FATF

PARTNERING IN THE FIGHT AGAINST FINANCIAL CRIME

DATA PROTECTION, TECHNOLOGY AND PRIVATE SECTOR INFORMATION SHARING

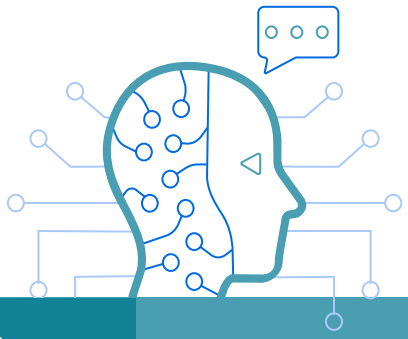
KEY RECOMMENDATIONS FOR RESPONSIBLE COLLABORATION

Collaboration and information sharing helps financial institutions to build a clearer picture of criminal networks and suspicious transactions, and better understand, assess, and mitigate their money laundering (ML), terrorist financing (TF) and proliferation financing (PF) risks. It can also provide authorities with better quality intelligence to investigate and prosecute these crimes and ultimately help prevent crime from reaching our streets.

However, such collaboration initiatives need to be designed and implemented responsibly, in accordance with data protection and privacy rules, so that the risks associated with increased sharing of personal data are appropriately taken into account.

The FATF has drawn on lessons learnt across the jurisdictions of its Global Network to develop recommendations for the public and private sector to avoid common pitfalls. Successful private sector collaboration initiatives involve a range of stakeholders, take into account local regulation and context, take a phased approach and build public trust and understanding. There is no one-size-fits-all solution that addresses all the objectives of data privacy and protection, anti-money laundering (AML), countering the financing of terrorism(CFT), and countering proliferation financing (CPF) for all financial institutions globally. Each information sharing initiative needs to be considered on a case-by-case basis depending on their unique characteristics and the relevant data privacy and protection requirements.

The following recommendations may help jurisdictions or private sector entities that are considering enhancing information exchange. These recommendations are based on observations and lessons learnt across jurisdictions.



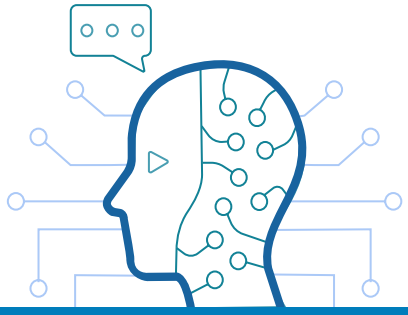
RECOMMENDATIONS FOR THE **PUBLIC SECTOR**

TAKE AN ACTIVE FACILITATION ROLE, FOR EXAMPLE BY:

- Updating legal or supervisory instruments if necessary to provide a clear legal basis for data sharing and processing in line with data protection and privacy considerations.
- Highlighting the particular offences, typologies or key data types that would most benefit from sharing, in order to align sharing initiatives with national AML/CTF/CPF objectives.
- Identifying a lead agency or contact point on private sector information sharing to maintain dialogue with relevant data protection and other government authorities and ensure consistent advice.
- Providing consistent guidance or checklists on relevant provisions to help the private sector understand and navigate AML/CFT/CPF, data protection, and other relevant requirements.
- Making use of regulatory sandboxes and pilot programmes to test information-sharing initiatives, understand the policy implications, and build trust, ideally with the involvement of both AML/CFT/CPF and data protection authorities).
- Building a secured platform for private sector information sharing to provide the required financial and technological resources and ensure accessibility and affordability for institutions.
- Developing projects to harmonise and standardise data, such as common data standards and definitions or data cleaning/structuring initiatives.

ENSURE AND PROMOTE REGULAR DIALOGUE BETWEEN DATA PROTECTION AND AML/CFT/CPF AUTHORITIES (INCLUDING INTERNATIONALLY), FOR EXAMPLE BY:

- Holding regular forums between AML/CFT/CPF authorities, data protection authorities and private sector institutions to share experience, discuss challenges, and develop relationships.
- Devising a joint strategy on information sharing with proper data protection and privacy safeguards to encourage industry initiatives.
- Providing joint guidance or sector-wide engagement on data protection and privacy requirements and technological solutions
- AML/CFT/CPF authorities providing assistance to industry initiatives and helping build links between the private sector and data protection authorities
- Conducting joint initiatives, such as regulatory sandboxes or technology sprints.



RECOMMENDATIONS FOR THE **PRIVATE SECTOR**

MAKE USE OF PRIVACY-ENHANCING TECHNOLOGIES

- While not a 'silver bullet', privacy-enhancing technologies can help support compliance with data protection and privacy obligations.
- In doing so, consider the interoperability and accessibility of different technologies to promote broader engagement.
- The Phase 1 Stocktake Report outlined in detail the various types of technology that could be applied and the risks and opportunities they may pose.

ENSURE HARMONISED DATA

- Data-sharing technologies, especially advanced analytics, work best with common data standards and formats. This also improves data accuracy and reliability.
- In designing initiatives, institutions could make use of existing data prepared in structured format (e.g. data fields used in SWIFT) or implement data cleansing/structuring initiatives (including by engaging technology providers).

PURSUE DATA PROTECTION BY DESIGN

- Data protection and privacy principles should be considered in the design phase of an information sharing initiative. A Data Protection Impact Assessment helps assess compliance and identify and mitigate risks. It also allows participants to pivot projects to align with relevant data protection and privacy requirements, thereby saving resources.
- Data sharing agreements/contracts clearly establish responsibilities and a framework for dealing with any customer complaints.
- A Human Rights Impact Assessment helps ensure compliance with human rights obligations (such as the right to privacy).
- A Legitimate Interest Assessment helps data controllers identify a legitimate interest for sharing data, assess whether processing is necessary to achieve this interest, and balance the interest against individual interests, rights and freedoms.

ESTABLISH EARLY AND ONGOING ENGAGEMENT WITH DATA PROTECTION AUTHORITIES

- Involvement of data protection authorities is critical for the success of any information-sharing project. Engagement should begin at the design phase, and continue through the preparation of a Data Protection Impact Assessment and on an ongoing basis as data collection and analytics begin.
- Involvement of the AML/CFT/CPF authorities can also be critical in the success of private sector-led initiatives.

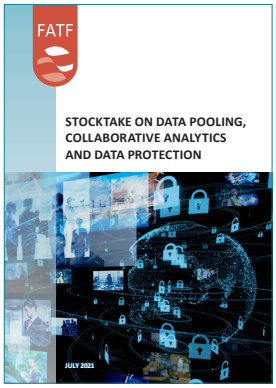
IDENTIFY METRICS TO MEASURE SUCCESS

- Setting clear performance indicators enables participants to assess whether the initiative is achieving its purpose and whether the information sharing continues to be necessary/ reasonable/proportionate in line with applicable DPP requirements.
- Sharing positive outcomes and results helps build trust and encourage broader involvement.

Download the complete report

Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing

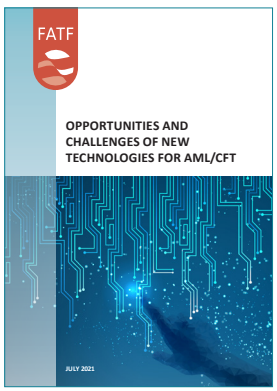
July 2022



Stocktake on Data Pooling, Collaborative Analytics and Data Protection

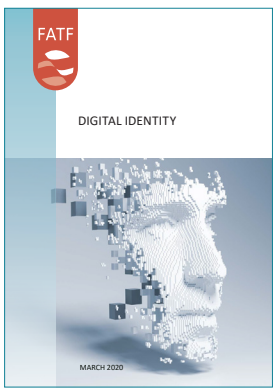
July 2021

also available on www.fatf-gafi.org :



Opportunities and Challenges of New Technologies for AML/CFT

June 2021



Digital Identity, FATF Guidance

February 2020