underlying expectations and designated contact persons. In the early stages, the terms might not contain great details of the cooperation if the relationship is dynamic and intended to evolve over time.
- **Creating familiar teams:** Limiting participation at the outset to relatively small groups of individuals with similar roles and responsibilities can nurture respect and trust and can develop understanding of each other's organizational capabilities and requirements.
- **Security, quality and traceability of shared data:** Implementing processes and technical safeguards to protect shared personal data from loss and manipulation is essential. Shared data later identified as erroneous or outdated should be rectified or updated by the cooperation partner who shared the data.
- **Involving data protection authorities:** Informing all relevant data protection authorities about the purpose and design of the envisaged cooperation, seeking their preliminary approval and keeping them updated about any changes ensures the lawfulness of the information sharing.
- **Preventing abuse:** Documenting the specific purposes of information requests made within the cooperation will protect against unauthorized or unlawful use of the information.
- **Avoiding unintended consequences:** Defining clear rules for situations that will require institutions to take action can prevent unfounded adverse consequences for customers.

Legal Context

For financial institutions, the biggest challenge will likely be reconciling operational mechanisms with pertinent data protection requirements. As a general principle, financial institutions are prohibited from disseminating customers' personal data pursuant to the EU General Data Protection Regulation (GDPR) and other national data protection laws (*e.g.*, banking secrecy laws). These data protection regulations provide for exemptions where specific requirements are fulfilled. For example, financial institutions may share personal data if a legitimate legal basis exists permitting such disclosure to investigative authorities.

Consequently, financial institutions must meticulously evaluate several critical factors when sharing data with investigative authorities, particularly:

- **Data minimization:** Financial institutions might need to limit the data processing through objective criteria.
- **Purpose limitations:** Personal data provided from an investigative authority can only be used for the purposes for which it was provided. Financial institutions need to ascertain that the information is not used for different purposes, *e.g.*, unlawfully terminating a business relationship with a specific customer.
- **Customers' access to information:** Financial institutions should act with caution when answering a customer's request to access information in order to avoid a "tip-off."

Europol Published Practical Guide for Cooperation Between Financial Institutions and Investigative Authorities

- **Data transfer from a third country:** When financial institutions have established third-country branches, the national data protection laws of the respective country must also be considered. Whether the data is intended to become directly accessible to authorities in the EU or whether the data only serves the EU head office as a basis to identify suspicious activities may make a difference in the shareability of information.

The Council of Europe's committee for the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108, which is a 1981 treaty) provides guidance regarding an appropriate level of data protection while facilitating cross-border data flows. These guidelines include further recommendations for public-private partnerships, such as determining the respective responsibilities for complying with data protection laws in case of a "joint controllership"-situation or processing personal data as anonymized or pseudonymized, where reasonable.

From 10 July 2027, the AMLR will provide an EU-wide legal basis for partnerships for information sharing between investigative authorities and financial institutions. Most notably for financial institutions, the regulation includes limits as well as obligations regarding the sharing of information. For example, parties must notify the respective supervisory authority, carry out their own assessments of transactions with customers or data protection impact assessments prior to processing any data, and record all instances of information sharing.

While the AMLR can provide additional clarity for these processes, the scope for judicial interpretation will remain. Financial institutions must verify whether their respective legal frameworks allow for the intended cooperation with investigative authorities and diligently assess all envisaged cooperation measures.