RIETI Discussion Paper Series 24-E-010

Information Sharing with the Private Sector under Anti-money Laundering and Countering the Financing of Terrorism Regulations

ISHII, Yurika
National Defense Academy of Japan

RIETI
Research Institute of Economy, Trade & Industry, IAA

The Research Institute of Economy, Trade and Industry
https://www.rieti.go.jp/en/

RIETI Discussion Paper Series 24-E-010
January 2024

Information Sharing with the Private Sector under Anti-Money Laundering and Countering the Financing of Terrorism Regulations[1]

Yurika Ishii
National Defense Academy of Japan

Abstract

Financial institutions and other entities find it beneficial to exchange customer identities and criminal risk data to enhance the effectiveness of money laundering and anti-terrorism regulations. Therefore, the Financial Action Task Force (FATF) recommends sharing relevant information among private companies. Additionally, some countries and operators are exploring the consolidation of information and utilization of artificial intelligence and other technologies to identify suspicious transactions. However, implementing cross-border regulations requires robust international collaboration. Unilaterally imposing mandatory information sharing on operators could conflict with national privacy, human rights norms, and data protection laws. This study delves into how various countries are addressing these challenges in the current context and analyzes the implications for international legal frameworks.

Keywords: Money laundering, anti-terrorist financing, financial privacy, data privacy protection, cross-border data transfer
JEL classification: K22, K23, K33

[1] This study is conducted as a part of the project “Comprehensive Research on the Current International Trade/Investment System (Part VI)” at the Research Institute of Economy, Trade and Industry (RIETI). A draft of this paper was presented at the RIETI DP Seminar. I am grateful to the participants in the project and the seminar for their valuable comments.

RIETI Discussion Paper

Information Sharing with the Private Sector under Anti-Money Laundering and Countering the Financing of Terrorism Regulations

Yurika Ishii

1 Introduction

1.1 AML/CFT Regulations and the Collection of User Information

Anti-money laundering and countering the financing of terrorism (AML/CFT) regulations are a part of financial integrity.[2] They comprise multilayered norms, including multilateral treaties, United Nations Security Council resolutions, Financial Action Task Force (FATF) recommendations, and domestic laws.

Central to these regulations is the sharing of customer and transactional information. AML/CFT regulations mandate financial institutions (FIs) to gather customer identification information and conduct customer due diligence (CDD) procedures based on reliable, independent source documents, data, and information. Such sources contain personal information, including any information related to an identifiable person such as name, home address, and nationality. Furthermore, these regulations require that FIs identify and verify beneficial owners (BOs) and understand organizational control structures. Customers must provide details, including identification data and transaction purposes, to designated entities. Identifying BOs is a crucial tool for identifying shell companies.

The scope of the shared information encompasses diverse facets. First, it includes an assessment of money laundering and terrorist financing (ML/TF) risks associated with an entity, enabling a comprehensive grasp of its nature and operations. Second, it involves scrutinizing customer information to ascertain whether individuals or entities have raised concerns about other institutions, both within and outside the financial network. In addition, customer transaction records are invaluable in detecting suspicious activities. Regular updates to customer information are indispensable for effective risk management, facilitating the swift and accurate identification of emerging criminal trends and enabling proactive responses.

Moreover, banks can now amass extensive data, including the usage patterns of automated teller machines and mobile net-banking systems, along with audio and visual data from these interactions. Users also have the option to voluntarily provide supplementary transaction-related information such as shopping histories and travel records. By creating and analyzing this dataset, FIs can enhance their ability to efficiently identify patterns and trends associated with money laundering and other illicit activities.

In practice, FIs already share customers' personal financial information, such as credit card

---

[2] International Monetary Fund, IMF Policy Paper, 2023 Review of the Fund's Anti-Money Laundering and Combating the Financing of Terrorism Strategy (December 2023) <https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/12/05/2023-Review-of-The-Funds-Anti-Money-Laundering-and-Combating-The-Financing-of-Terrorism-542015>.

numbers, social security numbers, and transaction records, to prevent fraud and other financial crimes. A recent trend is to use such datasets to monitor suspicious transactions and detect money laundering. Against this background is the expansion of the AML/CFT regulations. Historically, the initial purpose of the rules in the 1970s was to suppress and prevent crime, mainly organized crime and terrorism.[3] Today, its goal is to hinder the movement of funds from unexplained sources.[4] Henceforth, FIs must collect and provide extensive information about customers and fund transfers.

1.2 The Demand for Private-to-Private Information Sharing

1.2.1 Sharing User Information in the Private Sector

Criminals typically exploit information gaps among institutions using multiple institutions located in different countries to conceal the origin of funds. In other words, institutions usually have a limited and fragmented picture of the transactions. Accordingly, many countries permit or even require in-group information sharing in a domestic context or as a cross-border practice. Institutions share this information with entities within the same corporate group. For instance, global credit and debit card brands require issuers to convey customer information to subsidiaries under internal rules. They share customer information when they engage in cross-border payments.[5]

The FATF's 40 Recommendations of 2012 provide detailed guidelines for countries to permit FIs to rely on third parties to take CDD measures.[6] Recommendation 17 stipulates that institutions must promptly gather necessary information about CDD measures, ensure that a third party can provide the required documentation on request, confirm the third party's compliance with CDD and record-keeping requirements, and consider country risk when choosing the third party's location. Supposing that the third party is within the same financial group, adheres to specific CDD, record-keeping, and AML/CFT requirements, and is supervised by a competent authority, then the FI may apply specific measures through its group program, potentially waiving the need for certain preconditions based on its ability to manage higher country risk.[7]

In addition, Recommendation 18 provides detailed guidelines for internal controls, foreign branches, and subsidiaries. Financial groups must implement group-wide programs for money laundering and terrorism financing, including policies and procedures for sharing information within the AML/CFT group. They must ensure that their foreign branches and majority-owned

---

[3] William C Gilmore, *Dirty Money : The Evolution of International Measures to Counter Money Laundering and the Financing of Terrorism* (3rd ed., Council of Europe Publication 2004).
[4] Tom Obokata, *Transnational Organised Crime in International Law* (Hart Publisher 2010); Juan Carlos Zarate, *Treasury's War : The Unleashing of a New Era of Financial Warfare* (Public Affairs 2013).
[5] FATF, Cross-Border Payments: Survey Results on Implementation of FATF Standards (2021), <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Cross-Border-Payments-Survey-Results.pdf>, paras. 87-88.
[6] FATF, *International Standards on Combating Money Launering and The Financing of Terrorism & Proliferation* (2012).
[7] *Ibid*., Recommendation 17.

subsidiaries apply AML/CFT measures consistent with the home country's requirements. Recommendation 21 further provides that FIs and their directors, officers, and employees can disclose that a suspicious transaction report (STR) or related information has been submitted so long as it meets group-wide AML/CTF risk management requirements as set out in Recommendation 18.

The recent development of information-sharing mechanisms involves data pooling among multiple institutions and entities and collaborative analytics using privacy-enhancing technologies (PET), such as cryptographical capabilities, and trusted enforcement environments, such as distributed ledger technology (DLT). Many countries and private entities have started pilot programs, often involving entities from various countries.[8]

1.2.2 Use of Artificial Intelligence

Artificial intelligence (AI) can enhance the effectiveness of AML efforts by analyzing vast amounts of financial data to detect suspicious transactions and patterns that may indicate money laundering activities. AI-driven solutions provide constant real-time monitoring of transactions and reduce manual reviews and operational expenses.

However, the risks of data-driven technologies that generate, record, process, share, and use large amounts of big data have been recognized. Profiling with data may harm personal privacy and safety by making it difficult for individuals to make autonomous choices. It may also foster social discrimination. For example, specific demographics or regions may be unfairly targeted, or legitimate transactions from marginalized groups may be flagged more frequently. Legislation and policies are increasingly being developed based on data ethics in technological design.[9]

To mitigate the risks described above, it is essential to implement robust governance and oversight mechanisms, regularly audit AI models for bias and accuracy, and invest in ongoing training and awareness of personnel involved in AML compliance. Additionally, regulatory bodies should provide clear guidelines and oversight to ensure the responsible use of AI in AML treatment efforts.

To this end, the Organisation for Economic Cooperation and Development (OECD) adopted a Council Recommendation on AI in May 2019,[10] which led to the launch of the Global Partnership on AI (GPAI) initiative by volunteer countries, including Japan and the EU, in June

---

[8] For instance, *see* Deloitte, "The Case for Artificial Intelligence in Combating Money Laundering and Terrorist Financing," <https://www2.deloitte.com/mm/en/pages/financial-advisory/articles/the-case-for-artificial-intelligence-in-combating-money-laundering-and-terrorist-financing.html>.

[9] Jessica Fjeld and others, "Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI" [2020] Berkman Klein Center for Internet & Society <https://dash.harvard.edu/handle/1/42160420>. Data ethics is the ethics of evaluating the issues around algorithms and formulating morally desirable directions, including the generation, recording, curation, processing, distribution, sharing, and use of data and information.

[10] OECD, *Recommendation of the Council on Artificial Intelligence* (22 May 2019) OECD/LEGAL/0449 <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>.

2020.[11] The European Commission also proposed a new regulation on AI in April 2021, which was adopted by the Parliament in December 2023.[12] Using AI to assess the trustworthiness of individuals based on their social behavior or personal characteristics, which leads to negative treatment in unrelated social contexts, is prohibited by public authorities or on their behalf for market purposes, service deployment, or general use.[13] Other efforts include establishing the OECD Expert Network,[14] creating a special committee in the Council of Europe,[15] and formulating guidelines at the national level.[16]

1.3 Potential Conflicts with Data Protection and Privacy Regulations

States increasingly promote collaboration among private-sector entities since the FATF adopted the 40 Recommendations in 2012. This practice involves encouraging these entities to combine their data resources and employ artificial intelligence technology to identify and filter suspicious customers and transactions. Information sharing can yield several benefits when executed effectively, including enhanced cybersecurity, innovation, and operational efficiency. However, this raises concerns regarding privacy, security, and competition, which must be carefully addressed and managed. Issues would be compounded if such information sharing became mandatory as part of the regulations.

It is also important to consider a situation in which information is shared across national borders. Effective information sharing depends on trust and robust data governance practices. Establishing trust among participants is vital for successful cooperation and transparent data governance policies ensure that shared information is used ethically and appropriately. Requiring operators to share such information could conflict with national privacy laws, other human rights norms, and data protection and privacy (DPP) legislation.

The tension between the AML/CFT regulations and privacy is not new. There have been writings on this topic since the 1990s, albeit in small numbers. Privacy laws would require the collection of information to be kept to the minimum necessary level. Nonetheless, the current demand of AML/CFT regulations for extensive data may conflict with principles of proportionality and minimalism. Moreover, with the digitalization of transactions and the adoption of financial technologies, new challenges emerge concerning the data subject's privacy and other fundamental rights.

The privacy issues have been mainly discussed in the context of the government access to

---

[11] The Global Partnership on Artificial Intelligence < https://gpai.ai>.

[12] EU, Artificial Intelligence Act, adopted on 9 December 2023. *See also* European Commission, White Paper on Artificial Intelligence: a European approach to excellence and trust (19 February 2020), < https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en>.

[13] Artificial Intelligence Act Article 6 provides classification rules for high-risk AI systems.

[14] OECD Network of Experts on AI (ONE AI) < https://oecd.ai/en/network-of-experts>.

[15] Council of Europe, CAHAI (Ad hoc Committee on Artificial Intelligence) <https://www.coe.int/en/web/artificial-intelligence/cahai>.

[16] *See* OECD AI Policy Observatory <https://oecd.ai> for country developments. *See also* OECD AI Principles <https://oecd.ai/en/ai-principles>.

business data (G2B relations). The exchange of information between the private sector (B2B relations) or the provision of information from government to the business sector (B2G relations) needs to be closely examined.

1.4 Structure of The Paper

Given this context, this study examines recent information-sharing practices in the private sector. This raises potential questions about situations arising within international law owing to possible conflicts with foreign data protection laws and privacy regulations.

Section 2 examines applicable rules and principles. Section 3 explores recent developments, including the FATF's efforts to collect and share data among the private sector and primary state practices, including legislation in the United States (US), the United Kingdom (UK), the European Union (EU), and China. Section 4 examines whether the general DPP principles should be adhered to in the context of AML/CFT regulations.

2 Applicable Data Protection and Privacy Principles

This section explores applicable data protection, privacy principles, and regulations concerning cross-border data transfer. While describing the details of this legislation is beyond the scope of this study, it is necessary to articulate rules that may conflict with the AML/CFT Regulations.

2.1 Data Protection and Privacy Principles

The DPP legislation establishes the security management obligations of businesses concerning data handling, including nonpersonal information.[17] Its primary purpose is to require companies to manage their data for industrial promotion and security. In general, challenges in pursuing AML/CFT regulations include identifying a lawful ground for processing personal data, complying with information requirements, protecting the client data collected through due diligence process, sharing client data with law enforcement agencies, and FI's complying with data subjects' access requests.

However, the content and scope of the right to privacy reflects each society's historical, political, and cultural values.[18] Whether this right is a constitutional right that prevails over other legal rules or whether a comprehensive privacy law exists varies by country. In the EU, the right to data protection is guaranteed under the Charter of Fundamental Rights. By contrast, some countries, such as China, use personal data to protect individual rights and maintain state sovereignty.[19] The US emphasizes allowing IT companies to use data to create new technologies and industries. It does not have a comprehensive data protection law at the federal level, but has

---

[17] China, Data Security Law (adopted on 10 June 2021) <http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml> and Information Technology Act 2000 (India), The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (India).

[18] Joseph HH Weiler, *The Constitution of Europe: 'Do the New Clothes Have an Emperor?' and Other Essays on European Integration* (Cambridge University Press 1999) 101.

[19] *See infra,* Section 3.4.

relevant laws in disciplinary areas and at the state level.[20]

The right to privacy is enshrined in many international human rights treaties, including the Covenant on Civil and Political Rights. However, it is limited to the right not to be subject to government censorship and not to have one's private life indiscriminately exposed to third parties.[21] In contrast, the right to privacy in the digital age allows individuals to manage their information more proactively, given the nature of data that are easily transferred, distributed, and accumulated in large quantities for utilization.[22] The right to privacy in the current digital age has not yet been established internationally.

However, recent years have witnessed international efforts to establish high standards of privacy rights.[23] Various factors from different backgrounds influenced this trend.

A significant element is the digitization of information, which potentially enables third parties to access information. The circumstances in which traditional privacy principles apply have changed significantly.[24] There have been substantial increases in data collection, usage, and storage. Data are now used extensively in analytics to provide insights into individual and group trends, movements, interests, and activities. Access to such data by many actors can jeopardize or safeguard privacy. Such data are globally accessible and facilitated by communication networks and platforms, allowing for continuous multipoint data flows. Such factors transformed the context in which the principles are applied, necessitating a reevaluation of privacy laws and policies.

In a broader context, one must consider the impact of digitization on the structure of AML/CFT regulations. The transformation of the DPP legislation in the wake of digitization has affected many legal areas in addition to AML/CFT regulations. While some regulations acknowledge privacy protection and human rights, this has only been achieved through the guarantee of due process. The superiority of the regulation has not yet been questioned. In contrast, their digitalization shows that the issues involve the extent to which AI determines AML risks without human judgement, and that data are shared across borders. Digitization can be seen as the potential for fundamental change, extending into governance structures. When countries decide on AML regulations and information sharing, they must also decide on these constitutional issues.

The impact of digital technology on the constitutional structures of social values is well recognized. Digital technology can be used to either enhance or detriment democratic values. For instance, the EU's Action Plan on Human Rights and Democracy 2020-2024 includes new technologies in its agenda. The EU clarified that "digital technologies must be human-centred and

---

[20] Robert Wolfe, "Learning about Digital Trade: Privacy and E-Commerce in CETA and TPP" (2019) 18 *World Trade Review* 63, 77.

[21] International Covenant on Civil and Political Rights (adopted on 16 December 1966, entered into force on 23 March 1976) 999 UNTS 171, art 19.

[22] For a distinction between privacy and data privacy, *see* Lee Andrew Bygrave, *Data Privacy Law* (Oxford University Press 2014) 3.

[23] *Ibid*., 31.

[24] Christopher Kuner, "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future," *OECD Digital Economy Papers*, Vol 187 (2011), <http://dx.doi.org/10.1787/5kg0s2fk315f-en>.

human rights compliant."[25]

Another factor is the impact of EU law, including Directive 95/46[26] and the General Data Protection Regulation (GDPR) of 2016, which mandates that information transfers must be performed between countries with an equivalent level of data protection. The GDPR has a long arm requiring companies with access to the EU market to comply with EU standards. To level the playing field with their domestic competitors, these corporations lobbied their local governments to implement robust data protection laws. This is a prime example of the Brussels effect, which is the significant influence of EU regulations and standards on cross-border business practices and policies.[27]

Against this background, the DPP legislation has expanded in major developed countries. The OECD took the lead in established privacy guidelines in 1980 to reconcile potential conflicts between the US and Member States of the European Community (EC). The OECD updated the Privacy Guidelines in 2013 to establish standards for digitized environments.[28]

Furthermore, the OECD adopted the Declaration on Government Access to Personal Data Held by Private Sector Entities in 2022. The seven principles listed in the Declaration include the legal basis, legitimate aims, approval, data handling, transparency, oversight, and redress. It specifically rejected "any approach to government access to personal data […] that […] is inconsistent with democratic values and the rule of law, and is unconstrained, unreasonable, arbitrary or disproportionate." Against this background is the rise of authoritarian regimes that use private sector data. This assessment is based on constitutional values. The OECD member states' approach to government access is "per democratic values; safeguards for privacy and other human rights and freedoms; and the rule of law including an independent judiciary."

Transaction-related data may not inherently qualify as personal information. Nevertheless, if the transaction record contains individuals' identities, then DPP legislation could apply as the default regulatory framework.

The AML/CFT regulations may cause several concerns when they required to collect extensive user data. The first concern is the possibility of excessive data collection. Although gathering information is crucial for identifying and preventing illicit financial activities, institutions may collect all data related to users' financial activities, which may not be relevant to

---

[25] EU Action Plan on Human Rights and Democracy 2020-2024, https://www.eeas.europa.eu/sites/default/files/eu_action_plan_on_human_rights_and_democracy_2020-2024.pdf. ("New technologies can contribute significantly to the protection and promotion of human rights and democracy, including by making public participation easier and more effective, increasing access to public services, facilitating the documentation of violations and abuses.")

[26] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals in regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, 31-50.

[27] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).

[28] OECD, "Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data" (2013), C(80)58/FINAL, 11 July 2013, C(2013)79.

searching for such unlawful activities. It could be problematic if institutions utilize the data for purposes beyond those that AML/CFT regulations require to derive additional benefits. Examples would include using profiles to assess customer credibility.

The second is data management, which includes handling, storing, and deleting collected data. Concerns have arisen about the security and confidentiality of financial information. Ensuring the adequate protection of these data is crucial for safeguarding individuals' privacy.

The third is oversight. In numerous jurisdictions, including Japan, the government agencies responsible for financial regulations and those overseeing personal information protection operate independently and typically do not collaborate. This results in a distinct gap between these two regulatory frameworks.

The FATF recommends that information collection be compatible with the applicable laws and regulations. Nevertheless, there is a need for further clarification regarding how the requirements for data collection can be harmonized in compliance with the DPP legislation.

2.2 Cross-Border Transfer of Data

Another issue is cross-border sharing of data. Different countries have varying levels of data protection regulations and sharing information across borders can expose individuals to different privacy standards, potentially leading to inconsistencies in the safeguarding of personal information.

It is important to sustain a consistent level of protection in line with the guidelines for the cross-border transfer of personal data between nations. These safeguards should include robust enforcement mechanisms and measures established by data controllers. Restriction should be avoided and the limitations on the cross-border sharing of personal data should be balanced with the existing risks while considering the data's sensitivity and the specific purposes and context of data processing.[29] In 2007, the Council issued the Recommendation on Cross-Border Cooperation in the Enforcement of Laws Protecting Privacy[30] to encourage member states to "cooperate across borders in the enforcement of laws protecting privacy."[31] To this end, there are

---

[29] Ibid paras. 17-18. *See also* Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) of 1981. The 2018 Amended Protocol amended the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 10 October 2018, CETS No. 223. The Asia-Pacific Economic Cooperation (APEC) has adopted the Cross-Border Privacy Protection Rule (CBPR), in which Japan, the US, South Korea, Taiwan, and other countries participate. For practice in Asia, see generally Graham Greenleaf, *Asian Data Privacy Laws* (Oxford University Press 2014); Graham Greenleaf, "Asia's Data Privacy Dilemmas: 2014-2019" (2019) 4 *Revista Uruguaya de Protección de Datos Personales* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3483794>.

[30] Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, adopted on 12 June 2007, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0352.

[31] More specifically, it recommends that states take appropriate steps to: (1) improve their domestic frameworks for privacy law enforcement to better enable their authorities to co-operate with foreign authorities; (2) develop effective international mechanisms to facilitate cross-border

bilateral and multilateral enforcement arrangements or memorandums of understanding (MOUs) to improve cooperation among privacy enforcement authorities, albeit the fact that the standards are not uniform. Regional efforts include the Asia-Pacific Economic Cooperation's Cooperation Arrangement for Cross-border Privacy Enforcement.[32]

More than 70 countries, including Japan, restrict cross-border transfers in some form in their personal data protection legislation.[33] Data can easily be transferred to another country's territory, and businesses can easily lose adherence to the personal data protection legislation of the source country if the data are not adequately protected in the destination country. It also provides an equal footing or level playing field for domestic and foreign operators.

For example, the EU GDPR established rigorous requirements for cross-border data transfer, which must have a legitimate legal basis as provided by regulations. First, personal data can only be transferred to countries or organizations with adequate data protection. Adequacy is determined by the European Commission, which assesses whether the recipient country or organization's data protection laws and practices meet the GDPR standards. Second, if the data transfer is to a country without an adequacy decision, then organizations may use standard contractual clauses (SCCs) approved by the European Commission. SCCs are predefined legal agreements that ensure that data-protection standards are met. Third, multinational organizations can implement binding corporate rules (BCRs) and internal data protection policies approved by EU data protection authorities. BCRs allow for intragroup data transfer while maintaining GDPR compliance. In certain cases, a data-protection impact assessment is required before data transfer. This assessment evaluates the potential risks to individuals' rights and freedoms when transferring data.

The data subjects retain their rights even when their data are transferred. They can exercise their right to access, rectify, erase, or restrict the processing of data and objects to transfer. Data controllers must inform data subjects about the transfer, including its purpose, categories of data transferred, recipients, and how they can exercise their rights. Adequate security measures must be implemented to protect data during transfer. This includes encryption, access control, and other technical and organizational measures. First, personal data can only be transferred to countries or

---

privacy law enforcement cooperation; (3) provide mutual assistance to one another in the enforcement of laws protecting privacy, including through notification, complaint referral, investigative assistance and information sharing, subject to appropriate safeguards; and (4) engage relevant stakeholders in discussion and activities aimed at furthering co-operation in the enforcement of laws protecting privacy.

[32] Asia-Pacific Economic Cooperation, Cooperation Arrangement for Cross-border Privacy Enforcement <https://www.apec.org/groups/committee-on-trade-and-investment/digital-economy-steering-group/cross-border-privacy-enforcement-arrangement>.

[33] Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013) 1. For domestic legislation information for major countries, see Personal Data Protection Commission, "Survey of Systems for the Protection of Personal Data in Foreign Countries," <https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/>. *See also* "Survey on Transborder Transfer of Personal Data in Japan, the United States, and Europe" (January 27, 2022) by the Personal Information Protection Commission (Nomura Research Institute, Ltd.) <https://www.ppc.go.jp/files/pdf/nichibeiou_ See ekkyouiten_report.pdf>.

organizations that provide adequate data protection. Adequacy is determined by the European Commission, which assesses whether the recipient country or organization's data protection laws and practices meet the GDPR standards. The GDPR influenced many countries to adopt higher standards for the DPP legislation because of its broad jurisdictional scope.[34]

Most countries do not prohibit cross-border data transfers *per se* but rather impose conditions on the transfer. Such conditions typically require the consent of the concerned person. However, in light of the asymmetry of the information held by operators and users, and the formalization of approval, there are problems with allowing transfers if consent is obtained, regardless of the operator's system or the country in which the data are being transferred. Therefore, it is often required that the government in the relocation destination ensure that its legal system is secure, or that the operator of the relocation destination has taken appropriate security control measures. In determining their adequacy, they may refer to international standards such as the APEC Cross-Border Privacy Rules (CBPR).[35] While these rules are an important mechanism enabling operators to transfer data across borders within APEC economies, their protection level is not deemed sufficient by the GDPR standards.

In addition to privacy protection regulations, some laws require businesses to have the necessary equipment to conduct business in their home country, and the data collected in their home country must remain there. Such data are not limited to personal data but may include business and industrial data. The reasons vary from a country to another. Examples include raising barriers to entry for companies from other countries, protecting their industries by imposing such regulations, and preventing sensitive data from being taken to other countries for security reasons.

Such legislation encompasses various types of regulations that (1) require data to be retained within the home country; (2) mandate data processing and storage exclusively within the home country, along with the installation of necessary facilities; and (3) extend beyond (2) by prohibiting the export of data or certain items outside the country.[36]

Whether it is the regulation of cross-border transfers in personal data protection legislation or the obligation to store data in a country with data protection legislation, it is impossible to categorically determine whether an AML/CFT regulation or measure conflicts with such DPP legislation. Therefore, a substantive examination in terms of content, purpose, and effects is necessary.

---

[34] Bradford (n 27).

[35] Thailand is one country that uses the CBPR as a benchmark. Thailand, Personal Data Protection Act, 2019, Sec. 28. See the following as an unofficial English translation: Personal Data Protection Act, B.E. 2562 (2019). (Unofficial Translation) (27 May 2019), <https://thainetizen.org/wp-content/uploads/2019/11/thailand-personal-data-protection-act-2019-en.pdf>. For a study analyzing the practices of Asian countries, *see* Graham Greenleaf, *Asian Data Privacy Laws* (Oxford University Press 2014); Graham Greenleaf, 'Asia's Data Privacy Dilemmas: 2014-2019' (2019) 4 *Revista Uruguaya de Protección de Datos Personales* 49.

[36] Kuner (n 24).

2.3 The FATF's Approach

The FATF standards are crafted with the primary objective of curbing the movement of funds with undisclosed origins. While the FATF emphasizes the importance of privacy, it merely requires member states to comply with applicable DPP legislation. The organization is not mandated to designate how to reconcile these potentially conflicting demands.

After the FATF adopted its 40 Recommendations in 2012,[37] it advocated that FIs share information concerning financial activities with potential connections to criminal activities. These proposals are reflected in FATF Recommendations and Immediate Outcomes. The FATF acknowledges the numerous legal limitations and operational hurdles that hinder the efficient sharing of information among various FIs within the same corporate group and the exchange of information between unaffiliated institutions.

In light of these potential obstacles, the FATF issued a report in 2017 to articulate how to align the demands for information sharing, FATF Recommendations and DPP legislation.[38] The report includes case studies and examples of collaborations with the authorities responsible for data protection and privacy. In addition to this report, it published several guidelines and documents concerning information sharing among private sector members.[39]

The FATF proposes overarching recommendations for information sharing and collaborative analytics to improve the effectiveness of AML/CFT.[40] The first is to prepare a data protection impact assessment (DPIA) to define the purpose and objectives of information sharing; the data to be processed; why such data are necessary, reasonable, and proportional to achieve the purpose; and the legal basis and safeguards. The second is to engage with the DPP authorities from the beginning of the sharing project at the design stage. The third objective is to examine safeguards to adequately protect customer data. FATF is aware that no one-size-fits-all solution addresses all the AML/CFT/CPF and DPP objectives for all FIs at the global level.

Furthermore, the FATF adopted the San Jose Principles, a set of guidelines to promote cooperation between the public and private sectors concerning the use of innovative financial technologies, including AI and blockchain, and seeks a balance to encourage technological innovation and the management of AML/CFT risks. Most notably, it aims for a regulatory environment that is commercially neutral, respects the level playing field, and minimizes regulatory inconsistency, both domestically and internationally.

---

[37] FATF, *International Standards on Combating Money Launering and The Financing of Terrorism & Proliferation* (n 6).

[38] FATF, "FATF Guidance: Private Sector Information Sharing" (2017) <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private-Sector-Information-Sharing.pdf.coredownload.pdf>.

[39] FATF, "FATF Recommendations 18 and 23: The Application of Group-Wide Programmes by Non-Financial Businesses and Professions, Explanatory Materials" (2021) <https://www.fatf-gafi.org/content/dam/fatf/documents/recommendations/pdfs/Explanatory-Materials-R18-R23.pdf>.

[40] FATF, "Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing" (July 2022), <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf>.

However, privacy issues are not the primary concern of the FATF standards and regulations. This is evident in the FATF's fourth mutual evaluations, which occurred from 2020 to 2021.[41] From the fourth evaluation, the FATF introduced the Immediate Outcome to assess whether the country actually implemented the FATF recommendations and standards through FIs, other non-financial entities, and law enforcement authorities. On the other hand, it basically defers the privacy issues to the domestic laws of each state and do not necessarily specify the principles or guidelines when its requirements and the DPP legislation of relevant states conflict with each other.

3 Recent Developments

There is no binding international agreement governing information sharing in the private sector. Therefore, it is important to observe developments in major countries. Several countries are aiming to establish information-sharing mechanisms to the extent that such initiatives do not necessitate the enactment of new legislation. For example, the Monetary Authority of Singapore has been developing a digital platform called the Collaborative Sharing of Money Laundering/Terrorism Financing (ML/TF) Information & Cases (COSMIC), with six major commercial banks operating in Singapore: DBS, OCBC, UOB, SCB, Citibank, and HSBC.[42] This will allow FIs to share information on customers who show signs of potential financial crime. In the Netherlands, five major banks (ABN AMRO, ING, de Volksbank, Triodos Bank, and Rabobank) decided to establish the Transaction Monitoring Netherlands (TMNL) system in 2020.[43] This will enable FIs to monitor transactions across banks and institutions and identify suspicious transactions. Besides these leading examples, this section explores the major state practices that promote the private sector's collection and sharing of information on AML/CFT regulations.

3.1 The United States

3.1.1 AML/CFT Regulations

The US is the leading state in AML/CFT regulations and the most influential, as it holds the dollar clearing system and affects global financial transactions. The Bank Secrecy Act of 1970 first established the obligations of customers regarding the diligence and suspicious transaction reporting of institutions. The initial form of regulation required FIs to implement due diligence and report suspicious transactions.

However, the 9.11 terrorist attacks in 2001 were the turning point for AML/CFT regulations

---

[41] Mutual evaluations are peer reviews, where members from different countries assess another country's AML/CFT regulations. The assessed country must demonstrate that it has an effective framework for compliance. For an overview of the mutual evaluation mechanisms and the evaluation reports, *see* FATF, Mutual Evaluations, <https://www.fatf-gafi.org/en/publications/Mutualevaluations/More-about-mutual-evaluations.html>.

[42] Monetary Authority of Singapore, "COSMIC,"' <https://www.mas.gov.sg/regulation/anti-money-laundering/cosmic>.

[43] Transactie Monitoring Nederland B.V. (TMNL), <https://tmnl.nl/en/about-tmnl/>.

in the country. To monitor funds that could be used for terrorist activities and to prevent such crimes, the government implemented various measures to prevent the untraceable movement of money.

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001, enacted in response to the 9.11 attack, established a private-to-private information-sharing mechanism.[44] The law exempts the liability of institutions under US law and any contract or other legally enforceable agreements, including arbitration agreements, for such disclosures or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure. Section 314(b) allows FIs to share information under a safe harbor that offers protection from liability to better identify and report activities that may involve money laundering or terrorist activities. FIs may notify the Treasury Department of Registration. According to Section 314(b), participation in information sharing is voluntary, although the Financial Crimes Enforcement Network (FinCEN) encourages FIs to participate.

In 2020, the US updated its AML/CFT significantly under the Anti-Money Laundering Act (AMLA). [45] The Act provides on public-private information sharing, including through FinCEN,[46] a new Subcommittee on Innovation and Technology under the Bank Secrecy Act Advisory Group,[47] a Financial Crimes Tech Symposium[48] among others.[49]

The new regulation allows FIs to share details on suspicious transactions with overseas branches, subsidiaries, and affiliated entities. The law also requires the FinCEN, the financial intelligence units, and the Treasury to conduct a three-year study on the impact of information-sharing.[50] It requires the Secretary of the Treasury, in coordination with the FinCEN Director, to issue rules establishing a pilot program to permit financial institutions subject to BSA reporting requirements to share SARs and related information otherwise subject to SAR confidentiality limitations with their foreign branches, subsidiaries, and affiliates.[51] However, participating FIs may not share SAR information with foreign branches, subsidiaries, or affiliates located in prohibited jurisdictions, including China, Russia, a state sponsoring terrorism, a state that is subject to US sanctions, any jurisdiction identified by FinCEN as a primary money laundering concern, and jurisdictions the Secretary determines cannot reasonably protect the security and confidentiality of the relevant information.[52] In January 2022, FinCEN issued a notice seeking public comments on the proposed establishment of a limited-duration pilot program that permitted an FI with a suspicious activity report (SAR) reporting obligation to share SAR-related

---

[44] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56.
[45] Anti-Money Laundering Act of 2020 (AML Act), National Defense Authorization Act (NDAA) for FY2021, Division F, Pub .L. 116-283.
[46] *Ibid*., Section 6103.
[47] *Ibid*., Section 6207.
[48] *Ibid*., Section 6211.
[49] *Ibid*., Sections 6214 and 6306.
[50] *Ibid*., Section 6212.
[51] *Ibid*.
[52] *Ibid*.

information with its foreign branches, subsidiaries, and affiliates to combat illicit finance risk.[53]

3.1.2 DPP Legislation

However, the US does not have comprehensive data protection laws at the federal level. The country lacks a single data protection authority. Instead, it relies on a patchwork of laws and regulations covering various aspects of data privacy and security. Governance is based on a decentralized approach.

The Gramm-Leach-Bliley Act (GLBA) requires FIs to protect the privacy of consumers' financial information and inform them about their privacy practices. Most FIs, including banks, credit unions, and brokerage firms, are subject to GLBA and AML/CFT regulations. These institutions must comply with the provisions of the GLBA to safeguard customer financial information and the AML regulations to detect and prevent money laundering activities.

The GLBA requires FIs to maintain customer information privacy. The law generally restricts the sharing of nonpublic personal information, requiring institutions to obtain consent from customers before sharing such data with third parties. However, there are exceptions to sharing information for AML purposes. Therefore, FIs can share customer information with other entities to fulfil their AML obligations without customer consent. FIs must have robust security measures under the GLBA and require effective monitoring and reporting systems to fulfil their AML obligations.

Many US states have their own data protection laws at the state level. However, data breach notification laws typically require entities to inform users if their personal information has been compromised.[54] Therefore, the potential conflict between the AML/CFT regulations and DPP regulations has not been raised.

3.2 European Union

3.2.1 AML/CFT Regulations

In the EU, the inclusion of the Schengen Agreement in EU law catalyzed a significant boost in judicial cooperation. This was driven by both the pressing need to combat organized crime and the desire to enhance money-laundering controls within the EU. Notably, the establishment of specific economic crime regulations within the EU aimed at curbing fraud against the EU also played a role in this development.

In 1990, the Council of Europe (CoE) adopted the Convention on the Laundering, Search, Seizure, and Confiscation of the Proceeds of Crime.[55] The Convention contains detailed

---

[53] FinCEN, Pilot Program on Sharing of Suspicious Activity Reports and Related Information With Foreign Branches, Subsidiaries, and Affiliates, 87 FR 3719, https://www.federalregister.gov/documents/2022/01/25/2022-01331/pilot-program-on-sharing-of-suspicious-activity-reports-and-related-information-with-foreign.

[54] For instance, California has one of the most comprehensive state privacy laws, the California Consumer Privacy Act (CCPA), which gives California residents certain rights over their personal information held by businesses.

[55] Convention on the Laundering, Search, Seizure, and Confiscation of the Proceeds of Crime, signed 8 November 1990, entered into force 1 September 1993, CETS 141. *See also* Council of Europe, *Explanatory Report on the Convention on Laundering, Search, Seizure and Confiscation*

provisions for mutual assistance obligations. All EU member states ratified it and considered it a part of the law that applies between them. Mutual assistance provisions entail exchanging information on the existence, location, nature, legal status, and price of crime proceeds and converted objects. The specifics of mutual assistance include identifying and tracing proceeds.[56]

Starting in 1990, the European Community implemented extensive measures to combat money laundering within its borders. The first action taken was a Council Directive that obligated member states to act against the laundering of proceeds from drug trafficking under the 1988 Drug Convention.[57] This directive also imposed various requirements on FIs based on the FATF recommendations issued in 1990. These obligations include verifying the identities of customers, keeping records, prohibiting suspicious transactions, and reporting transactions.

Efforts to combat money laundering were strengthened in the late 1990s through Pillar III of the EU Treaty, which was built on the 1990 Directive. This was accomplished through the adoption of the 1998 Joint Action by the European Council[58] and the 2001 EU Framework Decision.[59] The latter extends the scope of predicate offences to include serious crimes. In 2001, the Council passed a directive criminalizing actions constituting the predicate offences identified in the 2001 Framework Decision.[60] In response to the FATF's 2003 Recommendation, a new directive was adopted in 2005 to harmonize legislation in EU member states relating to the financing of terrorism.[61] In 2015, the EU modernized its regulatory framework in response to the 2012 FATF 40 Recommendations.[62] This includes the Fourth Anti-Money Laundering Directive (AML4)[63] and Regulation 2015/847, which include the obligation to share information within a group of FIs.[64]

The Fifth Anti-Money Laundering Directive (AML5) of 2018 further expanded the obligation of information sharing among groups.[65] One of the purposes includes improving cooperation and

---

of the Proceeds from Crime (Council of Europe Publishing 1991) 22 para 35.

[56] UNODC & IMF, 'Model Legislation on Money Laundering and Financing of Terrorism' (2005).

[57] Council Directive 91/308/EEC, OJ L 166/77.

[58] 98/699/JHA, Joint Action of 3 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds from crime, OJ L 333, 1-3, 29 December 1998.

[59] 2001/500/JHA, Council Framework Decision of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime, OJ L 182, 1–2, 5 July 2001.

[60] Council Directive 2001/97/EC, OJ L 344/76.

[61] Council Directive 2005/60/EC, OJ L 309/15. *See also* Gilmore (n 3) 189.

[62] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-countering-financing-terrorism_en.

[63] Directive 2015/849.

[64] Article 45(8) ("[m]ember States shall ensure that information sharing 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").

[65] Directive 2018/843.

enhance communication among entities.[66] Article 39(3) provides exceptions prohibiting information sharing with third parties. It consists of the disclosure between credit and FIs from member states as long as they belong to the same group, or between those entities and their branches and majority-owned subsidiaries established in third countries. Additionally, these branches and majority-owned subsidiaries must fully comply with the group-wide policies and procedures and that the group-wide policies and procedures comply with the requirements set out in this directive.

In 2021, the European Commission submitted an AML/CFT regulatory proposal.[67] Chapter II, on the internal policies, controls, and procedures of obliged entities, provides the regulation of group information sharing. It requires that "[t]he group-wide policies, controls and procedures shall also include data protection policies and policies, controls and procedures for sharing information within the group for AML/CFT purposes."[68] The sharing of information within the group shall cover the identity and characteristics of the customer, its beneficial owners, or the person on behalf of whom the customer acts; the nature and purpose of the business relationship; and the suspicion that funds are the proceeds of criminal activity or related to terrorist financing reported to the FIU. Groups must establish comprehensive group-level policies, controls, and procedures to ensure that the information exchanged as per the initial clause receives adequate safeguards for confidentiality, data protection, and proper use.

Where branches or subsidiaries of obliged entities are located in third countries, where the minimum AML/CFT requirements are less strict than those set out in this regulation, the obliged entity concerned shall ensure that those branches or subsidiaries comply with the regulation requirements, including provisions concerning data protection or the equivalent.[69]

Where the law of a third country does not comply with the requirements of this regulation, obliged entities shall take additional measures to ensure that branches and subsidiaries in that country effectively handle the risk of money laundering or terrorist financing, and the head office shall inform the supervisors of their home member states. Where the supervisors of the home member state consider that the additional measures are not sufficient, they shall exercise other supervisory actions, including requiring the group not to establish any business relationship, terminate existing ones, or not to undertake transactions, or close down its operations in the third country.

Furthermore, the proposal specifies that the AMLA should develop draft regulatory technical standards and submit them to the Commission for adoption. These draft regulatory technical standards specify the type of additional measures, including the minimum action to be taken by obliged entities where the law of a third country does not permit the implementation of group-

---

[66] Preamble Paragraph 46 ("it is important to allow credit and financial institutions to exchange information not only between group members but also with other credit and financial institutions, with due regard to data protection rules as set out in national law").

[67] COM/2021/420 final, available at ttps://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420.

[68] Proposal, Article 13(1).

[69] *Ibid*., Article 14.

wide information sharing and the additional supervisory actions needed in such cases.

3.2.2 DPP Legislations

As mentioned in Section 2, the EU has the most robust DPP legislation. Private life and personal data protection are rights provided for in the EU Charter of Fundamental Rights.[70] It states that "[s]uch data must be processed fairly for specified purposes"[71] and "[c]ompliance with these rules shall be subject to control by an independent authority."[72] The AML measures must be compatible with the charter and case law of the Court of Justice of the European Union (CJEU).

Article 6 (1) of the GDPR provides principles for lawful data processing. Data subjects must provide consent for the processing of their personal data for one or more specific purposes, among other requirements. In addition, processing is necessary for the execution of a contract to which the data subject is a party, or to take steps at the request of the data subject prior to entering a contract. The implementation of the AML/CFT regulations meets these requirements.

The European Data Protection Board (EDPB) issued a statement noting that the required measures for anti-money laundering encompass extensive and comprehensive duties for financial services providers and other obligated parties. These duties involve identifying and understanding their customers, overseeing transactions conducted through their services, and reporting any transactions that raise suspicions. [73] Furthermore, the legislation stipulates a long retention period.[74] These measures cover the entire European financial services industry and therefore comprehensively affect all people using financial services each time they use them.[75]

In this context, the EDPB stresses that the intended update to the AML/CFT framework should not be undertaken without reviewing the relationship between anti-money laundering measures and the rights to privacy and data protection. The relevance and accuracy of the collected data play a paramount role in this discussion. A closer articulation between the two sets of rules will benefit the protection of personal data and the efficiency of the AML framework. In this respect, the EDPB reiterates the need for a clear legal basis for the processing of personal data that states the purposes and limits of such processing, in line with Article 5(1) of the GDPR. In particular, clarity is needed for information sharing and international transfer of data.

The European Data Protection Supervisor also addressed its views on the European Commission's action plan for a comprehensive union policy on preventing money laundering and

---

[70] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391-407, Articles 7 and 8(1).
[71] *Ibid*., Article 8(2).
[72] *Ibid*., Article 8(3).
[73] The European Data Protection Board, 'Statement on the Protection of Personal Data Processed in relation with the Prevention of Money Laundering and Terrorist Financing,' adopted on 15 December 2020,
<https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_20201215_aml_actionplan_en.pdf>.
[74] *Ibid*.
[75] *Ibid*.

terrorism financing.[76] It emphasizes the importance of ensuring rigorous and effective implementation of AML/CFT rules. Full compliance with DPP frameworks is a part of such an effort. The setting of the databases of a high amount of personal data should be compatible with the principle of accuracy, which is set by Article 5(1)(d) of the GDPR. It stressed that the regulations should be also attuned with the principles of proportionality, data protection-by-design, and accountability as provided under Article 6(1) of the GDPR.

The Court of Justice of the European Union (CJEU) judgements concerning AML measures show the court's stance that disclosing an individual's data to a third party is a serious intrusion and that the Court will carefully scrutinize any such disclosure. In its judgement in 2022, the CJEU Grand Chamber held that the provisions of Directive 2018/843 concerning the publication of beneficial ownership registers[77] were incompatible with the Charter of Fundamental Rights.[78] The Court found that while deterring money laundering was a valid objective, making the data available to the general public was neither a necessary nor a proportionate way of achieving that objective and was, therefore, contrary to the charter. According to this judgement, FIs and other operators must limit the scope of disclosure in light of the principle of necessity.

In a broader context, information sharing relates to the EU Digital Single Market, an effort that began in 2015 to integrate national digital markets. The three policy pillars are to improve access to digital goods and services; create an environment for digital networks and services by providing high-speed, secure, and trustworthy infrastructure and services; and maximize the growth potential of the digital economy. The AML/CFT regulations will also align with these policies.

3.3 United Kingdom

3.3.1 AML/CFT Regulations

The UK, a major financial center, has rigorous AML/CFT regulations. The UK criminalized the laundering of proceeds from drug offences through the Drug Trafficking Offences Act of 1986[79] and the Criminal Justice Act of 1990.[80] The Proceeds of Crime Act 2002, amended in 2005, further criminalized concealing the source of an offence above a specified amount. Its basis is the Terrorism Act 2000 (TA 2000); Proceeds of Crime Act 2002 (POCA 2002); Money Laundering, Terrorist Financing, and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR

---

[76] EDPS, Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, para. 3.1, available at https://edps.europa.eu/sites/edp/files/publication/20-07-23_edps_aml_opinion_en.pdf.

[77] Directive 2015/849 requires that EU member states establish a register of beneficial ownership (RBO) containing personal data about the owner of each legal entity, including their name, nationality, and ownership interest, and to make the RBO available to a range of financial entities such as banks. Furthermore, Directive 2018/843 allowed the member states to access the RBO, regardless of whether they could demonstrate a legitimate interest.

[78] C-37/20 and C-601/20, 22 November 2022.

[79] Drug Trafficking Offences Act of 1986, c.32.

[80] Criminal Justice (International Co-operation) Act 1990, c.5.

2017);[81] and Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (MLR 2019). The MLR 2017 and MLR 2019 were enacted to implement the rules established under the Fourth and the Fifth EU AML Directives, respectively. It also enacted the Criminal Finances Act 2017, which amended the Proceeds of Crime Act 2002 for confiscating terrorist property and proceeds of tax evasion. The law introduced an unexplained wealth order, which the court issues to compel the target the reveal the sources of their wealth.

The latest MLR, 2019, significantly expanded the scope of the application and CDD obligations provided under the MLR 2017. It provided that firms must have "policies, controls and procedures to identify and scrutinize transactions which are complex or unusually large or have unusual patterns of transactions or which have no apparent economic or legal purpose." It then states that firms must have group-wide policies, controls, and procedures for sharing information about clients with other group companies for AML/CTF purposes.

In 2014, the government launched the Forum is the Joint Money Laundering Intelligence Taskforce (JMLIT), a pilot project developed by the Home Office, National Crime Agency (NCA), City of London Police, British Bankers' Association (BBA) and other FIs. It aims to improve intelligence-sharing arrangements for AML/CFT regulations. Today, it covers more than 40 FIs and law enforcement agencies.[82] According to the National Economic Crime Centre, "JMLIT has supported and developed over 950 law enforcement investigations which has directly contributed 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 money laundering activity, and commenced over 6,000 of their own internal investigations."[83]

The Criminal Finances Act of 2017 allows the regulated sectors, including banks, lawyers, and accountants, to share information between themselves on a voluntary basis, where they have a suspicion of money laundering.[84] It also allows the National Crime Agency to seek information concerning money laundering on a voluntary basis from across the regulated sector.

The UK also has rigorous legislation in place to prevent and combat fraud. The UK's Cifas is essential for information sharing on fraudulent crimes directly connected to money laundering. Cifas is a non-profit organization with over 400 members who share fraud and financial crime data to prevent, deter, and detect fraud and broader financial crimes.[85] The organization manages the National Fraud Database, which is the largest fraud risk database.[86] Member organizations post cases of fraudulent conduct against their organizations in the relevant database, enabling other members to compare their own data. Data and intelligence are shared in real-time and are

---

[81] SI 2017/692. See also https://www.lexisnexis.co.uk/legal/guidance/aml-data-protection.

[82] National Economic Crime Centre, https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre.

[83] *Ibid*.

[84] Criminal Finances Act 2017, c. 22, Section 11.

[85] Evidence submitted by Cifas (ECR0037), <https://committees.parliament.uk/writtenevidence/89879/html/>.

[86] Cifas website, <https://www.cifas.org.uk/fraud-prevention-community/member-benefits/data/nfd>.

always available online.[87] The database contains first- and third-party fraud risks, such as account takeover, identity fraud, false insurance claims, and false applications.[88] However, the issue concerning cross-border data sharing remains because Cifas's abilities are limited to conduct within the UK. FIs can earmark funds exiting the UK but cannot follow the proceeds of crime.

3.3.2 DPP Legislation

The UK DPP legislation may similarly pose challenges in pursuing AML/CFT regulations, including sharing data with law enforcement agencies and other institutions.[89] After the EU adopted the Data Protection Directive of 1995, the UK had established the Data Protection Act of 1998.[90] When it left the EU, the UK enacted the Data Protection Act (DPA), which is equivalent to the GDPR. It has robust data protection principles, which require the use of information to be fair, lawful, and transparent. However, information sharing under the AML/CFT regulation, as described above, is exempt from the DPA. Therefore, the AML/CFT regulation and the DPP legislation do not conflict, at least formally.

3.4 China

3.4.1 AML/CFT Regulations

China enacted its Anti-Money Laundering Act in 2006. Most recently, it published a draft updating the legislation in 2021.[91] The provision of customer identification data, transaction information and investigative information obtained per AML obligations to other "units" is required by law.[92]

The AML Monitoring and Analysis Center of China's FIU is responsible for managing a centralized and unified national AML information database and for taking measures necessary to maintain the security of AML information.[93]

---

[87] *Ibid*.
[88] *Ibid*.
[89] *See in general* LexisNexis Risk & Compliance expert, AML and Data Protection, <https://www.lexisnexis.co.uk/legal/guidance/aml-data-protection>.
[90] In 2002, the government issued Guidance Notes for the Financial Sector concerning the UK's anti-money laundering legislation and the Data Protection Act of 1998. The main issue here was, however, "the relationship between the obligation not to 'tip off' an individual about whom a Suspicious Transaction Report (STR) has been made on the one hand, and the individual's right of access to his personal data and the corresponding obligations on financial institutions on the other." The UK's Anti-Money Laundering Legislation And The Data Protection Act 1998, Guidance Notes For The Financial Sector, April 2002, para. 2, <https://assets.publishing.service.gov.uk/media/5a7ca3e140f0b6629523ad9a/money_laundering_1_.pdf>.
[91] Anti-Money Laundering Act [中华人民共和国反洗钱法], < https://www.gov.cn/jrzg/2006-10/31/content_429245.htm >.
[92] Anti-Money Laundering Act (n 91), Article 6.
[93] Ibid., Article 14. The center's main duties include (1) collecting, collating, and preserving information on large-value and suspicious fund transactions and related investigations and case information; (2) analyzing and studying information on large-value and suspicious transactions,

The administrative department of the State Council in charge of anti-money laundering may obtain the necessary information from relevant state agencies, departments, and institutions, and applicable state agencies, departments, and institutions shall provide such data per law.[94] Companies, enterprises, and other market entities shall report beneficial ownership information through the relevant information systems of the market supervision and management departments.[95] When FIs identify customers through third parties, they shall do so by investigating the CDD management capabilities of such third parties.[96] Other detailed rules exist regarding the handling of customer information.[97] The State Council may supervise and control FIs established in China and their foreign branches.[98]

China enacted the Measures for the Supervision and Administration of Anti-Money Laundering and Counter-Terrorist Financing of Financial Institutions in August 2021. This was a response to the FATF's fourth mutual evaluation, from 2018 to 2019. It enlarged the scope of organizations subject to regulation to include loan companies, asset management subsidiaries of commercial banks, non-banking payment institutions, insurance agents, and insurance brokers.

It also provides for the sharing and use of information by organizations according to laws and regulations.[99] If the local law is stricter for foreign subsidiaries and branches, it is followed. If this restricts or prohibits the implementation of these laws, then the head office must take appropriate supplementary measures to combat AML and report them to the People's Bank of China.[100]

3.4.2 DPP Legislation

Since the late 2010s, China has updated its DPP legislation to address the growing importance of digital technology. The key DPP legislation includes the Cybersecurity Law of 2017, the Personal Information Protection Law (PIPL) of 2021, and the Data Security Law of 2021. The PIPL sets comprehensive rules for processing personal information, including consent requirements, data subject rights, cross-border data transfers, and the appointment of data protection officers. It resembles the GDPR, but its purpose is to protect national sovereignty and data security, reflecting China's approach. The data security laws include provisions concerning the export of controlled

---

examining and consulting with relevant departments on clues about suspicious fund transactions, and cooperating with relevant departments in conducting joint investigations on clues of suspicious fund transactions; (3) studying and analyzing the ways, means, and development trends of anti-money laundering crimes, and providing the basis for the formulation of anti-money laundering policies; and (4) researching and formulating technical standards for reporting information on large-value and suspicious transactions in conjunction with relevant departments. *See* "反洗钱中心简介," <http://www.pbc.gov.cn/fxqzhongxin/3558093/3558095/index.html>.

[94] Anti-Money Laundering Act (n 91), Article 15.
[95] Ibid., Article 17.
[96] Ibid., Article 29.
[97] Ibid., Chapter 3.
[98] Ibid., Article 24.
[99] Ibid., Article 12.
[100] Ibid., Article 13.

data, and security reviews for data processing. In particular, it prohibits operators of important infrastructures from transferring critical data relevant to national security without government authorization.

3.5 Summary

Currently, there is a lack of established international laws specifically addressing human rights norms within the framework of AML/CFT regulations. The concept of democratic values serves as a cornerstone in developed countries, including the G7 member states, where these principles are deeply embedded in governance and societal structures. However, some states diverged from this approach by opting for more authoritarian regulatory practices. These differing perspectives are at the core of the complex approaches to financial regulation and human rights considerations.

4 Concluding Remarks

The analysis highlights the importance of data protection and the constitutional value of privacy, notwithstanding the fact that these elements are often considered secondary in the context of AML/CFT regulations, as law enforcement authorities find it difficult to collect information. However, in practice, there seems to be little dispute concerning two areas of law: AML/CFT regulations and DPP legislation. FIs should be capable of complying with former regulations while respecting the latter principles.

The analysis of this report has a direct relevance to Japan's policy on information sharing among private FIs. Such regulations concerning the use of data by the FIs have developed in recent years. The information sharing among a group corporation, including the cross-border sharing, is governed by the Financial Service Agency's Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism (the FSA Guidelines), last updated in 2021.[101] FIs are generally obliged not to disclose the customer's information to a third party. In addition, Personal Information Protection Act in principle prohibits the operators from disclosing personal information.[102] However, the exceptions include the case when there is a legal basis, which includes the established AML/CFT regulations and financial crime investigation purposes. No conflict exists between these regulations and DPP legislation formally.

The Japanese government plans to advance towards more active information sharing among FIs.[103] The FSA Guidelines, provides on FIs' obligations concerning remittance and the

---

[101] Financial Services Agency, Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism, Provisional Translation, July 19, 2021, < https://www.fsa.go.jp/common/law/amlcft/210730_en_amlcft_guidelines.pdf>.

[102] Act on the Protection of Personal Information Act, No. 57 of 2003.

[103] In 2019, the Banking Act was amended to enable FIs to provide customers' information, both natural and legal persons, to a third party. Banking Act, Act No. 59 of 1981, Article 10(2)(xx). *See* a report of a working group established under the Institute for Monetary and Economic Studies, Bank of Japan, Kin'yū Sābisu ni okeru Kokyaku Jōhō no Riyou o Meguru Hōritsu Mondai Kenkyūkai, *Hōkoku-sho: Kokyaku Jōhō no Rikatsuyō ni kansuru Kōi Kihan no Arikata Kin'yū Sābisu ni okeru Kokyaku Jōhō no Riyou o Meguru Hōritsu Mondai Kenkyūkai* [Japanese], <https://www.imes.boj.or.jp/research/papers/japanese/kk40-1-1.pdf>.

recommendation on the pro-active use of fintech.[104] In addition, in 2022, Japan amended Payment Services Act which allows FIs to share the customer's information for the monitoring suspicious transactions with funds transfer transaction analysis service provider.[105] The provider, as authorized by the Financial Service Agency, will undertake the examination whether customers and users are subject to sanctions (transaction filtering) and whether there is any suspicious transaction (transaction monitoring) based on the collected data.[106] It will then notify the FIs of the results. In this context, the same additional regulations under the Personal Information Protection Law for FIs, including obligation to establish governing mechanisms, would apply. The personal information provided by each FI to this mechanism will be managed separately and will not be shared with other FIs. The methodologies contributing to the analysis will be shared among the FIs, in a form which does not include personal information. As the scope of the information sharing widens, a detailed analysis regarding its possible impact on the interests safeguarded by DPP legislation may be necessary, as this paper discussed in the previous sections.

Although reconciling these two areas is difficult, other data governance contexts encounter similar situations. Governments must commit themselves to their democratic values when it is the basis of the country. Otherwise, the digitalization of financial information and sharing of such information would degrade such values. To this end, law enforcement authorities must secure citizens' trust in government access. In this context, the OECD Declaration on Government Access to Personal Data Held by Private Entities as stated in the introduction is relevant.[107] It lists the principles of the legal basis, legitimate aims, approval, data handling, transparency, oversight, and redress. In particular, it recommends that "[m]echanisms exist for providing transparency about government access to personal data that balance the interest of individuals and the public to be informed with the need to prevent the disclosure of information that would harm national security or law enforcement activities."[108] It is therefore essential to protect their rights and interests to ensure democratic mechanisms in the spirit of the OECD Declaration in the context of the AML/CFT regulations.

---

[104] Financial Services Agency, Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism (July 19, 2021), <https://www.fsa.go.jp/common/law/amlcft/210730_en_amlcft_guidelines.pdf>.

[105] Act No. 59 of 2009, last amended Act No. 61 of 2022, Articles 2, 63-23 - 63-42 < https://elaws.e-gov.go.jp/document?lawid=421AC0000000059>.

[106] *See* the Comprehensive Guideline for Funds Transfer Transaction Analysis Service Provider, June 2023 < https://www.fsa.go.jp/common/law/guide/ftta/index.html >.

[107] OECD Declaration on Government Access to Personal Data Held by Private Entities, adopted on 14 December 2022 <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487>.

[108] *Ibid*, Principle V.