Data Privacy Experts Working Group Paper

Fighting Financial Crime & Protecting Data Privacy Through Responsible Data Sharing: A Path Forward

I. Introduction

The estimated global proceeds of financial crime each year is 2-5% of global GDP or $800 billion-$2 trillion up to 2009 and by 2018 as more crimes are included, estimates from proceeds could be as high as 6.7% of global GDP, excluding the proceeds from corruption & tax crimes with profits available for laundering at 5.1%, with most proceeds generated from fraud, goods piracy, illicit drugs, acquisitive crime, human & wildlife trafficking, smuggling including people smuggling.

At 6.7% of global GDP, that would represent approximately US$7 trillion in 2023. In addition to being an offence in its own right, financial crime also has grave human consequences, often allowing criminals to profit from devastating crimes like human trafficking, modern slavery and the illegal drug trade. The grim corollaries of financial crime include political violence, human rights violations, torture, discrimination and financial harm. For more on harms and estimates of illicit proceeds from financial crime, the GCFFC have updated its Information Wall for 2024[1].

The mission of the Global Coalition to Fight Financial Crime (**GCFFC**) is to promote more effective information sharing between public and private entities and to advocate for the adoption of smarter international regulations, standards and measures to better fight financial crime.

The GCFFC's Data Privacy Experts Working Group (**DPEWG**) consists of financial crime industry and privacy specialists. Members of the DPEWG were tasked with ensuring compliance with both global fighting financial crime regulations (**FFC**) (including related Anti-Money Laundering (**AML**) and Countering the Financing of Terrorism (**CFT**) measures) and global data protection and privacy laws (**DPP**) across multiple jurisdictions and complex financial workflows.

This purpose of this paper is to set the scene and to provide preliminary recommendations to enable stakeholders to work towards solutions for FFC that uphold privacy rights for individuals and provide necessary and proportionate protections for society at large.

I.I Acknowledgements:

The GCFFC would like to thank Chairs Vivienne Artz OBE FCSI (Hon) CMgr CCMI AIGP and Dr Michelle Frasher PhD, CAMS as well as the following members of the DPEWG for their immeasurable contributions to this paper: Ronen Cohen, Gem Conn, Sadie Falconer-Bowen, Daniel Forbes, Georgina Kon, Janet Lane, Beatrice Marinoiu and Sujit Raman. Also with thanks to a number of GCFFC members for their invaluable contributions: LSEG & TRM Labs and non Members: Duality, Dow Jones, Alix Partners LLP, LexisNexis Risk Solutions and Linklaters LLP.

II. Scope

This paper sets out a multi-disciplinary explanation of the intersection between FFC and DPP along with recommendations for the adoption of international regulations, standards and measures to fight financial crime while still providing protection for individual's data privacy. Achieving a balance between FFC and DPP is not a zero sum game, with only winners and losers.

Where differences arise as they will, resolution will only come from a better understanding of why and how activities are undertaken and why and how these can be carried out consistent with the aim of FFC as well as safeguarding rights for DPP. This paper provides an introduction (See Sections I, II & III) and explanations of:

(A) key factors affecting the complexity of marrying FFC and DPP compliance, including:

- the interests of individuals which must be balanced against the need for FFC measures (see Section IV);
- the diverse range of stakeholders in the extensive ecosystem of FCC players and the complex web of FFC and DPP that impact them (see Section V and Annex 1);
- the benefits and challenges associated with AML/CFT information sharing under the key data sharing regimes used for FFC[2] (see Section VI);

(B) Recommendations including as to how key stakeholders might come together to support the optimal operationalisation of DPP in FFC (see Section VII); and

(C) Key conclusions and next steps for the DPEWG (see Section VIII).

III. Executive Summary of Recommendations

The DPEWG recommends the following actions:

Recommendation 1. Explicit support for Information Sharing in the FATF Recommendations

We generally support the recommendations made by the FATF in its 2022 paper on Data Protection, Technology and Private Information Sharing, which recognised that, "*misuse of data, unnecessary sharing or a lack of protections, have the potential to negatively impact individuals who are not engaged in malicious activities".* It also concluded by making a number of high level recommendations, but in so doing made it clear that any of these were *"in no way a requirement under current FATF standards"*.

We respectfully believe that many countries will as a result ignore these recommendations, unless and until they are included in the 40 Recommendations. When the FATF published its first 40 recommendations in 1990, it recognised that privacy laws, especially as they applied to financial secrecy, and to information held overseas, were being abused and stymied legitimate law enforcement work. The first 40 recommendations published by the FATF in 1990 warned about this and presented actions to address these concerns.

We believe that the FATF should consider explicitly including its non binding recommendations from its 2022 paper into an Interpretive Note and to amending Recommendation 9 which currently states that *"Countries should ensure that FI secrecy laws do not inhibit implementation of the FATF Recommendations"* and could be amended to state that*, "Countries should ensure that FI secrecy laws do not inhibit implementation of the FATF Recommendations AND that country DPP laws do not prevent necessary and proportionate information sharing, between FI's and with other entities, whether public or private, provided other DPP obligations are complied with".*

Recommendation 2: Achieve Greater Legal and Regulatory Alignment, through:

- *the creation and work of formal FFC and DPP forums in international and regional organisations, as well as industry groups containing key FFC and DPP ecosystem players (covering both current and evolving laws and regulations).*

- *inclusion of language in regional and national legislation to embed and recognise the compliance systems identified by these forums/groups.*

- *alignment of regulatory and/or legal guidance on data types which Obliged Entities and service providers may use with the aim of providing clear legitimate pathways for processing sensitive personal data and criminal convictions data along with consistent use of associated data typologies.*

- *development of best practices and consistent standards (including regulator-approved codes of conduct and certification schemes) for data and technology service providers across the FFC/DPP workflow.*

Recommendation 3: Devising Global Standards for Data Governance and Data Management, through:

- *alignment of data categories for risk methodologies, red flag indicators, and data classification schema published by international, regional and national bodies.*

- *public body sponsorship of proof-of-concept exercises to demonstrate the effectiveness of data sharing partnerships incorporating DPP principles while achieving FFC goals.*

- *FCC ecosystem players incorporating DPP data governance and management tools as part of their risk assessment methodologies.*

- *engagement of FFC/DPP leaders for education and collaboration on strategic and tactical risk methodology formulation.*

Recommendation 4: Encouraging the adoption of Privacy Centric Technologies to support FFC & the responsible use of Technology (For example, Artificial Intelligence), through:

- *the promotion of privacy-centric FFC technologies and systems, benefitting from privacy by design, privacy enabling technologies, data interoperability, encryption and data security*

- *support for regulatory sandboxes to help encourage FFC risk assessment model improvements using artificial intelligence (**AI**) and machine learning (**ML**) techniques, as well as regulatory understanding of those technologies*

- *continued promotion of a regulatory environment that supports and develops current thinking on interoperability and/or agreed alignment between global FFC and DPP standards and regulations*

- *promotion of consistent global technical standards for the storing and processing of data to encourage interoperability*

- *the promotion of the ethical and fair use of data*

- *consideration of clear legal pathways for automated decision making for FFC purposes, with safeguards.*

CONCLUSIONS AND FURTHER WORK

Whilst there is an acknowledgement of the benefits which come from harmonisation in global FFC and DPP regimes, and consistency in the requirements of those separate regimes, there are still a number of challenges to be overcome to ensure there is sufficient regulatory clarity on how the FFC ecosystem works and what data sharing is permitted to best counter the negative effects of the illicit economy. This paper aims to set out preliminary actionable recommendations, but further work is still needed. The DPEWG believes the further work could include a i) Cross-disciplinary Working Group to study and provide technical recommendations for private groups, ii) Detailed study on public sector challenges and their interaction with private players & iii) Examination of privacy concerns for Web 3.0.

IV. Public and Individual Interests

The vast majority of impacted organisations will incorporate the standards set by the global intergovernmental body, the Financial Action Task Force (**FATF**), into their FFC programmes, through compliance with national FFC requirements. Over 200 jurisdictions have committed to implementing these standards in an effort to prevent financial crimes linked to organised crime, corruption, terrorism, drugs trafficking, the illicit arms trade, cyber fraud and other serious crimes. However, although DPP regulators recognise the importance of FATF Recommendations and to international efforts to FFC, there are concerns from DPP regulators and individuals that FFC checks may be overly invasive and/or unnecessary.

Balancing FFC and the protection of individual rights is a complex area and one in which significant further clarity is needed. Where initial FFC checks flag that an individual may be linked to financial crime activity, the financial transaction that the individual or their associated company (or other entity) is attempting to make, can be delayed (while further checks are made to verify links to financial crime) or even stopped. In a worst-case scenario, an inaccurate FFC check may result in an individual – or entities associated with that individual – wrongly being denied access to critical payments services, for example.

Therefore, it is no surprise that individuals, regulators and the financial services industry are each sensitive to the need for FFC checks to be carried out in compliance with DPP designed to protect individuals' personal information from being used inappropriately. Principles of transparency, purpose limitation, data minimisation, accuracy, integrity and more, all need to be translated from principles-based DPP and applied to specific FFC scenarios.

Common complaints from individuals about FFC include objections that they do not wish to be (or have wrongly been) flagged as politically exposed persons (**PEP's**) or suspected criminals, that their inclusion on sanctions or Interpol lists is mistaken or politically motivated, or that they object to the retention of their personal information within watchlists, or other tools intended to identify high risk transactions at speed. Parents may complain that, under the FATF Standards, children of PEP's may themselves be considered PEP's which leads to the processing of child data for FFC compliance purposes. On the other side, those involved in carrying out FFC checks are concerned about removing or suppressing information about individuals on request, as this is liable to undermine the ability of financial institutions, government and law enforcement to detect and prevent financial crime. They also recognise that complaints made by individuals about international standards or that call into question national policies, are ones that are best answered by governments and regulators.

Despite the clear complexity of the interaction between FFC and DPP, individuals and customers have little patience for that complexity. They expect each and every one of the hundreds of millions of FFC checks required on a daily basis to produce an almost instantaneous and highly accurate result – even though it is impossible in some cases to verify with 100% accuracy whether an individual is involved in financial crime. These high expectations inevitably, along with the movement and global footprint of criminals, mean that data needs to be shared and processed at a large scale and across borders in order to ensure that checks are as seamless and useful as possible. At the same time, both current, evolving and new data protection, bulk transfer and data localisation requirements, highlight the risks posed by this sharing (including across borders) and at scale. Compliance with FFC and with DPP each appear to lead organisations in different directions.

For all of these reasons, the challenge of designing scalable, repeatable and technology-enabled, real time FFC checks to meet FFC requirements, in a manner designed for compliance with DPP, can appear unending. While there are no perfect answers, the aim of the DPEWG is to build industry, government and regulatory consensus around FCC processes and procedures that strike the optimal balance between both the public's and individuals' best interests – and to *improve outcomes* for both the *public* and for *individuals*.

V. Key FFC and DPP Developments, Stakeholders & Information Flows

The FFC regime has evolved over a number of decades and in most instances independently of each other. The FFC regime involves the collection, processing and sharing of significant amounts of data and information by and between many public and private groups, each with their own roles and (sometimes overlapping) responsibilities.

For example, national Financial Intelligence Units, responsible for collecting private sector reports on financial crime, can have roles which are administrative, which are in law enforcement, or which are prosecutorial. Issues arise where, for DPP purposes, private sector FFC reporting cannot be shared with administrative FIUs, because in some countries those administrative FIU's are not permitted to handle information processed for law enforcement purposes. Further, in many jurisdictions, authorities may only process personal data linked to a possible investigation or prosecution. The split between private and public sector DPP regulations adds an additional layer of regulatory complexity for FFC organisations trying to design compliant data governance across their businesses and for necessary data sharing with third parties.

Therefore, for the purpose of this paper, we begin by charting some of the key FFC and DPP developments, the key information flows, and identifying the key stakeholders within the FFC ecosystem, their roles and examples of how current FFC and DPP regimes in particular regions or countries apply to them. For more on the FFC stakeholders see Annex 1. Given the complexity and detail of these regimes, it is not possible to provide an exhaustive list of them in an easily digestible manner in one paper. This very fact demonstrates the nature of the challenge impacting those within the FFC ecosystem.

V.1 The Development of FFC and DPP

The genesis of FFC starts internationally with the passing of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances in 1998 which also included provisions for countries to criminalise what was described as money laundering in addition to the drug crimes as proceeds of crime as an independent target on the war on drugs and international co operation was seen as essential new steps. The FATF was established a year later by G7 leaders at their summit in Paris France in 1989 and the first 40 FATF recommendations were published a year later in 1990.

While FFC and DPP requirements both have the protection of individuals at their heart, the respective systems and controls have largely been designed independently. Frameworks used today evolved over decades since 1990, and also predate the internet and the wider digital world in which we now live. While the FFC frameworks are anchored in the original 40 FATF recommendations, the availability of data and the application of technology and computing power has been transformational, which enables FFC frameworks to operate at current levels as encouraged by FFC policy makers.

The FFC regime involves many public and private groups, each with their own roles and (sometimes overlapping) responsibilities. This multiplicity of roles and responsibilities means that compliance with some FFC obligations results in millions of different data processes being applied to data (including personal data) for many different purposes on a daily basis. Each individual processing of personal data may potentially be seen through many different local DPP lenses.

A key role in the FFC regime is played by the national Financial Intelligence Units (**FIU's**), responsible for i) receiving suspicious transactions and other reports largely but not only from the private sector, ii) analysing them & iii) disseminating financial intelligence from these reports to for example law enforcement and or judicial authorities. They also should be able to share information with foreign FIU's. Whilst these roles are well understood, how FIU's carry them out and the DPP regimes that apply to them are often complex and varied, with some FIU's facing restrictions on sharing information as expected.

The split between private and public sector DPP regulations adds an additional layer of regulatory complexity for FFC organisations trying to design compliant data governance across their businesses and for necessary data sharing with third parties.

V.1.1 Timelines for Important FCC & DPP Developments

For a summary of main FFC (FATF focused) & DPP (EU focussed) events in a timeline see below.

Timelines for Important FFC & DPP Developments			
FFC Focussed on FATF		**DPP Focussed on the EU**	
1970	US Bank Secrecy Act passed requiring the reporting of information by Banks to US LEA's on financial transactions, ushering in the first ML type legislation globally.	1948	UN Human Rights Convention Art 12 Right To Privacy that, *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence".*
1973	US Supreme Court held by a majority 6-3 decision that reporting. (CTR's) under the BSA 1970 was constitutional & didn't violate the 4th amendment to the US Constitution which prohibits the USG from conducting *"unreasonable searches and seizures"*) but it did believe that additional extended reporting further could do so.	1950	EU Convention on Human Rights (Article 8) protects the right to *"respect for private life, the home and correspondence"*, including privacy of messages, phone calls, & emails. Essentially the right to live life privately without government interference, unless in special cases - national security/tackling crime/public safety etc.
1988	UN Vienna Convention Drugs & ML passed requiring country ML laws.	1973	EU Resolution on Principles for Data Protection in the Private Sector
1989	FATF Established at the G7 Summit (plus EU) in France by G7 leaders.	1974	EU Resolution on Principles for Data Protection in the Public Sector
1990	FATF 40 Recommendations published which focus on actions to combat ML from public (LEA's) & private (Bank/FI) sectors with AML programmes required & with privacy as a potential block & information sharing key to progress in FFC incl SAR reporting.	1981	Council of Europe Data Protection Convention (in force by 1985) was the first international instrument to require public & private sectors to fairly & lawfully collect data, to use the data strictly for a lawful purpose, to retain only as necessary & ensure data quality & accuracy.
2001	FATF included an additional 8 Special Recommendations to combat Terrorism Finance following the 9/11 attacks (adding a 9th in 2004).	1995	EU Data Protection Directive, reflected 1981 CofE Convention which adopted by many EU countries, & was a harmonising Directive DP across the EU. Also established Art 29 Work Party of EU DP experts.
2003	Updated FATF 40 Recommendations 40 plus 8 CTF Recommendations & Extended Regulation beyond Banks/FI's To DNFBP's & requirements on transparency of BO.	2000	EU Charter Fundamental Human Rights includes Art 7 *"Right to Private & Family Life"* & Article 8 *"Protection of Personal Data"* but rights not absolute & in force in 2009.
2012	Revised FATF 40 Recommendations which also extended ML to include ""all crimes" including proliferation finance and tax.	2012	EU Commission proposed a DP reform package as the rules on DP needed modernising due to technological advances & globalisation.
2013	FATF 11 Effectiveness Criteria - Immediate Outcomes (IO's) to test outcomes & not just compliance with 40 Recommendations. Whilst 8 relate to ML (1-8), 2 to TF (9 & 10) & 1 to PF (11). Of the 8 that relate to ML these reflect the focus on the key ecosystem stakeholders, namely LEA, FIU's, Company Registries & the Private Sector obliged entitues, such as Banks FI's Casinos's, DNFPB's and VASP's.	2016	EU General Data Protection Regulation (GDPR) is considered the strongest DP law in the world & applies to the private sector anywhere, if they target or collect data related to people in the EU. DP essential components include Lawfulness, Fairness, Purpose Limitation, Data Minimisation, Accuracy, Storage limit, Integrity & Confidentiality & Accountability (in force in 2018).
2018	FATF agrees to include Virtual Currency Service Providers (VASP's) as be8ng included under Recommendation 15 New Technologies". Note - By 2023 75% of countries report only at best "partial compliance" with FATF VASP R15.p requirements.	2016	EU Data Protection Board (EDPB) est by GDPR (replacing Art 29 WP under DP Directive 1995). The EDPB issues guidelines interpretating the GDPR, gives opinions & is also called to rule by binding decisions on disputes regarding cross-border processing activities.
2022	FATF publishes "Report on the State of Effectiveness and Compliance with the FATF Standards" revealing low levels of effectiveness in FFC after 4th round of country evaluations.	2016	EU Data Protection Law Enforcement Directive (LED) established comprehensive harmonised EU rules for processing domestic & cross border data by LEA's & other competent authorities (in force in 2018).
2022	FATF publishes "Partnering in the FFC Data Protection, Technology & Private Sector Information Sharing" - includes advice for the public & private sectors to avoid common pitfalls sharing information But doesn't change recommendations to require greater information exchange.	2020	EDPB statement released following the EU publishing its AML Action Plan, warning that the Action Plan should be compatible with EU DP laws & regulations & in particular that actions proposed including on information sharing should be justified as being necessary and proportionate.
2024	FATF starts the 5th round of country assessments (to 2030) to measure progress, though no assessment possible on information sharing or DP compliance.	2024	EU Artificial Intelligence Act comes into force which requires existing EU data protection standards will apply to all processing of data using AI

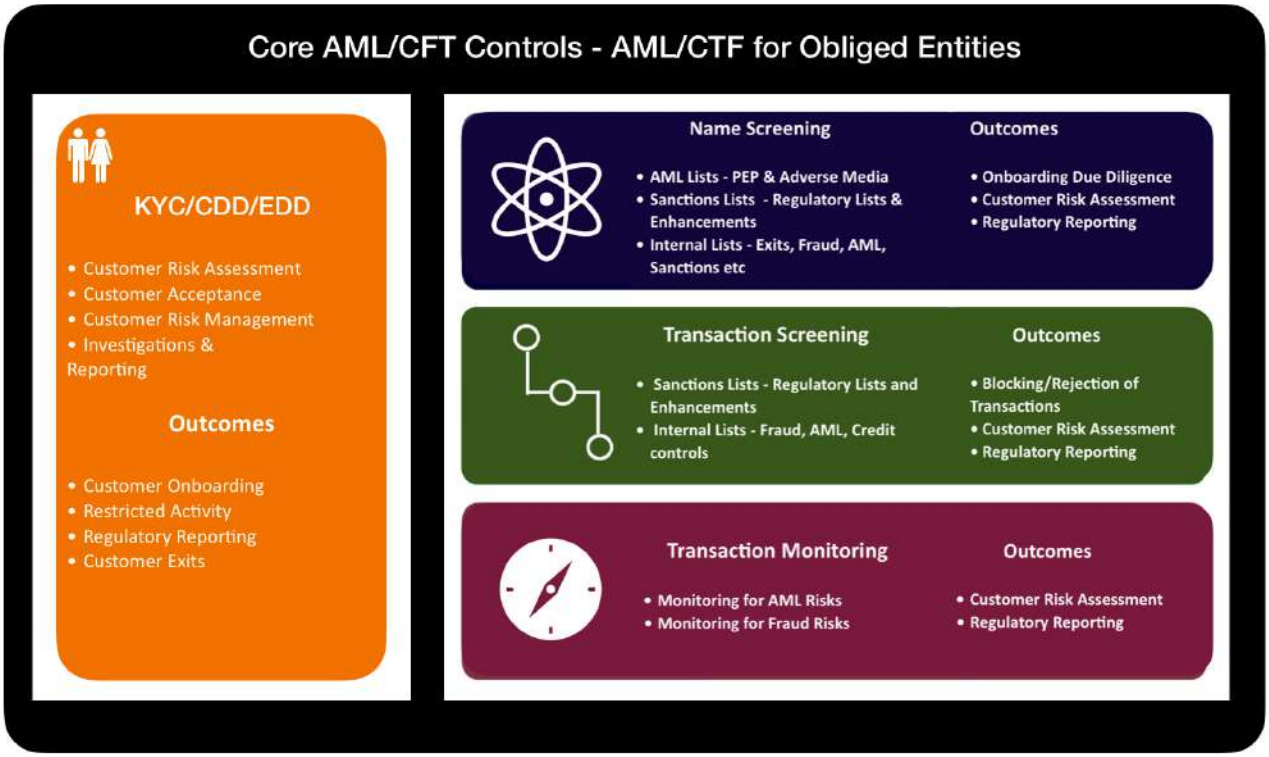
V.2 Data flows through the AML/CFT System with Obliged Entities at the Centre

Information sharing is a critical and necessary part of FFC. Without timely FCC checks, most businesses and individuals who are the subject of those checks would not be able to access critical banking and payment systems in the largely frictionless manner, that they do today.

Where data sharing within the AML/CFT workflow is appropriately designed for compliance with both FCC and DPP, the benefits can be significant. However, navigating the obligations for both is complex[3].

The diagram below shows the data heavy nature of FFC activities to comply with AML/CTF obligations, which has been broken down into 3 stages. Stage 1 is the collection of data, Stage 2 the assessment and analysis of data and Stage 3 the decisioning in relation to this data, support by robust technology and analytic tools. Whilst the regulatory responsibility falls to the Obliged Entities (OE's), which include Banks and other Financial Institutions, Casinos, and other Designated Non Bank Financial Institutions. Significant reliance is placed on third party service providers in order to verify and complete key controls such as KYC due diligence, screening, monitoring, investigation and reporting activities.

The data and the activities that are carried out where data is processed are largely those core processes that are required for Obliged Entities carrying out AML/CFT controls. See the chart below.



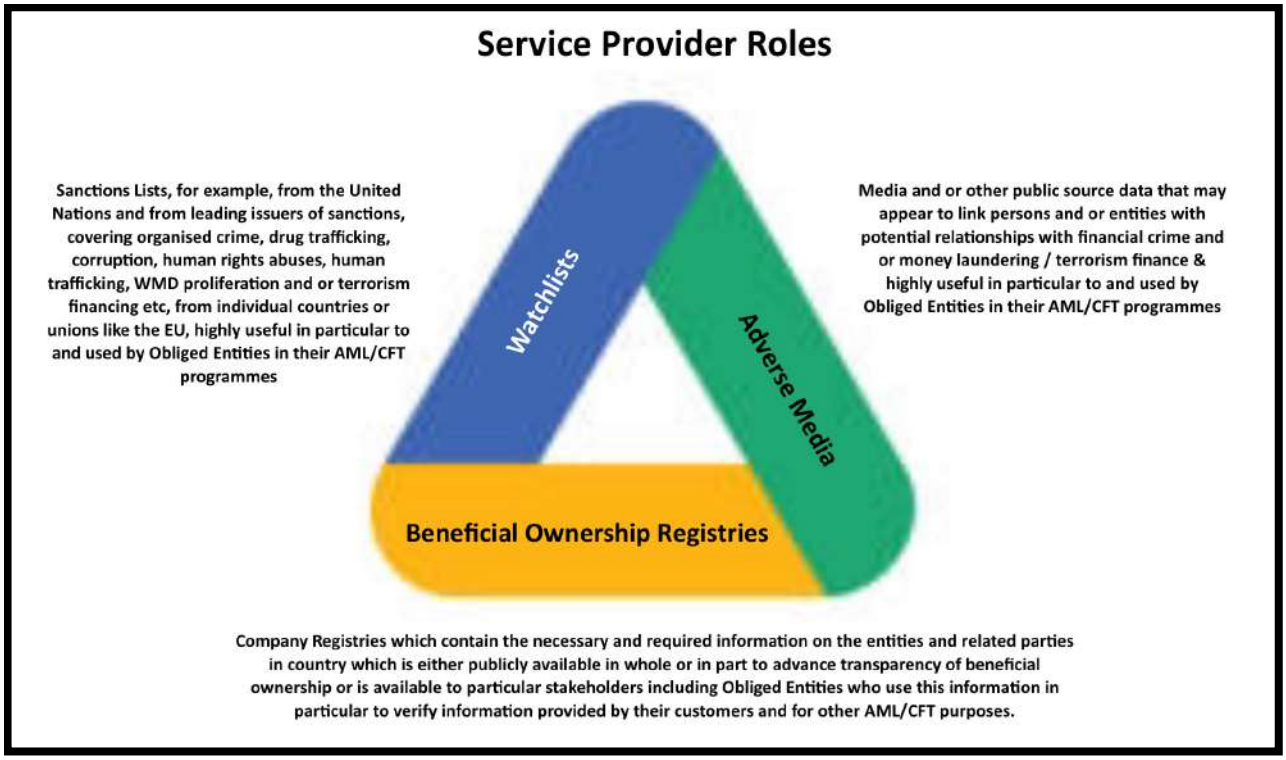
Whilst the roles of the Obliged Entities and those that may receive the information, for example FIU's following a reporting, are well understood and most activities are anchored on specific legal and regulatory bases, other ecosystem members are reliant on "legitimate interests" and other bases for processing, even though their activities as service providers are an important and necessary part of the FFC infrastructure. These include data and technology service providers who are an essential partner to Obliged Entities and authorities in the FFC ecosystem. Without them, financial crime fighters would not be able to perform their legally mandated obligations.

V2.1 Service Provider Roles

European Data Protection Board ("EDPB") letters in 2021[4] & 2022[5] observed that FFC imposes broad and far reaching obligations on Obliged Entities to identify and know their customers, to monitor transactions undertaken using their services, and to report any suspicious transactions, using large amounts of data (personal data). They recognise that private to private data sharing occurs today and is in use by a "*vast majority of*" Obliged Entities via the use of externally sourced "watchlists" sourced by third party providers. These watchlist service providers offer "*easier and faster*" access to information about high risk entities and individuals, allowing FFC checks to be cleared at speed and flagging potentially high risk activity for further investigation.

Data and technology service providers are an essential partner to Obliged Entities and authorities in the FFC ecosystem. Without them, financial crime fighters would not be able to perform their legally mandated obligations. However, they are often overlooked in FFC and are not sufficiently provided for, even though many of their operations and services are covered under other laws, such as DPP and information security requirements. This creates real challenges for Obliged Entities, who rely on these service providers, and threatens the efficacy of efforts to identify and fight illicit finance. The important role that service providers play in the FFC ecosystem has been recently recognised by EU DPP regulators[6].

The DPEWG considered three specific issues which highlight the importance of the role played by service providers and the challenges they face: Watchlists, Adverse Media & Beneficial Ownership Registry Access.



V2.2 Watchlists

The accuracy and reliability of data is an important aspect, not only to protect individuals from a data protection perspective (as enshrined in the EU General Data Protection Regulation (GDPR) Article 5(1)(d) & other data privacy laws), but also to promote the effectiveness of AML/CFT checks undertaken in the public interest to detect and prevent financial crime. The task of making decisions about what data is accurate and what is not, is made more difficult by reason of attempted obfuscation by criminals, who will often resort to using aliases and whose activity spans across many different jurisdictions using these aliases in multiple languages.

While individual Obliged Entities can and do make efforts to check the accuracy and reliability of data, often third-party providers, who specialise in collating and checking that data for multiple Obliged Entities, are able to invest significantly greater resources than any single Obliged Entity, in doing so. They may have teams of hundreds of researchers ensuring that data adheres to strict inclusion and reliability guidelines and have appreciably heightened industry professionalism and standards for watchlist data. This benefits society both from the perspective of supporting more effective FFC, but also enabling the reduction of false positives that might otherwise result in a delay in an individual accessing specific financial services.

Therefore, third-party providers make a critical contribution to the effective implementation of the AML/CFT obligations. However, as this contribution is not explicitly recognised in EU FFC regulations, these providers cannot confidently state that, for the purposes of EU DPP, their processing is lawful by reason of their compliance with EU FFC regulations. There are also no clear guidelines about what safeguards should be in place to ensure that the processing is lawful. This means that the providers must often rely on less certain EU DPP grounds for processing personal data, and that neither providers nor affected individuals benefit from specific legislative guidance about the effective technical and organisational measures that will ensure EU DPP compliance. This issue is particularly acute where third-party service providers have no choice but to process sensitive categories of personal data, or criminal convictions data – both of which can only be handled in very limited circumstances under many DPP regimes – in order to provide watchlist services.

To promote DPP compliance and create more legal certainty for Obliged Entities, the EDPB recommended that the EU's AML/CFT instruments contain specific provisions regarding the general conditions governing the lawfulness of processing by Obliged Entities and the personal data that is provided by third parties for these purposes, as well as codes of conduct and/or certification schemes for watchlist providers.

V2.3 Adverse Media

FATF guidance advises financial institutions to conduct "*adverse media searches…to have a better understanding of who they are doing business with and the risks to which an FI is exposed*". Thus, adverse media/negative news (**AM/NN**) screening is a widely-adopted practice and is a standard test in regulatory audits. OE's must rely on data providers to collect and deliver structured AM/NN and other data used in the FFC workflow, because it would be incredibly time and cost-intensive for each Obliged Entity to do so independently, and the quality of data would inevitably be lower.

However, legal and regulatory guidance gaps on the use of AM/NN place OE's and their data providers at risk. This is because, whilst applicable FFC legislation may not explicitly mention the use of credible AM/NN in screening, they are part of regulatory guidance and inspections. Furthermore, the DPEWG notes that the GDPR's Article 10, which governs criminal convictions data, does not clearly define what that criminal convictions data is. Broadly interpreted, the text could include credible media reports regarding investigations or in-process court proceedings.

A lack of regulatory consistency as to the scope of the definition of "criminal convictions" data may curtail the ability of service providers to provide AM/NN data services, as under GDPR any "*comprehensive register of criminal convictions [must be] kept only under the control of official authority*". An expansive interpretation of this provision would hinder service providers from effectively collecting AM/NN, forcing Obliged Entities to each individually conduct their own, less effective, FFC screening and facilitating evasion of FFC checks by financial criminals.

V2.4 Beneficial Ownership Registry Access

Beneficial ownership registries are essential in sanctions screening to identify ownership and influence for US OFAC, UK, EU & other listed entities, and are helpful to understand complex, multi-jurisdictional corporate structures that may be used for sanctions evasion as well as generally hiding identities. Access to such registers is an example of how the interplay between legislative requirements and court decisions can lead to adding uncertainty for financial institutions and service providers.

For example, the 5th Anti-Money Laundering Directive required EU Member States to establish "*a clear rule of public access*" to "*any member of the general public*" for national beneficial ownership registries. However, in November 2022, the European Court of Justice invalidated unencumbered public access to these registries, citing a disproportionate risk to fundamental privacy rights. The ruling did not apply to authorities or Obliged Entities, and specifically envisaged access rights for journalists and academics based on their legitimate interest.

However, no provision was made for service providers, despite this being the medium through which, in practice, most Obliged Entities access beneficial ownership registers. The EU's latest AML Directive (AMLD6) has started to address service provider issues. For example, it provides that (despite the clear cross-border aspects of good FFC compliance) service providers hold a legitimate interest in accessing UBO (Ultimate Beneficial Owner) information, provided that the data obtained from the EU register is offered to Obliged Entities and public authorities *only* in the European Union.

To best support effective and accurate collection and sharing of data, in a manner compliant with EU DPP, there should be a consistent right for access by service providers on the basis of controls which enshrine privacy protections.

The above service provider examples show how a mismatch between just the EU's FCC and DPP regimes casts doubt on the extent to which, and the conditions under which, those providers are permitted to carry out FFC compliance activities within a single region, the European Union. This problem is amplified when considered on a global level. Many Obliged Entities are global in reach, but FFC and DPP compliance regimes are localised on a per-region, per-country and sometimes even per-state basis, making reconciling all of the competing requirements an impossible task.

The FATF sets recommended global intergovernmental standards for the carrying out of financial crime checks. These standards are not in themselves law, and the different approaches to implementing those standards into binding national legislation or guidance has also produced contradictions, whether in drafting of legislative texts or in differing regulatory interpretations. Such contradictions – along with divergences in local DPP – create challenges for global organisations. It is extremely challenging for them to maintain and apply consistent FFC programmes across their regional and global businesses. This makes it harder for the current FCC stakeholders to identify or prevent illicit finance.

V.3 Focus on Effectiveness by reducing International Inconsistency

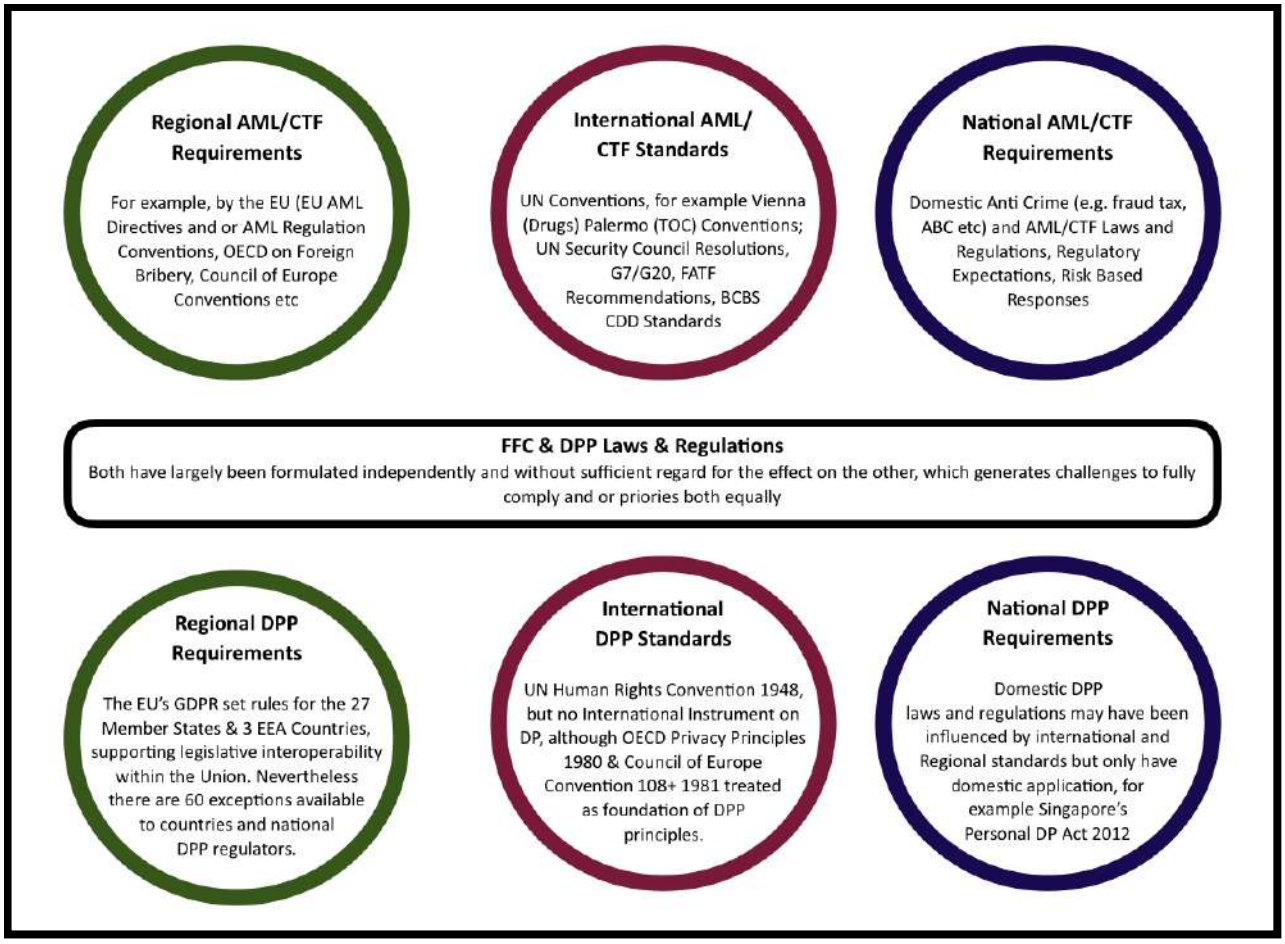
Europol[7] estimates that the EU's current legal structure has enabled law enforcement to take away at most 2% of the annual proceeds of financial crime from criminal networks targeting the EU. Elsewhere the estimates are likely less than 1% except in a handful of countries. Greater regulatory consistency across borders offers the potential for greater success in curbing illicit finance, given the globalised nature of financial services and the digitised world. Innovations in the financial services sector are increasingly borderless by design, as are illicit networks that leverage the FFC ecosystem to launder the proceeds of crimes. The transnational nature of finance and crime drives discussions around legal, regulatory, and technical interoperability in multiple forums such as the US - UK Financial Regulatory Working Group[8].

For DPP, although many in the global community, such as the OECD, have some consensus on foundational principles for privacy, they are by no means universal and there can be inconsistencies in application even within regions with a harmonised set of legal requirements. Whilst FFC requirements are largely a result of international standard setting, DPP laws and regulations are less so.

As Europe currently has the world's most developed regional DPP regime, there is significant focus on the decisions and guidance that have been promulgated by the EU's courts and regulators. For example, it is not uncommon for Obliged Entities to review AML risk scores calculated by third-party service providers (using technology) in conducting their overall AML checks. The 2024 European Court of Justice *Schufa* case is complex. One reading suggests that, in certain circumstances, third party risk score calculations could be considered *automated decision-making* in the EU, even though Obliged Entities must make independent decisions about how to use those scores. If this were the case, those risk scores could not be calculated without the consent of the individual *unless either*: (i) that calculation is necessary for the performance of a contract between the individual and the entity calculating the risk score (N.B. usually inapplicable for service providers assisting OE's with scoring) *or* (ii) the law authorises the calculation (N.B. there is currently insufficiently clear authorisation in law for this). Financial criminals are unlikely to consent to the processing of their personal data for financial crime detection purposes. The outcome appears unworkable for significant parts of the FFC ecosystem – even though that ecosystem seeks to mitigate risks to individuals by allowing for humans to review automatically calculated risk scores and make final decisions about how to treat individuals.

Issues with the harmonisation of DPP and FFC are not confined to the EU, and neither are they confined to regimes with mature DPP. Beyond the EU, data localisation laws prevent information sharing that is crucial to FFC. In the United States of America, a February 2024 Executive Order directs the Department of Justice to introduce prohibitions on the bulk transfer of sensitive data (including, without limitation, financial data) to certain "countries of concern". The Protecting Americans' Data From Foreign Adversaries Act of 2024 (passed as part of H.R. 815) also prohibits data brokers from selling personally identifiable sensitive data to countries considered to be, or to be controlled by, "foreign adversaries". If these prohibitions are drawn broadly enough to cover certain types of publicly available information, they could conceivably prevent or restrict the sort of cross-border data sharing that FFC compliance systems rely on. In addition, drafts of the

USA's latest attempt at agreeing a federal comprehensive privacy legislation (currently known as the American Privacy Rights Act) suggest that the difficult *Schufa* principles could be embedded at a federal level; that it may not be possible to rely on any legitimate interests processing ground in order to use personal data within FCC compliance systems; and that entities will not be able to provide any personal data within the FCC compliance data to government entities in exchange for payment or otherwise on a commercial basis.



Given these evolving challenges, a much needed move towards greater global consistency or alignment in FCC and DPP rules would offer the potential for clearer regulation and less market confusion. Doing so has the potential to drive greater success in making compliant partnerships and information-sharing easier, quicker, and cheaper, to design and deploy where standards are clear. Legal consistency can generate greater trust and confidence among the actors and their workflows within the FFC ecosystem.

As stated by The World Economic Forum in Overcoming Regulatory Friction in Cross Border Payments - 2023, "*The challenges identified during this multi stakeholder collaboration, including disparities in regulatory frameworks across jurisdictions, complexities in anti-money laundering/combating the financing of terrorism (AML/CFT) compliance, stringent data privacy and security regulations, and regulatory barriers to accessing payment systems and infrastructure. Such challenges contribute to cost increases and impede transactions".*

V.4 Information Sharing

FATF considers information sharing "*crucial*" to fight Money Laundering (**ML**) and Terrorist Financing (**TF**)[9], noting that since financial crime networks operate across lines of business and are often transnational, data sharing has the potential to assist FI's and authorities to reduce data collection and pinpoint suspicious activities with more accuracy, for better AML/CFT outcomes if proper DPP safeguards are in place. Annex 2 contains current examples of information sharing initiatives.

Benefits of information sharing include:

- less data collection by OE's and authorities;
- enhancing data quality;
- aiding in customer identification and verification;
- identifying red flags or emerging suspicious trends across lines of business and groups;
- verifying risk ratings;
- identifying and visualising connected persons, entities, networks and transactions;
- augmenting dynamic risk management to reflect new information or changes in behaviours; and
- sharing best practices and analytical techniques to optimise current ways of working.[10]

Nevertheless, there are significant legal and operational guidance gaps between:

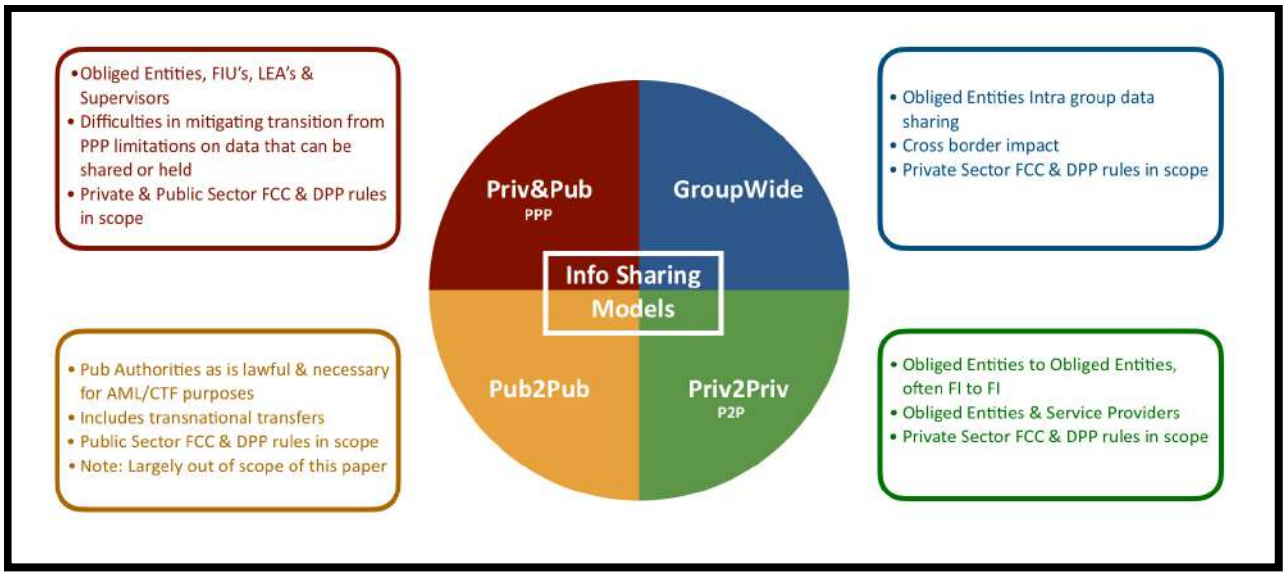
(A) FFC regimes, which require Obliged Entities to process data (including personal data) to conduct their legally mandated regulatory duties, but do not mandate – or provide a clear legislative pathway to enable – inter-entity sharing of information; and

(B) DPP regimes that require controllers to process minimum personal data and only disclose the minimum amount of data to third parties necessary to achieve a defined purpose.

Ensuring there is a clear legal basis which Obliged Entities can rely on to share information – and clear guidance about the extent of permitted data sharing – is central to the success of data sharing regimes, as is understanding how to respect broader DPP regime requirements.

DPP regulators[12] support data sharing *when DPP safeguards are in place,* such as data privacy impact assessments; data transfers that recognise data rights; clearly defined and documented purposes for data sharing and data governance that is proportionate and necessary to avoid scope creep and non-compliance. However, currently there is no comprehensive regulatory guidance explaining or confirming how these concepts should work alongside the FFC workflow. The early successes and promise of data sharing relationships has confirmed the significance of, and benefit to, the public that would be served by such guidance.

There are broadly four key types of data sharing regime, as more particularly described in the diagram below. Each of these involves private entity and/or public entity information sharing.



According to the Future of Financial Information Sharing (FFIS), initiative which has researched information sharing globally and published leading papers describing the various iterations, the preference as far as

nomenclature in this area is a hierarchy where information sharing is a form of collaboration or cooperation, but that established or institutionalised AML/CTF Information sharing should be described as Partnerships or even better Financial Information Sharing Partnerships (FISP's), which could be made up of various parties, for example public to private (PPP) or private to private (P2P). For more on the work of the FFIS see here[11].

V.5 Data Exchange Regimes[12]

For private entities, limitations imposed by both FFC (e.g., confidentiality or secrecy requirements that do not allow suspicious activity reports (**SARs**) or potential SAR data to be shared, otherwise known as "*tipping off*") and DPP laws (e.g., restrictions on sharing data where there is no strict legal requirement) impact what can be shared legally.

Public entities are governed by their own FFC and DPP obligations that may restrict them from sharing information with private entities when it is involved in an investigation or intelligence gathering for a number of reasons, including fear of divulging the sources of that intelligence or compromising the investigation. However, authorities may have constraints in communicating with other authorities in their own jurisdiction (e.g., regulatory to law enforcement, or regulatory to regulatory), or collaboration limitations with another country's authorities, even if memorandums of understanding (**MOUs**) are in place. Recent geopolitical changes, including Brexit, have extended the complexities involved in cross-border data sharing[13] [14]. The divergences between public and private data governance rules adds an additional layer of complexity in the design and maintenance of robust AML/CFT processes.

A. Enterprise or Group

Uncertainties about regulatory requirements and the challenges of non-interoperable systems pose challenges to data sharing even on an intra-group basis.

Challenges that arise from restrictions on the flow of data across borders can impact not just external data sharing between two separate organisations, but also internal data sharing, within an enterprise or group (for example, across lines of business or within subsidiaries and affiliates). Intra-group sharing must consider data localisation and data privacy laws[15], and regulatory divergencies across jurisdictions, making it difficult to establish a common data and compliance framework. These considerations are exacerbated by fears of breaching FCC confidentiality or secrecy laws that prohibit "*tipping off*". The secrecy problem is most starkly demonstrated by the US Bank Secrecy Act (BSA) restriction of sharing underlying data across a group, or the presence of an SAR filing in a foreign branch of a US financial institution, as foreign branches are not subject to BSA requirements. Instead, foreign branches can only share with the parent company[16].

As noted in Section V above, uncertainty around the application of DPP Laws and inconsistent requirements between different jurisdictions can inhibit data sharing.

Outside of restraints arising from the legislative environment, the Working Group noted that there were data and technological hinderances which stifled data sharing. For example, even within the same corporate group, the lack of a consistent data formats has led to data quality and interoperability issues that hinder integration and data sharing. This can be as a result of numerous factors, including mergers and acquisitions, independently operated divisions with independent technologies, platforms and teams, and antiquated legacy systems and siloed data repositories. Finally, sharing sensitive customer information across the group raises concerns about data security, where there is not a single aligned standard.

Public Private Partnerships	
Opportunity	**Challenges**
PPPs are collaborative knowledge sharing forums that allow dialogue between public and private groups, with an opportunity to share information, including entity-level tactical data in accordance with the law, the development of coordinated typologies or alerts regarding financial crime threats, and can enable some private-private sharing among the participants of the groups. Since the UK's Joint Money Laundering Intelligence Taskforce (JMLIT) was established in the UK in 2015, the practice has been replicated, in some form, around the globe. It is possible to design compliance, and by extension data sharing networks, to satisfy both FCC and DPP requirements. As noted above, DPP regulations do not prevent data processing if there is an appropriate legal basis, but guidance is needed to frame operational and technical standards to ensure AML processes and the impact of information sharing is assessed, proportionate, necessary and legitimate to the aims pursued. Further, the same data considerations apply to protecting AML confidentiality.	However, the DPEWG note that PPP's can be reticent to share data without clear legal frameworks and guidance, for fear of breaching DPP requirements. By ensuring there is a clear legal framework and guidance to allow sharing with relevant players, legislators and regulators have an opportunity to unlock valuable data for the benefit of all. EU policy-makers have supported expanding Europe's data sharing mandate and have included language in the AMLR to provide legal clarity. However, Data Protection Authorities such as the European Data Protection Board (EDPB) and France's national DPA, Commission nationale de l'informatique et des libertés (CNIL) have raised concerns about the scale of processing and have asked for more collaboration on setting appropriate safeguards for data processed for these purposes. EDPB opinions and letters have called for appropriate legislative checks and balances, noting that obliged entities are required to process personal data which allow them to draw intimate inferences about individuals and which can lead to the exclusion of legal and natural persons from a right or service (e.g. a banking service).

B. Public-Private Partnerships (PPP's)

Public-private partnerships constitute a key and critical aspect in the global fight against money laundering and terrorism financing, as the prevention and detection of potential ML/TF cases is significantly dependent on the private sector and PPP's can contribute to improving the quality of suspicious reporting, the prioritisation of effort, improving the understanding of ML/TF risks in a country and to the identification of opportunities and ways of improving a country's AML/CFT framework. However, challenges of public-private data sharing persist because of a lack of clear legal frameworks and guidance which give public bodies the confidence to share personal data, for example on suspects known to law enforcement lawfully with the private sector in these fora.

Nevertheless PPP's have evolved and come in many shapes and guises. According to the FFIS[17], "*since 2015, led by the example of the UK Joint Money Laundering Intelligence Taskforce (JMLIT), an international shift in thinking at the policy-making level has gathered pace; driving an evolution in anti-money laundering and counter terrorist financing (AML/CFT) regulatory reporting processes to become more 'intelligence-led'. Partnerships have moved away from compliance 'tick-box' activity to place voluntary information sharing and collaboration across public and private sector partnership members at the heart of national efforts to detect and respond to financial crime risks. As at June 2020, countries with a national public–private financial information-sharing partnership account for 41% of world GDP and 20 out of the top 30 global financial centres are covered by a public–private financial information sharing partnership.*

Partnerships, to varying degrees, can now demonstrate benefits in terms of:

- *An increase in the number of suspicious activity reports addressing threats prioritised by the respective partnership;*
- *More timely and relevant reporting in response to active investigations or live incidents;*
- *Improved quality and utility of suspicious reporting; and*

- *Improved law enforcement outcomes supporting investigations, prosecutions, asset recovery or other disruption of criminal networks".*

Since then more PPP's have been established but they are yet to be mandated by FATF though their benefits have been acknowledged.

C. Private to Private (P2P)

Private to Private information sharing is less developed than other forms of data sharing and similar challenges in respect of interoperability and regulatory inconsistency need to be resolved to encourage the development of this type of information sharing.

Private to Private (P2P) information sharing is not yet as prevalent as PPP's, but FATF's 2017 Guidance on Private Sector Information Sharing supports continuing dialogue. FATF noted multiple AML benefits in P2P information sharing, including allowing an Obliged Entity to share with another Obliged Entity where a customer has been blocked for potential AML/CFT offences that could provide a red flag to the OE to investigate before considering whether to accept a similar transaction. Such information (combined with Obliged Entity intelligence) can then also help to better inform FIU's when investigating escalated SAR's.

Similar interoperability challenges as in intra-group sharing exist in P2P networks, including the lack of data standardisation among financial institutions which makes it difficult to share data relating to strategic or tactical intelligence or which can lead to inconsistencies in risk assessment and identification of suspicious activities.

There are also legal and regulatory barriers that restrict sharing of customer data across institutions and jurisdictions. This can include concerns regarding tipping off, or confidentiality and secrecy, which may deter Obliged Entities from sharing information, for fear of potential legal or reputational risk. Also, there is a concern not to allow receiving Obliged Entities to rely on the information shared and also concerns over sharing internal client data that might compromise market position. As chronicled above for PPP's, P2P networks must comply with all applicable local laws, including DPP, and the data used in such schemes must be proportionate and necessary. New laws, such as the EU's AMLR Article 75, continue to assess the appropriate balance, and regulators continue their involvement to support the appropriate balance to reduce the risk for people wrongly suspected of an AML/CTF risk being excluded from access to banking services. Again, the European Banking Federation has included as one of its four priority areas where it considers ineffectiveness in the current EU AML/CFT framework urgently needs to be addressed, as insufficient co-operation between actors of the AML/CFT system.

As mentioned, a new development at the EU level for FFC data sharing is the new Article 75 provisions of the AMLR[18] which explicitly permits the sharing of data, (private to private) but is subject to a complex range of requirements and restrictions which will take time to understand how they will work in practice.

D. Public-Public

Public to public information sharing is beyond the scope of this paper.

VI. Key Successes and Challenges

The DPEWG notes that whilst there have been some successes in advocating for closer alignment between FFC and DPP regimes, there are still material challenges in ensuring legislation and regulatory guidance is best set up to fight financial crime. This section summarises some of those key successes, as well as the benefits and challenges of responsible data sharing.

Successes

- Continued advocacy from FATF encouraging open dialogue with FFC and DPP leaders.
- Recent drive in both policy (e.g., from the Global Privacy Assembly, G7 and OECD) and in regulator launched pilot programmes to consider possible areas to enhance interoperability and responsible information sharing.
- Steps forward, including with support from regulators, in developing privacy enhancing technologies that could support greater information sharing[19], including in the private – private sphere[20].
- Establishment of successful data sharing initiatives, such as JMLIT[21] and others (for more information see Annex 2).

VII. DPP in FFC[22]: Recommendations

Responsible information sharing carried out for effective AML/CFT compliance that complies with applicable DPP regulation has many benefits, not least in the development of new trends and insights, enhancement of best practice techniques and in successful investigations that result in the reduction and/or penalising of criminal access to the financial system.

Responsible Data Sharing	
Benefits	**Challenges**
1. Increased security, controls and governance. Partnerships can support OEs to take the benefit of expert practices in enhancing the quality of data held, the controls maintained and its security and governance practices. As noted above, DPP regulations do not prevent data processing if there is an appropriate legal basis, but guidance is needed to frame operational and technical standards to ensure AML processes and the impact of information sharing is assessed, proportionate, necessary and legitimate to the aims pursued. Further, the same data considerations apply to protecting AML confidentiality.	**1. Legislative concerns:** Disparities in regulatory frameworks across jurisdictions, complexities in anti-money laundering / combating the financing of terrorism (AML/CFT) compliance, stringent data privacy and security regulations, can add regulatory barriers that add delays or costs to planned data sharing.
2. Previous reports have acknowledged that **shared knowledge can work to advance best practices and analytical techniques**, allowing both parties to validate and develop to optimise current ways of working.	**2. Scope creep.** Data sharing initiatives that don't plan clearly defined and documented purposes for agreed data sharing risk scope creep and legislative non-compliance.
3. Enrichment of insights and risk perspectives. There are numerous examples (see case studies below) where new or additional insights into money laundering risks have been identified through the work of AML partnerships.	**3. Failures to design appropriately.** For data sharing to work well, appropriate processes need to be built in. The parties should carry out the appropriate impact assessments and build in appropriate processes including those needed for compliant data transfers and to recognise individuals' personal data rights.

Whilst it is right to flag privacy and data protection challenges as a core consideration for developing any appropriately robust programme for information sharing, as seen by the examples above, it is possible to work in effective partnerships and design data sharing initiatives in compliance with both FFC and DPP regulations. This has been recognised by both FFC[23] and DPP regulators, most notably, recently, by the EDPB, in their 2022 correspondence to the European Commissioner for Financial Services, financial stability and Capital Markets Union[24].

Cross-border data transfers bring in scope additional complexities, and important work by bodies including the Global Privacy Assembly[25], the OECD[26] and the G7[27] amongst others[28], continue to bring new developments and important thinking to this field, of useful support to multinational enterprises involved in global AML/CFT compliance. However, keeping cross-border issues aside, data sharing and appropriate partnerships within national borders lend valuable support in both private-private and private-public endeavours.

The recommendations below are not intended to be separate activities, rather they should be viewed as concurrent and overlapping efforts.

Recommendation 1: Explicit support for Information Sharing in the FATF Recommendations

We generally support the recommendations made by the FATF in its 2022 paper on Data Protection, Technology and Private Information Sharing, which recognised that, "*misuse of data, unnecessary sharing or a lack of protections, have the potential to negatively impact individuals who are not engaged in malicious activities".* It also concluded by making a number of high level recommendations, but in so doing made it clear that any of these were *"in no way a requirement under current FATF standards".*

We respectfully believe that many countries will as a result ignore these recommendations, unless and until they are included in the 40 Recommendations. *When the FATF published its first 40 recommendations in 1990, it recognised that privacy laws, especially as they applied to financial secrecy, and to information held overseas, were being abused and stymied legitimate law enforcement work. The first 40 recommendations published by the FATF in 1990 warned about this and presented actions to address these concerns.*

We believe that the **FATF should consider explicitly including its non binding recommendations from its 2022 paper into an Interpretive Note and to amending Recommendation 9** which currently states that *"Countries should ensure that FI secrecy laws do not inhibit implementation of the FATF Recommendations"* and could be amended to state that*, **"Countries should ensure that FI secrecy laws do not inhibit implementation of the FATF Recommendations AND that country DPP laws do not prevent necessary and proportionate information sharing, between FI's and with other entities, whether public or private, provided other DPP obligations are complied with".***

Recommendation 2: Legal and Regulatory Alignment

Summary: The lack of a comprehensive and joined up approach to FFC/DPP has created a disjointed set of legal and regulatory regimes – both current and anticipated – which fail to recognise the realities of the complex ecosystem of FFC players and their roles in the financial crime workflow. Few practitioners on either the FFC or DPP side having cross-disciplinary expertise, which makes legal and regulatory alignment challenging, and hinders workable technical solutions.

Recommendations:

- Creation of formal FFC and DPP forums in international and regional organisations.
    - Formal groups should include **cross-disciplinary working groups** to break down educational and information silos at legal, regulatory, operational and technical levels, and promote transferable and practical guidance on DPP using best practices.
    - Forums should seek to set **transnational guidance** which can be formally adopted by regulators in multiple jurisdictions to give clarity on permitted sharing of data and the constraints which will apply and **encourage consistency** across regulatory regimes.
- Industry groups containing the **key players** within the FFC ecosystem should **co-operate** to continue to identify challenges and propose actionable recommendations.
- Include language in regional and national legislation to give **clear authorisation (or create a presumption of compliance)** for intra-group, private-private, and public-private data sharing, where guidance formulated by FCC/DPP technical working groups noted above is adhered to, building on the FATF Recommendation 9 and the 2022 paper on Data Protection, technology and Private Information Sharing.
- **Alignment of regulatory and/or legal guidance** on the **data types** Obliged Entities and service providers may use with the aim of providing clear legitimate pathways for processing sensitive personal data such as criminal convictions data along with consistent use of associated data typologies.
- Develop best practices and **consistent standards** (including **regulator-approved codes of conduct and certification schemes**) for data and technology service providers across the FFC workflow, bringing together FFC and DPP experts and regulators for alignment in developing those standards.

Recommendation 3: DPP as a Tool: Data Governance and Data Management in Risk Methodologies and Suspicion

Summary: Customer data is an essential element of both the relationship and compliance aspects of an FI's business model, and that same data can be highly regulated – for example if it includes criminal convictions data or sensitive personal data. Relevant, timely and accurate data is critical to identifying suspicious actions to report or investigate, and to establish accurate and reliable trend models to underpin strong and adaptable risk models and assessments. The data that enables risk assessments lies at the heart of DPP concerns, because it necessitates the use of large volumes of personal data, including potentially sensitive

personal data. For DPP, it is imperative that the FCC community shows what data is being used, why it is necessary, and how that data use will be protected.

Recommendations:

- **Alignment of data categories for risk methodologies**, red flag indicators, and data classification schema published by international, regional, and national bodies to determine crossovers by product or service across the FCC workflow. This will allow more consistent data classification to explain what data is being used and improve the ability of organisations to justify its use.

- Public sponsorship of **proof-of-concept exercises** to demonstrate the effectiveness of data sharing partnerships incorporating DPP principles, including through initiatives like the IMDA's PET Sandbox[29] or the ICO's regulatory sandbox[30].

- Players within the FCC ecosystem to incorporate **DPP data governance and management tools as part of their risk assessment methodologies** and ensure DPP principles such as data minimisation, proportionality and accountability are embedded throughout standard workflows. Incorporate tools and technologies which help support these principles and help track any data sovereignty requirements.

- Engage DPP leaders to educate and **collaborate on strategic and tactical risk methodology** formulation and demonstrate its effectiveness using a proof-of-concept comparative approach using privacy by design tools and technical solutions.

Recommendation 4: Encouraging the adoption of Privacy Centric Technologies to support FFC & the Responsible use of Technology (for example, Artificial Intelligence), through:

Summary: While data lies at the core of data privacy principles, technology enables insights and informs actions from that data. From a data protection perspective, a technology's functionality, how it arrives at results, and even how an interface presents data to a user can influence compliance decisions, determine escalations, investigations, reporting, and have an impact on an individual.

Recommendations:

- **Promote technology that embeds privacy by design**, privacy enabling technologies, data interoperability, encryption, and data security. Ensure data protection impact assessments are used to evaluate new proposals such that privacy is considered from the beginning of any new technology project.

- **Support regulatory sandboxes** to help encourage risk assessment model **improvements using AI and ML techniques**, as well as regulatory understanding of those technologies.

- Continue to promote a regulatory environment that supports and **develops current thinking on interoperability** and/or agreed alignment in global FCC and DPP standards and regulations.

- Promote **consistent technical standards** for the storing and processing of data across jurisdictions to encourage interoperability by making the technical process of sharing data across systems, corporate groups, private and public entities simpler.

- Promote the ethical and fair use of data.

- Consider clear legal pathways for automated decision making for FFC purposes, with safeguards.

VIII. CONCLUSIONS AND FURTHER WORK

Whilst there is an acknowledgement of the benefits which come from harmonisation in global FFC and DPP regimes, and consistency in the requirements of those separate regimes, there are still a number of challenges to be overcome to ensure there is sufficient regulatory clarity on how the FFC ecosystem works and what data sharing is permitted to best counter the negative effects of the illicit economy.

This paper aims to set out preliminary actionable recommendations, but further work is still needed. The DPEWG recommends further possible work to focus on, for example:

- Cross-disciplinary Working Group to study and provide technical recommendations for private groups.

- Detailed study on public sector challenges and their interaction with private players.

- Examination of privacy concerns for Web 3.0.

Annex 1: Key FCC Ecosystem Players

1. Policy Makers & Standard Setters

1. Policy Makers & Standard Setters			
Type	**Description**	Examples	Roles
Intergovernmental Organisations	Intergovernmental standard setting bodies that are composed of three or more countries/jurisdictions that set agendas & recommendations on FCC & DPP for their members to transpose into national laws and regulations or serve as co-ordinating forums among government authorities.	The Financial Action Task Force (FATF, The International Monetary Fund (IMF), United Nations (FCC/ DPP, Council of Europe (CoE), Basel Committee on Banking supervision (BIS), OECD (Foreign Bribery), EU AML/ CTF & DPP, The Egmont Group, Interpol & Europol.	Policy Making & standards setting. Sometimes decisions are legally binding depending on nature of the organisation and agreement. Some organisations here are also involved in the investigations/ prosecutions of FCC.
Government Decision-Makers	Members of law-making and policy bodies involved in the writing and enactment of legislation and other rule-setting within a sovereign area. Includes regional institutions such as the European Union.	National executive and legislative leaders	Law and policy formation. Depending on the country, some regulatory standards may be set at this level, or these may be delegated wholly or in part to one or multiple regulatory authorities.
Regulatory Authorities	National or regional authorities legally tasked with enacting guidelines for implementation or enforcement of FCC or DPP rules. Can include industry groups officially recognised by government regulatory bodies. Regulatory bodies may have authority over an entire jurisdiction or a business sector.	United Nations Security Council, European Banking Authority (EBA), UK Financial Conduct Authority (FCA), Monetary Authority of Singapore (MAS), Hong Kong Monetary Authority (HKMA), The Office of the Comptroller of the Currency (OCC), The US Federal Reserve, FinCEN, FinTRACK, SepBLAC, AUSTRAC, Japan Financial Services Authority, The UAE Central Bank, & many others & for DPP The European Data Protection Board (EDPB), US Federal Trade Commission (FTC), U.K. Information Commissioners Office (ICO), Personal Data Protection Commission (PDPC) & European Data Protection Supervisor (EDPS)	Sets requirements and guidance for implementation and best practices, typically with feedback from industry and interested groups. Also play supervisory and enforcement roles to ensure standards are met and may be able to levy punitive actions for infractions.

2. Policy Makers & Standard Setters

2. Public Sector Enforcement			
Type	**Description**	Examples	Roles
Financial Intelligence Units (FIUs)	A central, national agency responsible for receiving (and as permitted, requesting), analysing and disseminating to the competent authorities, disclosures of financial information: (i) concerning suspected proceeds of crime and potential financing of terrorism; or (ii) required by national legislation or regulation, to combat money laundering and terrorism financing. FIU models: judicial, law enforcement, administrative, and hybrid.	US FinCEN Singapore – Suspicious Transaction Reporting Office (STRO) UK Financial Intelligence Unit (UKFIU), FIC in South Africa, finTRACK in Canada, AUSTRAC in Australia	Accept, analyse and distribute intelligence received from private sector to relevant authority groups within jurisdiction.
Law Enforcement	Individuals and government agencies that investigate crimes and make arrests of those suspected of MF/TL.	US FBI, Europol, UK National crime Agency (NCA), Commercial Affairs Department of the Singapore Police, Others	Enforcement. Investigations, arrests, and presentation of evidence for use in alleged criminal activity.
Prosecutorial and Judicial Authorities	Government authorities	Crown Prosecution Service (UK) Department of Justice (MLARS) European Public Prosecutors Office (EPPO) Attorney General, Economic Crimes and Governance Division (Singapore)	Enforcement.

3. Private Sector Groups

3. Private Sector Groups			
Type	**Description**	Examples	Roles
Industry Groups	A non-governmental association of member business entities or a cross-industry group that works together to inform industry positions on matters of policy, public affairs and government relations.	Wolfsberg Group, EBA industry working groups, European Banking Federation (EBF), Association for Financial Markets in Europe (AFME), UK Finance, the US Bank Policy Institute	Implementation & best practices setting at an industry level from groups of Obliged Entities & other key stakeholders within the FCC ecosystem. Groups may engage with authorities at various levels to convey concerns & shape laws & regulations.
Financial Institutions	A company engaged in the business of dealing with financial & monetary transactions & encompass a broad range of business operations within the financial services sector.	Banks, Insurance companies, Brokerage firms, Investment banks and dealers & Pension funds	Obliged entities that *must* comply with legal & regulatory mandates. Individually responsible for translating requirements to "house" operational policies & processes.
Designated Non-Financial Businesses and Professions (DNFBPs)	A broad set of "non-financial" businesses identified as susceptible to ML/TF due to the nature of their business and the transactions.	Real estate agents, Precious metals and stone dealers, Lawyers Notaries, Trustees Accountancy firms	Providing professional services which support and or enable the placement layering or integration of financial crime proceeds, unwittingly in most cases.
Service Providers	Includes FCC third-party services such as data providers, technology firms, and outsourcing services. Some develop and offer products that may include entity screening across FCC workflow (KYC, CDD), payments processors, transaction monitoring, payments screening, enhanced due diligence (EDD) investigations, sanctions, and so on. Service providers may be regulated directly by DPP laws depending on the nature of their business.	Consultancy firms Technology service providers Shared Utilities/Data Repositories Identity Management and Security services Automated AML/Fraud Research platforms Big Data platforms AML/Fraud risk modelling and automated monitoring of client activity.	Technology, data, & service support players to Obliged Entities. Some develop and offer data & products that support AMl/CTF controls. Data providers offer watchlists, ultimate beneficial owner information and material from adverse media, as more specifically described in Section V of this paper. May be covered directly by either or both FCC or DPP obligations or required to fulfil regulatory standards due to clients' obligations, which can leave their services legally vulnerable. Service providers may also group in industry bodies and provide leadership on regulatory impacts either with or separately from OE industries.

Annex 2: Information Sharing Examples

With thanks from Future of Financial Information Sharing from the work of Nick Maxwell[31].

Example 1: Group/Enterprise Data Sharing

European Union 🇪🇺 The 4th Anti-Money Laundering Directive (4AMLD), Articles 45(1) & (8) stipulate that "*Member States shall require Obliged Entities that are part of a group to implement group-wide policies & procedures, including data protection policies & policies & procedures for sharing information within the group for AML/CFT purposes*"; & "*Member States shall ensure that the sharing of information within the group is allowed. Information on suspicions that funds are the proceeds of criminal activity or are related to terrorist financing reported to the FIU shall be shared within the group, unless otherwise instructed by the FIU*".
United Kingdom 🇬🇧 Guidance in 2020 published by HM Treasury and the Home Office promotes information sharing within corporate groups. "*Information-sharing on a group-wide basis is a useful tool to prevent, recognise, investigate, and report specific cases of ML/TF. It also enables global risk assessments, which corporate groups should undertake across all branches and majority-owned subsidiaries as the basis for their whole-group policies*".
United States of America 🇺🇸 FinCEN allows US-based multinational financial (depositary) institutions to share SARs with head offices, but not with its foreign branches and affiliates as they are not under BSA jurisdiction. However, the law does require foreign branches to implement US-level AML policies and comply with local standards. In 2006, FinCEN allowed sharing with confidentiality agreements, and in 2010 recognised affiliates who were subject to SAR regulations. In 2022 FinCEN launched a pilot programme on data sharing with foreign branches. As of March 2024, the results are pending.

Example 2: Private-Private Data Sharing Legal Gateways

European Union 🇪🇺 A new development announced in 2024 at the EU level for FFC data sharing is the new Article 75 of the AmL Regulation which explicitly permits the sharing of data, (private to private) but is subject to a complex range of requirements and restrictions which will take time to understand how they will work in practice.
United Kingdom 🇬🇧 Sections 188 & 189 of the 2023 UK Economic Crime and Corporate Transparency Act offers the potential for an AML regulated firm to share information with another regulated firm to prevent, detect and investigate economic crime, without involvement from law enforcement or a request from the recipient firm. Provided certain conditions are met, the sharing and recipient firms are protected from certain civil claims by the relevant customer or any other party. A regulated entity will have two options: (1) Direct sharing of information with another firm in the AML-regulated sector (s.188); and (2) Indirect sharing of information via a third-party intermediary (s.189).
United States of America 🇺🇸 US PATRIOT 314b is a voluntary programme whereby FIs and any association of FIs may register with FinCEN to share information, under a legal safe harbour, with one another regarding individuals, entities, organisations, and countries suspected of possible terrorist or money-laundering activities.

Example 3: Public-Private Partnerships (PPP's)

Leading Countries with Established PPP's

-Argentina Fintel - AR 2019	Hong Kong Fraud & ML Intelligence Taskforce (FIMLIT) 2017	New Zealand Financial Crime Prevention Network 2017 (NZ - FCPN)
Australia Fintel Alliance 2017	Ireland Joint Intelligence Group (JIG) 2017	Singapore AML/CTF Industry Partnership 2017 (ACIP) & COSMIC 2024 (PPP & P2P)
Austria PPP Initiative 2018 (APPPI)	Latvia Cooperation Coordination Group 2018	Sweden AML Intelligence Taskforce (SAMLIT) 2020
Canada Project Protect 2016, followed by Project Chameleon, Project Guardian, Project Athena & Project Shadow	Lithuania Centre of Excellence in ML 2020	South Africa AML Integrated Taskforce (SAMLIT) 2019
EU Europol Financial Intelligence PPP (EFIPPP) 2017	Malaysia Financial Intelligence Network (MyFINet) 2019	UAE UAA PPP Committee 2021
Finland AML/CTF Expert Working Group on a PPP Basis 2020	Malta Financial Intelligence Reporting Partnership (FINREP) 2019	UK Joint ML Intelligence Taskforce 2015 (JMLIT)
Germany Anti Financial Crime Alliance (AFCA) 2019	The Netherlands 1) TF Taskforce (NL-TFTF) 2017, 2) Fintell Alliance (FA - NL) 2018, 3) Serious Crime Taskforce (NL - SCTF) 2018	USA FinCEN Exchange 2017

Selected Examples of PPP's

The Australian Fintel Alliance Partners: major banks, remittance service providers, gambling operators, law enforcement & securities agencies from Australia and overseas.The Fintel Alliance brings together experts for shared intelligence to deliver innovative solutions to detect, disrupt and prevent money laundering and terrorist financing. In 2021 and 2022, successes include: Identification of significant fraud involving $850 million in potentially fraudulent payments made to around 40,000 individuals, leading to more than $1 billion in attempted fraud being stopped by the Australian Taxation Office (ATO); 343 intelligence products provided to law enforcement & intelligence partners, & 2 international awards received for projects targeting IWT & professional ML.

The German Anti Financial Crime Alliance: Partners: As of June 2024, The AFCA's membership consists of 58 members, of which 18 are public authorities (led by the FIU, Bafin (supervisor) and the BKA (police). With 31 Financial Institutions and 9 from the DNFBP's sector. The Alliance exchanges strategic information to increase understanding of ML/TF risks and threats and enabling Obliged Entities to calibrate their detection systems to more effectively fight financial crime.

The Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT). Partners: the Hong Kong Police Force, the Hong Kong Monetary Authority and 23 banks.Up to Q3 2022, the Fraud and Money Laundering Intelligence Taskforce (FMLIT) identified over 19,000 suspicious accounts & networks associated with crimes under investigation by the law enforcement agencies, with HKD 820 million in criminal proceeds restrained or confiscated.

The Singapore AML and CFT Industry Partnership (ACIP). Partners: members from the financial sector, regulators, law enforcement agencies and other government entities. Its co-chairs are the Commercial Affairs Department of the Singapore Police Force and the Monetary Authority of Singapore. Its Steering Group currently comprises the Association of Banks Singapore (ABS) and eight banks. ACIP strengthens AML/CFT in the market through the release of best practice papers, industry dialogue and workshops. The Partnership advances technology developments and their impact on ML/TF and sanctions risks – one such example being the establishment, in August 2022, of the Digital Assets Risk Management Group, and its July 2023 publication on Industry Perspectives on Best Practices.

The Netherlands Terrorist Financing Taskforce Partners: The police, the Fiscal Information and Investigation Service (FIOD), Public Prosecution Service (PPS), the Financial Intelligence Unit of the Netherlands (FIU-the Netherlands) and six banks. Acknowledged by the Netherlands FIU that participating banks deliver better reports using police information, and a mutual understanding of each other's processes has resulted in more informative reports. The Netherlands promotes the Terrorist Financing Task Force's approach of sharing information between public-sector and private-sector parties within the existing statutory frameworks as a world first.

UK Joint Money Laundering Intelligence Taskforce (JMLIT) Partners: Over 40 financial institutions, the Financial Conduct Authority (FCA), CIFAS and five law enforcement agencies: the National Crime Agency (NCA), Her Majesty's Revenue & Customs (HMRC), the Serious Fraud Office (SFO), the City of London Police and the Metropolitan Police Service. JMLIT has supported and developed over 950 law enforcement investigations directly contributing to over 280 arrests and the seizure or restraint of over £86m. JMLIT private sector members have identified over 7,400 suspect accounts linked to ML activity, and commenced over 6,000 internal investigations, while continuing to develop and enhance systems and controls for mitigating the threat of financial crime. Financial sector-led Public-Private Threat Groups and time-limited Cells provide a platform for members to discuss current or emerging threats and identify ways of collectively combating these threats.

2001 USA PATRIOT Act Section 314a requires the Secretary of the Treasury to adopt regulations that encourage co-operation among FIs, regulatory authorities, and law enforcement, to share information regarding individuals, entities, and organisations that are engaged in, or reasonably suspected of engaging in, terrorist acts or money-laundering activities based on credible evidence. Through the US FIU, FinCEN, federal, state, local, and foreign law enforcement agencies have access to 14,000 financial institutions. 95% of 314(a) requests have contributed to arrests or indictments. To ensure requests are used for appropriate cases, FinCEN's process requires law enforcement to certify that the investigation is based on credible evidence of TF or ML.

GLOSSARY

Term	Meaning
4AMLD	Fourth Anti-Money Laundering Directive (EU)
AML	Anti-money laundering
AMLR	EU Anti-Money Laundering Regulation
BSA	Bank Secrecy Act (US)
CDD	Customer due diligence
CFT	Countering the financing of terrorism
DNFB	Designated non-financial businesses and professions
DPA	Data protection authority
DPEWG	Data Privacy Experts Working Group
DPP	Data protection and privacy laws
FATF	Financial Action Task Force
FCC	Financial crime compliance regulations
FI	Financial institution
FinCEN	U.S. Financial Crimes Enforcement Network
FIU	Financial intelligence unit
GCFFC	Global Coalition to Fight Financial Crime
GDPR	General Data Protection Regulation
JMLIT	Joint Money Laundering Intelligence Taskforce (UK)
KYC	Know your Customer
ML	Money laundering
OE	Obliged entity
PATRIOT	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (US)
PET	Privacy enhancing technology
PPP	Public-Private Partnerships
SAR	Suspicious activity report
SAR	Subject Access Request (DPP)
STR	Suspicious transaction report
TF	Terrorist financing
UTR	Unusual transaction report

Endnotes:

[1] https://www.gcffc.org/wp-content/uploads/2024/09/GCFFC-Information-Wall-2024.pdf

[2] This paper recognises the important role of public-public data sharing, however, the detail of these arrangements has been intentionally carved out as out of scope for this paper. This is on the understanding that today these arrangements rely on agreed legal bases, reliant on national MoUs (Memorandum's of Understanding) between regulators and governments.

[3] https://bankingjournal.aba.com/2023/03/practical-data-privacy-compliance-amid-regulatory-swirl/

[4] See: https://edpb.europa.eu/system/files/2021-05/letter_to_ec_on_proposals_on_aml-cft_en.pdf

[5] https://www.edpb.europa.eu/system/files/2022-05/edpb_letter_out2022-0030_aml_cft_proposal_council_en.pdf

[6] https://edpb.europa.eu/system/files/2022-05/edpb_letter_out2022-0035_aml_cft_proposal_ec_en.pdf Page 6, Section 3.

[7]https://www.europol.europa.eu/cms/sites/default/files/documents/The%20Other%20Side%20of%20the%20Coin%20-%20Analysis%20of%20Financial%20and%20Economic%20Crime%20%28EN%29.pdf, pg. 19.

[8] https://home.treasury.gov/news/press-releases/jy1773

[9] https://www.fatf-gafi.org/content/dam/fatf/documents/Partnering-int-the-fight-against-financial-crime.pdf and https://www.fatf-gafi.org/content/dam/fatf/documents/recommendations/Private-Sector-Information-Sharing.pdf

[10] See also FFIS, "*Lessons in Private-private financial information sharing to detect and disrupt crime*" July 2022. https://www.future-fis.com/lessons-in-private-private-financial-information-sharing-to-detect-and-disrupt-crime.html; and European Commission https://finance.ec.europa.eu/system/files/2022-10/221028-staff-working-document-aml-public-private-partnerships_en.pdf; Asian Development Bank. https://dx.doi.org/10.22617/BRF210250-2

[12] https://edpb.europa.eu/system/files/2022-05/edpb_letter_out2022-0035_aml_cft_proposal_ec_en.pdf, page 2. "The EDPB also underlines that ensuring a better consistency between the AML legislative proposals and GDPR principles, such as the accuracy principle or the data minimisation principle, would improve the efficiency of the implementation of the AML/CFT legal framework."

[11] https://www.future-fis.com/lessons-in-private-private-financial-information-sharing-to-detect-and-disrupt-crime.html

[12] Public-public information sharing is beyond the scope of the DEWG's efforts but is listed for completeness.

[13] https://www.theguardian.com/politics/2023/mar/01/uk-police-and-border-force-to-remain-locked-out-of-eu-database-of-criminals

[14] https://finance.ec.europa.eu/system/files/2022-10/221028-staff-working-document-aml-public-private-partnerships_en.pdf

[15] FSB, "*Stock take of International Data Standards Relevant to Cross-Border Payments. "Addressing tensions between different data frameworks, notably those associated with data privacy and AML obligations, was a common challenge*" 25 September 2023.

[16] See https://www.govinfo.gov/content/pkg/FR-2022-01-25/pdf/2022-01331.pdf

[17] https://www.future-fis.com/uploads/3/7/9/4/3794525/five_years_of_growth_of_public-private_partnerships_to_fight_financial_crime_-_18_aug_2021.pdf

[18] https://service.betterregulation.com/document/739340

[19] https://www.gov.uk/government/news/uk-and-us-launch-innovation-prize-challenges-in-privacy-enhancing-technologies-to-tackle-financial-crime-and-public-health-emergencies

[20] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/case-studies/

[21] https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre

[22] https://bankingjournal.aba.com/2023/03/practical-data-privacy-compliance-amid-regulatory-swirl/

[23] The FCA uses Information Sharing Protocol arrangements to share information with other UK government departments. This clarifies the data protection roles and responsibilities in scope to allow effective information sharing that meets Financial Services Act 2012 requirements. https://www.fca.org.uk/publication/corporate/information-sharing-protocol-fca-hmt.pdf. The 2019 MOU (https://ico.org.uk/media/about-the-ico/documents/2614342/financial-conduct-authority-ico-mou.pdf) between the UK's FCA and ICO identifies closer co-operation between the two regulators to share any potential breaches of legislation regulated by the other. Based on these arrangements, recent ICO case studies have included support of a public-private data sharing initiative in the AML space, designed to share personal information for the purpose of detecting and preventing financial crimes and related harms, using PET technologies, specifically homomorphic encryption, to do so. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/case-studies/

[24] https://edpb.europa.eu/system/files/2022-05/edpb_letter_out2022-0035_aml_cft_proposal_ec_en.pdf, page 2. "*The EDPB also underlines that ensuring a better consistency between the AML legislative proposals and GDPR principles, such as the accuracy principle or the data minimisation principle, would improve the efficiency of the implementation of the AML/CFT legal framework*".

[25] https://globalprivacyassembly.org/wp-content/uploads/2022/11/2.2.b.-Global-Frameworks-and-Standards-Workin-Group-English.pdf; https://edps.europa.eu/system/files/2021-10/21-10-25-gpa-resolution-government-access-final-adopted_en.pdf

[26] https://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf

[27] http://www.g7.utoronto.ca/healthmins/G7-Open-Standards-and-Interoperability-Final-Report.pdf

[28] https://www.wto.org/english/res_e/reser_e/1_richard_wto-gpa_slides.pdf

[29] Privacy Enhancing Technology Sandboxes | IMDA - Infocomm Media Development Authority

[30] Regulatory Sandbox | ICO

[31] https://www.future-fis.com/#:~:text=The Future of Financial,detect, prevent and disrupt crime.