GLOBAL COALITION TO FIGHT FINANCIAL CRIME

Fighting Financial Crime & Protecting Data Privacy through responsible Data Sharing: A path forward

By the GCFFC Data Privacy Experts Working Group

October 2024

Fighting Financial Crime & Protecting Data Privacy through responsible Data Sharing: A path forward

The GCFFC thanks all the DPEWG Experts for their contributions

Acknowledgements

The Experts formed a working group led by Co Chairs Vivienne Artz OBE FCSI (Hon) CMgr CCMI AIGP and Dr Michelle Frasher PhD, CAMS and they would like to thank 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 & Linklaters.

GLOBAL COALITION TO FIGHT FINANCIAL CRIME

Fighting Financial Crime & Protecting Data Privacy through responsible Data Sharing: A path forward

GLOBAL COALITION TO FIGHT FINANCIAL CRIME

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.

Summary published on 9th September 2024

The Main Report now published 14th October 2024

See GCCFC Website

GLOBAL COALITION TO FIGHT FINANCIAL CRIME

Fighting Financial Crime & Protecting Data Privacy through responsible Data Sharing: A path forward

Context & Background

- *Financial crime has become global, embracing new technologies eg digital assets and areas eg wildlife crime and is digitally borderless*
- *FFC and DPP regimes have generally evolved independently over recent decades*
- *National, Regional and Global approaches to FFC and DPP*
- *Multiple parties eg Regulators, FIU's, Obliged Entities, Service Providers etc*
- *Tension between "know your customer better" vs "secure privacy rights"*
- *Data localisation vs borderless digital ecosystem*
- *Effective and efficient data sharing is key*

GLOBAL COALITION TO FIGHT FINANCIAL CRIME

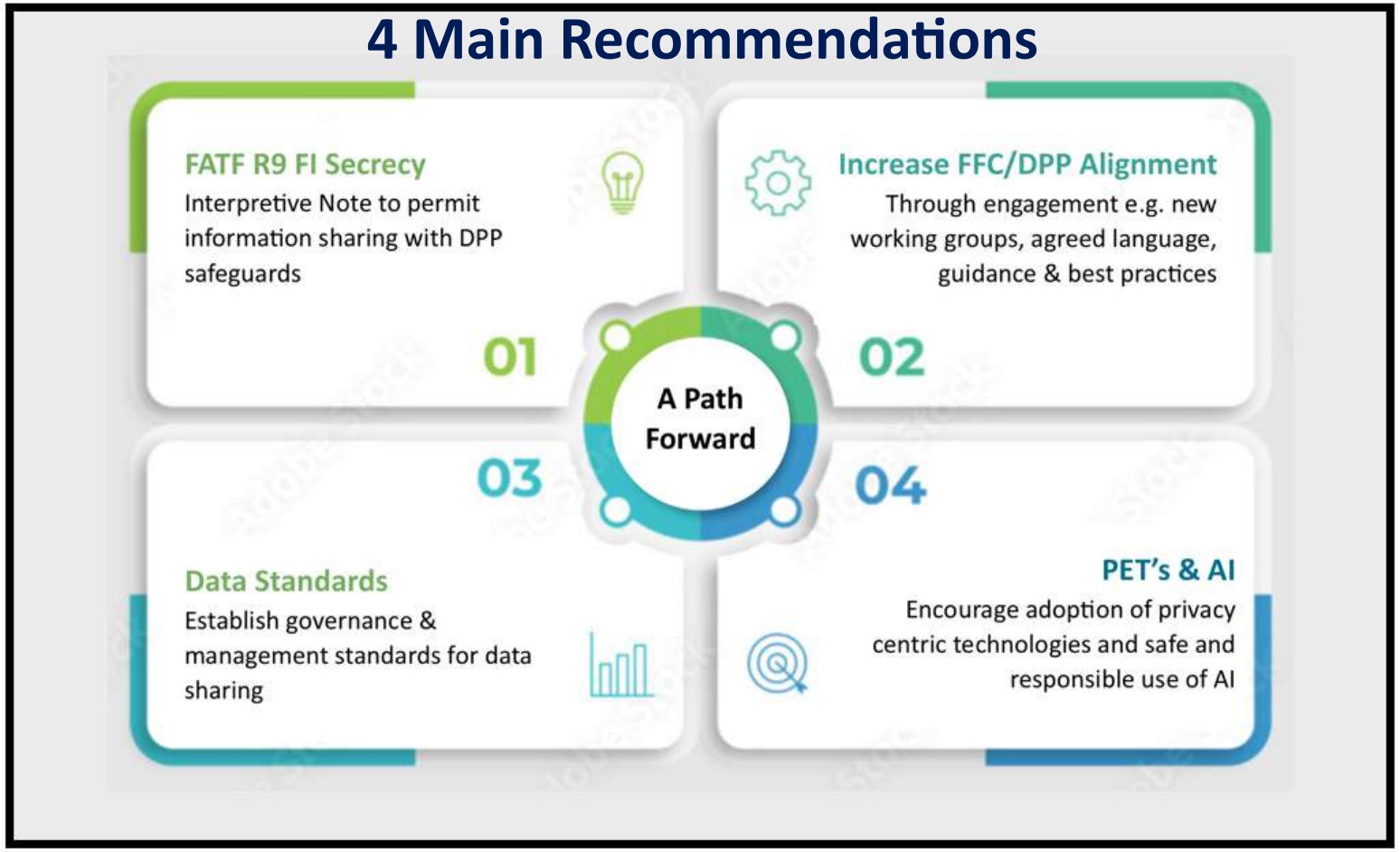
Fighting Financial Crime & Protecting Data Privacy through responsible Data Sharing: A path forward

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. **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. **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.	**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. 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. 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.

GLOBAL COALITION TO FIGHT FINANCIAL CRIME

Fighting Financial Crime & Protecting Data Privacy through responsible Data Sharing: A path forward



GLOBAL COALITION TO FIGHT FINANCIAL CRIME

Fighting Financial Crime & Protecting Data Privacy through responsible Data Sharing: A path forward

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

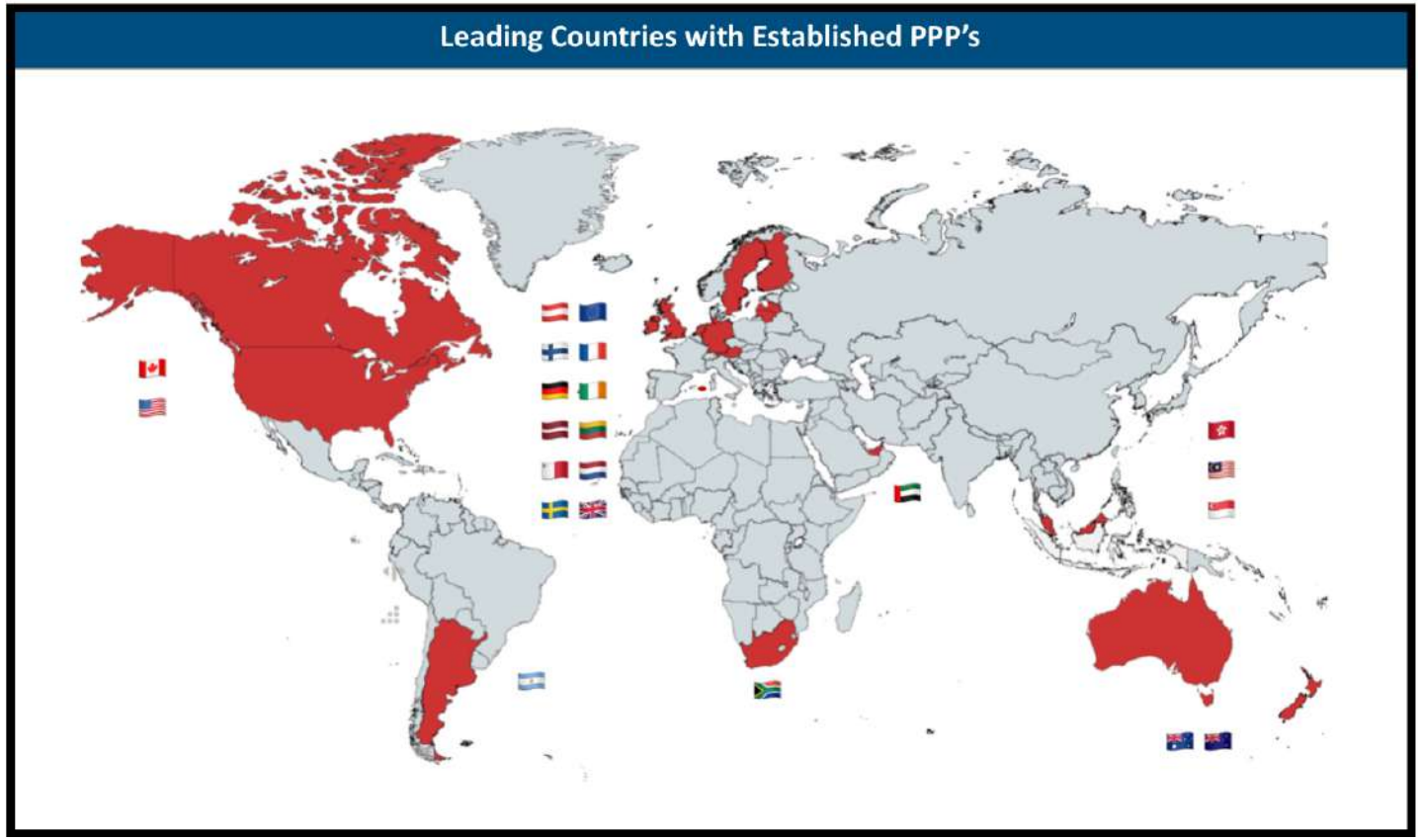
- FATF should consider explicitly including its non binding recommendations from its 2022 paper into an Interpretive Note and to amending Recommendation 9 which currently states that *"Countries should ensure that FI secrecy laws do not inhibit implementation of the FATF Recommendations"*

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".*

GLOBAL COALITION TO FIGHT FINANCIAL CRIME

Fighting Financial Crime & Protecting Data Privacy through responsible Data Sharing: A path forward



Argentina, Australia, Austria, Canada, EU (Europol), Finland, Hong Kong, Germany, Latvia, Lithuania, Ireland, Malaysia, Malta, New Zealand, The Netherlands, Singapore, South Africa, Sweden, UAE, UK, USA

Private to Private (P2P) legal gateways available in the USA, UK, EU and in Singapore (pilot via Cosmic) and also being considered for example in Hong Kong, UAE and elsewhere.

GLOBAL COALITION TO FIGHT FINANCIAL CRIME

Fighting Financial Crime & Protecting Data Privacy through responsible Data Sharing: A path forward

Recommendation 2: Legal and Regulatory Alignment

- 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.
- 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.

GLOBAL COALITION TO FIGHT FINANCIAL CRIME

Fighting Financial Crime & Protecting Data Privacy through responsible Data Sharing: A path forward

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

- 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.
- 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 or the ICO's regulatory sandbox.
- Players within the FFC 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

GLOBAL COALITION TO FIGHT FINANCIAL CRIME

Fighting Financial Crime & Protecting Data Privacy through responsible Data Sharing: A path forward

Recommendation 4: Encouraging the adoption of Privacy-centric technologies to support FFC & Responsible use of Technology for example, Artificial Intelligence)

- 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 FFC 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.

GLOBAL COALITION TO FIGHT FINANCIAL CRIME