Data Privacy Experts Working Group Paper

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

1. INTRODUCTION

The GCFFC's Data Privacy Experts Working Group (**DPEWG**) consists of financial crime industry and privacy specialists. Members of the DPEWG are tasked with ensuring compliance with both global financial crime compliance regulations (**FCC**) (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.

A discussion paper is the first in a series of papers that the DPEWG plans to release. Its purpose is to set the scene and to provide preliminary recommendations to enable stakeholders to work towards solutions for FCC compliance that uphold privacy rights for individuals and provide necessary and proportionate protections for society at large. This is a summary extract of that paper, which will be published in full in the coming weeks, focussed on the recommendations,

The paper sets out a multi-disciplinary explanation of the intersection between FCC 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. The detailed paper provides an introduction and explanations of:

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

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

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

(C) Key conclusions and next steps for the DPEWG

The detailed paper will be published by the end of September 2024 and will be available on the GCFFC website and available for the GCFFC Secretariat.

2. SUMMARY OF THE DPEWG RECOMMENDATIONS

The DPEWG recommends the following actions:

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".* For details see above.

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 FCC and DPP forums in international and regional organisations, as well as industry groups containing key FCC 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 Obliged Entities and service providers may use with the aim of providing clear legitimate pathways for processing sensitive personal data and as 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 FCC/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 FCC goals*

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

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

Recommendation 4: ENCOURAGING THE ADOPTION OF PRIVACY-CENTRIC TECHNOLOGIES TO SUPPORT FCC COMPLIANCE & RESPONSIBLE USE OF TECHNOLOGY (FOR EXAMPLE ARTIFICIAL INTELLIGENCE), through:

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

- *support for regulatory sandboxes to help encourage FCC 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 FCC 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 FCC purposes, with safeguards.*

3. CONCLUSIONS AND FURTHER WORK

Whilst there is an acknowledgement of the benefits which come from harmonisation in global FCC 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 FCC 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 further work is necessary, including a i) Cross-disciplinary GCFFC 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.

ACKNOWLEDGEMENTS

The GCFFC and Chairs Vivienne Artz OBE FCSI (Hon) CMgr CCMI AIGP and Dr Michelle Frasher PhD, CAMS would like to thank the following members of the DPEWG for their immeasurable contributions to this paper: Ronen Cohen, Gem Conn, Sadie Falconer-Bower, 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.

September, 2024

[1] 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.