The current issue and full text archive of this journal is available on Emerald Insight at:
https://www.emerald.com/insight/1368-5201.htm

How does the General Data Protection Regulation (GDPR) affect financial intelligence exchange with third countries?

Md. Zahurul Haq
School of Law, Universiti Utara Malaysia, Sintok, Malaysia

Abstract

Purpose – This paper aims to examine the probable effect of the General Data Protection Regulation of the European Union on the transfer of financial intelligence to a third country without an adequacy decision.

Design/methodology/approach – This is an analytical study of the financial intelligence exchange mechanisms between the Bangladesh Financial Intelligence Unit (BFIU) and its foreign counterparts. The research analyses the key challenges this national agency faces in using the Egmont Group membership to import financial intelligence from jurisdictions with a superior data protection regime.

Findings – Membership in the Egmont Group of Financial Intelligence Units does not guarantee unrestricted international intelligence exchange. Existing data protection regulations in Bangladesh are inadequate. This may forbid the transfer of the financial intelligence linked to European Union (EU) data subjects to Bangladesh.

Research limitations/implications – This paper does not cover a thorough discussion on any specific alternative tools for data transfer from the EU to a third country except for "appropriate safeguards" options.

Practical implications – The results of this study will help understand the existing legal and institutional limitations that may prevent intelligence exchange between the BFIU and its EU counterparts.

Originality/value – The study helps ascertain the legislative reform necessary in Bangladesh, a third country, to facilitate the transfer of financial intelligence from the EU.

Keywords General Data Protection Regulation, Egmont Group, Money Laundering, Financial Intelligence Unit, Bangladesh

Paper type Research paper

Introduction

One of the critical challenges domestic anti-money laundering and combating the financing of terrorism and proliferation (AML/CFT) initiative is likely to face may not necessarily be coming from the criminals. It may not result from the constant evolution of methods and trends of illicit activities. Still, it may emerge as an obvious by-product of the incompatible national legislative initiatives towards a safer information society.

Modern information and communication technology made it significantly easier to generate personal data and simpler to collect and process it for numerous purposes, which sparks privacy concerns. While the evolution of privacy laws has been remarkable in some jurisdictions, many failed to keep pace with the rapid advancements in technology. Let alone responding to unforeseen technological advancements with time-neutrality in legislation, in some instances, laws do not even adequately recognise the connection between personal data, business and law enforcement.

Journal of Money Laundering Control
Vol. 27 No. 1, 2024
pp. 158-170
© Emerald Publishing Limited
1368-5201
DOI 10.1108/JMLC-09-2022-0137

One outcome of these uneven responses is the lack of coherence in the global privacy framework. National laws regulating data processing are often principally incompatible with one another. Some jurisdictions withhold even the most basic rights of data subjects triggering an unguided evolution in data processing. In the ever-growing interactions among people, businesses and governments worldwide, this domestic practice may remain less problematic only until an agency decides to benefit from an international intelligence exchange relationship. For instance, expanding membership in the Egmont Group of Financial Intelligence Units (after this, the Group) has left nations with minimum choices regarding applying local privacy standards.

The Group – a platform to facilitate the international exchange of financial intelligence between national Financial Intelligence Units (FIUs) to investigate and prevent money laundering – "recognises that financial intelligence sharing [. . .] has become the cornerstone of international efforts to counter money laundering" (Group, 2022). The Group's intelligence sharing network allows member FIUs to exchange information upon request based on reciprocity. The requirement is that a recipient adheres to the Group's data protection and confidentiality principles and protects received intelligence, at a minimum, with the same confidentiality provisions that apply to similar information from domestic sources (Group, 2013, Clause 33). However, this collaboration could face difficulties if the FIU receiving the transfer request belongs to a jurisdiction that prohibits the transfer of personal data to a country that has lower privacy standards compared to its own.

For example, any request from the Bangladesh Financial Intelligence Unit (BFIU) to import personal data from a member of the Group from the European Union (EU) may face this challenge. The General Data Protection Regulation (GDPR), an important component of the privacy law of the EU, generally prohibits the transfer of the personal data of EU data subjects to a third country. Such a transfer is permitted when the third country concerned has obtained an adequacy decision from the European Commission (EC), or the requesting entity agreed to impose "appropriate safeguards", for instance, adopting the EU Standard Contractual Clauses (SCCs), or the data subject has explicitly consented to the proposed transfer (Regulation 2016/679, Article 45–49). As of September 2022, Bangladesh has not taken any of these steps yet, although over half of Bangladesh's total annual exports go to the EU, and both parties have signed multiple agreements on trade, economic development, human rights and good governance (European Union, 2021). However, the matter is not going unnoticed, and the consequences are piling up.

In July 2022, the Minister of Foreign Affairs of Bangladesh told reporters at an event in Dhaka that "foreigners (foreign agencies) do not share (with us) intelligence on money laundering because of the (potential violation of) their privacy laws" (The Daily Prothom Alo, 2022a, July 27). Later, the BFIU also confirmed in a report that 66 out of 67 requests for intelligence sharing from the FIU of Switzerland remained unsuccessful (Star Digital Report, 2022b, August 14). Earlier, in May 2022 EU raised concerns regarding the framework of the Digital Security Act (DSA), 2018 (Bangladesh) during the EU and Bangladesh 10th Joint Commission meeting in Brussels (European Union, 2022). One major criticism of this law is that it gives law enforcement agencies the power to search any premise, seize any equipment and arrest any person without a warrant, requiring only suspicion that a crime has been committed (Riaz, 2021). In this meeting, the EU recalled that Bangladesh's current status as the largest beneficiary of the EU's Everything but Arms unilateral preferential trade arrangement was conditional on respect for human rights (European Union, 2022).

Bangladesh is yet to face severe consequences for its virtually non-existent data protection regime. However, the ultimate cost to the international cooperation of BFIU is predictable following a recent decision of the Court of Justice of the European Union (CJEU).

In Schrems (II), the CJEU ruled that US surveillance laws did not afford EU data subjects adequate levels of protection under the GDPR and invalidated the existing legal framework for transatlantic exchanges of personal data (Case C-311/18, 2020). Connecting this development to the recent statement of the Minister of Foreign Affairs, one can argue that the BFIU is running a similar risk of disruption in international intelligence sharing if the current state of data protection remains unchanged.

Openness versus caginess

Developed to facilitate international intelligence sharing on financial crime, some of the Group's principles are comparable with similar principles of GDPR. The Group's principles for Intelligence exchange between FIUs dedicate six specific Articles to data protection and confidentiality (Group, 2013, Article 28–33), which overlap in scopes, yet broadly cover four out of seven GDPR principles, namely, (i) security, (ii) lawfulness, fairness and transparency, (iii) integrity and confidentiality and (iv) purpose limitation (Regulation 2016/679, Article 5–11).

Nevertheless, there are contrastable ones that may require further inquiry.

The two regimes are different in nature and their objectives. One is a non-political international entity founded on principles to be voluntarily accepted by national agencies; the other is a binding regulation adopted by a political and economic union of European countries. They serve two different purposes, but it is the area of international information sharing where they meet and do not necessarily greet. Especially the Schrems (II) case's outcome has further fuelled the ongoing discussion on the applicability of data protection rules to FIUs (Quintel, 2022) and if the differing principles bring two regimes at fundamental odds or if they differ only in the specific and narrow domains.

The Group upholds the contemporary national foreign policy doctrine that opposes interference with domestic politics but supports international commitments at the same time. It urges the FIUs to ensure, within their domestic legal framework, to provide the broadest range of international cooperation to combat predicate crimes, money laundering and the financing of terrorism. Naturally, the Group emphasises the free and spontaneous exchange of information among the FIUs upon request (Group, 2013, Article 9–16). On the contrary, GDPR, as a privacy regulation, gives EU data subjects enhanced protection against collection, processing and retention of all personal data except under the strict principles it sets. It integrates accountability as one of its core principles and requires organisations to protect against potential misuse and data loss with appropriate legal, technical and institutional measures. In case of violations, GDPR may levy hefty fines (Regulation 2016/679, Article 83).

From the perspective of GDPR, international intelligence sharing could fall under two broad categories – sharing between one EU Member State with another Member of the Union or a third country with an adequacy decision; or between an EU Member State and a third country without an adequacy decision. This Article focused on the second category and chose Bangladesh as a case study. It investigates how the alleged clash between two parallel regimes may affect financial intelligence sharing between BFIU and a member of the Group from the EU, to investigate and prevent money laundering. Therefore, this Article has not covered how some of the EU regulations, including the 5th Anti-Money Laundering Directive (Directive (EU) 2018/843), Law Enforcement Directive (LED) (Directive (EU) 2016/680) and Directive on Law Enforcement Access to Financial Information (Directive (EU) 2019/1153) may or may not affect the cooperation between FIUs in the EU.

How is Bangladesh currently using its Egmont group membership?

The latest Asia/Pacific Group on Money Laundering (APG) mutual evaluation report, 2016, indicates that Bangladesh obtained membership in the Group in 2013 and had been very diligent in using the Egmont Secure Web (ESW) to seek information from foreign counterparts (APG, 2016, p. 106). The following table shows the number of international intelligence sharing requests BFIU made and received through ESW from 2016 to 2021 (Annual Report, 2020–21, p. 45):

Financial year	Request received	Requests made
2016–2017	17	388
2017–2018	28	57
2018–2019	34	62
2019–2020	18	103
2020–2021	22	191

Source: Bangladesh financial intelligence unit, annual report 2020–2021

Table 1.

The data does not show how many of the requests eventually succeeded or how helpful the information was. Except for a few occasional statements by officials to the news media, no publicly available information shed light on the quality of the information BFIU received and whether such cooperation affected BFIU's effectiveness in performing the functions of an FIU. For example, in one statement, the head of BFIU shared their experience with Switzerland and said they were 'very conservative in providing information. Not all information is available on demand. Swiss FIU preserves only the suspicious transactions reports; hence, it is impossible to get the information on all deposits made by Bangladeshi citizens through this method (ESW) alone'. (The Daily Prothom Alo, 2022b, August 18)

On another occasion, a BFIU official announced in a public seminar in Dhaka that they had "gathered information on 800 [. . .] individuals and organisations from different countries" (The Daily Observer, 2022, June 20), but no details if the information collected played any role in money laundering prosecutions. The official added that they "[had] received information on 67 Bangladeshi individuals and organisations from the Swiss National Bank" (The Daily Observer, 2022, June 20). This announcement came when illicit capital flights from Bangladesh to various Swiss banks made frequent headlines. The government came under intense criticism at home for failing to act against the alleged illicit transfers. The latest report from the Swiss National Bank shows that funds deposited in 2021 by Bangladeshi citizens with different Swiss banks saw a massive rise of 55% to 871 million Swiss francs compared to the previous year (Byron and Hasan, 2022).

The discussion turned into a heated debate following a statement by Nathalie Chuard, Ambassador of Switzerland to Bangladesh. When responding to the allegation that most of the money deposited by Bangladeshi citizens in various Swiss banks had an illicit origin, she reportedly claimed Bangladesh had never sought any specific information on those funds (Star Digital Report, 2022a, August 10). This claim met with instant criticism from the Minister of Foreign Affairs of Bangladesh, who replied that Bangladesh had repeatedly sought information on the bank account of Bangladeshi citizens from Swiss authorities, but they did not reply and labelled the ambassador's claim as "untrue" (The Daily Star, 2022, August 11). At this stage, the BFIU shifted its position. An August 2022 BFIU report submitted to the Supreme Court of Bangladesh revealed that only one of those 67 requests

was eventually successful. Earlier, the Supreme Court passed a *suo motu* order asking for clarifications on the matter following the growing debate (Star Digital Report, 2022b, August 14). The foregoing examples are in no way comprehensive in scope, but only illustrative of the general nature of the problem BFIU is facing in intelligence sharing across jurisdictional borders. Now, what are the key issues the debate highlights?

The Swiss ambassador further stated, "Switzerland is committed to maintaining international standards" in intelligence exchange, and exchange of such information is possible only "on the basis of the consent of the two parties" (Star Digital Report, 2022a, August 10). The process of obtaining mutual consent plays an essential part in helping the parties to be clear about their roles, relevant international legal framework and the consequence of a breach, among others. The ambassador's statements did not refer to any "specific set of principles on data sharing" of a "particular international standard", but they are of general relevance that may concern any aspects of cross-border data sharing requests.

Still, the applicability of a particular set of principles on data sharing can be deduced from the analysis of the context in which the ambassador made the statement and the public statement of the Bangladeshi Foreign Minister in the previous month. "Foreigners (foreign agencies) do not share (with us) intelligence on money laundering because of the (potential violation of) their privacy laws" (The Daily Prothom Alo, 2022a, July 27). This general claim supports the proposition that there is no specific authority to take appropriate technical and organizational measures to protect personal data if shared with BFIU. This also substantiates the finding of the APG's third follow-up report on Mutual Evaluation of Bangladesh, 2019, which claims, "[o]verall, there do not appear to be Data Protection and Privacy obligations on competent authorities, FIs or DNFBPs that impede the AML/CFT requirements" (APG, 2019, p. 5). Therefore, the outcome of the recent debate is a crucial addition to a concern previously raised by both BFIU and APG in 2019.

Intelligence sharing between BFIU and a group member from the EU

Although the 5th Anti-Money Laundering Directive does not regulate the intelligence sharing of the FIUs from the Union with the FIUs of third countries, it requires the EC to assess the framework for FIUs' cooperation with third countries {Article 65 (2)}. Some provisions of the Directive require members to identify high-risk third countries with strategic deficiencies in their national AML/CFT regimes that may pose significant threats to the financial system of the Union (Article 9). The obliged entities are then prohibited from disclosing financial intelligence to their branches and majority-owned subsidiaries in those jurisdictions which do not impose requirements on personal data protection equivalent to those laid down in the Directive {Directive (EU) 2018/843, Article 38}.

A 2019 survey by the Directorate-General for Justice and Consumers (EC) shows that FIUs from the EU regularly exchange information with FIUs of third countries based on the Charter of the Egmont Group. Besides, bilateral agreements and memoranda of understanding (MoU) with specific countries play a crucial role. The latter type of cooperation depends on various legal conditions set in respective national legislation, reciprocity and agreement on the security of shared information, among others. In brief, when an EU member state signs a bilateral agreement with a third country to share AML/CFT-related information, they act on their own outside the institutional framework of the EU. However, it is still an "intelligence exchange", and the relevant EU data protection rules apply. Most of the FIUs that replied to the survey reported following the principles laid down in the Law Enforcement Directive (LED) (EU 2016/680) in intelligence sharing with third countries [European Commission COM (2019) 371, 2019]. But how firmly may this practice stand any legal scrutiny?

Privacy regulations on EU financial intelligence sharing with third countries

BFIU annual report for 2020–2021 says that they collect information from both Egmont and non-Egmont member FIUs and have signed 78 MoU to strengthen international cooperation beyond the requirements of the Egmont cooperation network (Bangladesh Financial Intelligence Unit, 2020–21, pp. 43–45). However, the report is silent on the geographic location of the FIUs, the success rate of information sharing, and grounds for refusal of requests, if any. These issues are relevant because there is a general awareness of the inferior data privacy regime in Bangladesh. Some of the requests foreign FIUs have previously turned down were on the ground that sharing would violate their respective privacy laws, as mentioned earlier. Therefore, the BFIU must explicitly identify the legal and institutional shortcomings that may prevent the transfer of personal data from the EU, among others, because seven of those 78 FIUs are from EU member countries (Bangladesh Financial Intelligence Unit, 2022) and are covered by GDPR.

As the 2019 survey indicates, BFIU, an FIU from a third country, is eligible to receive AML/CFT-related data of EU data subject under the LED only, provided they fulfil the general principles for transfers of personal data to third countries under this Directive {Directive (EU) 2016/680, Article 35 (1)}. However, activities of all EU-based FIUs are governed by the 5th Anti-Money Laundering Directive, which categorically mentions that the processing of personal data under this Directive is subject to GDPR {Directive (EU) 2015/849, Article 41(1)}. Hence, FIUs concerned are obliged to apply both LED and GDPR, especially when the personal data of EU data subjects leaves EU territory. As established in Schrems I, GDPR is crucial to ensure the protection of the fundamental rights and freedoms of EU data subjects is "essentially equivalent" to that offered within the EU when personal data is shared with third countries (Case C-362/14, 2015).

LED has similar provisions as GDPR on transferring EU personal data to a third country. All transfers must be based either on an adequacy decision from the EC (Article 36), appropriate safeguards (Article 37), or derogations for specific situations (Article 38). If a third country obtains an LED adequacy decision, they are considered to provide an equivalent level of protection for personal data as any EU member does. Therefore, a transfer will not require any further safeguards. However, currently, no such decision exists (Drechsler, 2020, pp. 52–53; Drechsler, 2021, p. 182).

On the other hand, derogations under Article 38 are allowed only on specific grounds – to protect the vital interests of the data subject or another person, to safeguard the legitimate interests of the data subject, to prevent an immediate and severe threat to public security in a member state or a third country, to assist in individual cases for law enforcement purposes, and for the establishment, exercise or defence of legal claims of the data subject (Article 38). However, the guidance issued by the European Data Protection Board on GDPR explains that the derogations provided (Regulation 2016/679, Article 49) must be interpreted restrictively to allow processing activities only on an occasional and non-repetitive basis (European Data Protection Board, 2020, p. 6), that is, "no massive and structural transfers of personal data, or large-scale transfers of data, but only when strictly necessary" (Directive (EU) 2016/680, recital 72).

The other options for transferring EU personal data to a third country under LED and GDPR are appropriate safeguards. Under GDPR, appropriate safeguards may be provided by a legally binding and enforceable instrument between public authorities, binding corporate rules, standard data protection clauses, an approved code of conduct and an approved certification mechanism {Regulation 2016/679, Article 46 (2) a–f}. Here, authorisation of the EC or the Data Protection Authorities (DPA) is required for nearly all options except for international agreements {Regulation 2016/679, Articles 46–47}. Under

LED, a transfer, in this case, may occur either through legally binding bilateral agreements or a self-assessment by law enforcement authorities that there are appropriate safeguards regarding personal data protection {Directive (EU) 2016/680, Article 37}. Unlike GDPR, LED does not name specific legal instruments to ensure appropriate safeguards or require authorisation from the EC or DPA for applying any options for appropriate safeguards. Therefore, the unavailability of an adequacy decision and inapplicability of derogations in ordinary circumstances render the appropriate safeguard under Article 37 of LED the only available effective option for transferring data from the EU to a third country as part of law enforcement cooperation (Drechsler, 2020, pp. 52–54).

Legal arrangements on data exchange between BFIU and EU member states

By persuading the government to enact the Mutual Legal Assistance in Criminal Matters Act, 2012 and signing several MoU with foreign counterparts, including seven EU-based FIUs, BFIU has demonstrated its moral intent to fight against financial crime. Similarly, the government of Bangladesh has also shown its political commitment to provide mutual legal assistance to foreign countries on criminal matters by introducing the necessary legal basis for such cooperation and signing mutual legal assistance agreements with India and South Africa (The Daily Prothom Alo, 2022b, 18 August). However, these commendable efforts to strengthen BFIU's capacity as a central national agency fighting financial crime may be seriously undermined by the growing privacy concern.

BFIU's recent experience with financial intelligence sharing with Switzerland shows that membership in Egmont Group is essential yet, only a preliminary step towards accessing information held by countries with a more robust data protection regime. Currently, there is no MoU between BFIU and Swiss FIU, therefore, the Egmont charter is the most relevant basis for financial intelligence sharing between the two countries. In other words, parties are not officially aware of each other's competing demands for privacy and data access.

How reliable is the current arrangement?

The Group's membership never guarantees the unrestricted and automatic flow of information. A requested FIU may always fall back on Group's principles for Intelligence exchange and deny a request if they are dubious about the security of the information to be shared (Group, 2013, Article 28–33). This probability has been substantiated by the Swiss ambassador in Dhaka (Star Digital Report, 2022a, August 10) and the Foreign Secretary of Bangladesh alike. Both diplomats recognised the absence of an agreement between the two countries as a significant impediment to intelligence exchange (Ejaz, 2022). The interactions with Switzerland, a non-EU and non-GDPR country, indicate that BFIU may face an even stiffer challenge in accessing similar data from the EU.

From the EU perspective, "[e]veryone has the right to respect for his or her private and family life, home and communications", and protecting personal data is a fundamental right guaranteed under the Charter of Fundamental Rights of the European Union (CFR) (Charter of Fundamental Rights of the European Union, 2012, Article 7–8). In Schrems I, the Court of Justice of the European Union confirmed that transferring EU personal data to a third country is an "interference" with this right (Case C-362/14, paragraph 87). Therefore, any such interference should be limited to what is strictly necessary (Case C-362/14, paragraph 92) and must comply with Article 52 (1), which provides that "[a]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms" (Charter of Fundamental Rights of the European Union, 2012). If these principles are not respected, any transfer of EU personal data to BFIU could be

successfully challenged, as in Schrems I. What alternatives may BFIU opt for, among the options available under LED and GDPR, to avoid any such challenge?

Available options for BFIU

Although BFIU has already signed several MoU with EU member states, none of the diplomats seemed to favour this option for financial intelligence exchange between Bern and Dhaka. In the post-Schrems world, either they are sceptical about the general effectiveness of MoU for these tasks or doubtful about its adequacy for this particular case. But both agree on one issue: privacy has become the key concern for the parties about data transfer. If a traditional MoU is not a suitable answer to the privacy concerns felt by Switzerland, then it may not be the right tool to negotiate intelligence transfer from the EU.

As recognised by the Vienna Convention on the Law of Treatise, it is the intent of the parties concerned to conclude a written agreement governed by international law, not the title attached to the document that makes it legally binding. "Documents intended to have moral or political weight, but not to be legally binding, are not international agreements" (McNeill, 1994, p. 823). Therefore, the use of an MoU in this regard could be initially challenged on the ground that it "[is] not a source of independent legal rights and duties but 'consensual subsequent practice of the parties" (Shaw, 2014, p. 657) and a questionable choice when it comes to safeguarding the fundamental rights of the EU data subjects.

Would a mutual legal assistance agreement between Bangladesh and an EU member state adequately address this vital legal concern? It probably would, but the signing of any such agreement would require solid legal commitment from both sides, something currently unavailable. Especially, it is not clear exactly how Bangladesh will secure the "standard of essential equivalence" (Drechsler, 2021, p. 8) for the protection of fundamental rights of the EU data subject. For example, the 2016 Umbrella Agreement between the USA and the EU allows EU citizens to seek judicial redress before a US court in case of unauthorised disclosure of their personal information in the US, among others.

But the Constitution of Bangladesh only guarantees the protection of the home and privacy of the citizens' correspondence (Article 43), not personal data. Even the most relevant pieces of legislation dealing with information security are virtually silent on this issue. For instance, the Information and Communication Technology (ICT) Act 2006 deals only with data breaches by an authorised (e.g. an employee) persons {Section 63 (1)}. The law does not recognise any rights of the data subjects. Similarly, the DSA, 2018 declares it punishable to collect, sell, possess, supply, or use personal information of any person without lawful authority {Section 26 (1)}. Then again, the law does not define what personal data is and who may collect it lawfully, and how. In brief, the concept of national supervisory authority and basic principles of data processing do not exist.

This brings the discussion to the issue of lawful access to personal data by the law enforcement authority. Section 43 (1) of the DSA empowers a police officer to enter any premises, search any place or person, and confiscate any electronic devices and documents without a court order. The officer concerned may act on mere suspicion. This provision directly conflicts with the finding of the CJEU in Schrems I. In this case, the CJEU ruled the EU-US International Safe Harbor Privacy Principles – the data exchange framework in the absence of an adequacy decision – invalid. One of the main grounds behind this ruling was that US law allowed its intelligence authorities unfettered access to EU personal data held by US companies initially processed in the EU (Case C-362/14, para 15, 22). The Safe Harbor agreement was later replaced by EU-US Privacy Shield, which was also challenged in court. In the Data Protection Commissioner v Facebook Ireland (commonly known as Schrems II), this new vehicle for data sharing was also struck down by the CJEU because it did not

provide adequate protection to EU data subjects from government surveillance (Case C-311/18).

Besides, as the 2019 Report from the Commission to the European Parliament and the Council observed, adherence to the Group's principles for intelligence exchange between FIUs – the current vehicle of financial intelligence exchange between many EU-based FIUs with non-EU FIUs – or the inclusion of such provisions in an MoU does not serve the purpose. "[T]hese provisions regulate only the issues of confidentiality and security of the data processed or contain restrictions to their use. They, however, do not guarantee that appropriate safeguards exist in terms of the enforceability or available remedies of data subject rights" [European Commission COM (2019) 371, 2019].

Under Article 47 of CFR, the right to an effective remedy and a fair trial is guaranteed for everyone whose rights and freedoms are guaranteed by the law of the EU. Similarly, GDPR provides that "a controller [. . .] or processor may transfer personal data to a third country [. . .] only if the controller [. . .] has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available" (Article 46). The absence of clarity on the appropriate remedy for EU data subject in the event of unlawful access or use of data, among others, (Case C-362/14, para 23), was another key reason why the Safe Harbor agreement was declared invalid.

Searching for similar provisions under relevant laws in Bangladesh does not show there is any satisfactory legal remedy to deal with this problem. Under Section 63 (1) of the ICT Act 2006, a court may impose a maximum fine of up to US$2000 in addition to imprisonment for two years or both if there is a breach of confidentiality by a person who is authorised (e.g. an employer) to have access to confidential data. It is not clear how the law may or may not apply against an unauthorised intruder. Under DSA 2018, any information shared for the purpose of the investigation is allowed but needs to be kept confidential {Section 47 (1–2)}. If *anyone* (emphasis added) fails to maintain such confidentiality shall be fined up to US $1,000 or imprisoned for not more than two years or both {Section 47 (2)}. DSA has a broader remedial provision as it authorises action against *anyone* (emphasis added) responsible for the alleged breach. However, in the absence of any principles of data protection, it might be near impossible to identify any legal issues associated with the illegal creation, collection, storage, processing and sharing of information to establish a breach of confidentiality.

Although regular access to foreign sources of information is inevitably based on reciprocity, a mere promise to reciprocate is inadequate. Any such international arrangements may require an adequate level of protection of data subjects' rights. Therefore, even if BFIU succeeds in signing an MoU with a GDPR state under the current circumstances, it shall always remain highly vulnerable to legal challenges within the EU on the grounds already specified in Schrems I and II.

Probable way out

The EU Member States are under obligation to ensure that transfers of information to FIUs of third countries are compliant with the Union's data protection framework, and they use one of the options available under the GDPR [European Commission COM (2019) 371, 2019]. The preceding discussion shows that resorting to any of the tools under appropriate safeguard for the international transfer of financial intelligence is the most appropriate option for data importers, including FIUs, from third countries. GDPR permits the use of contractual clauses as one of the appropriate data protection safeguards in this regard. This includes SCCs approved by the Commission on 4 June 2021 (European Commission, 2021) for data transfers from controllers or processors in the EU (the data exporter) to controllers

or processors established outside the EU (the data importer). Therefore, a binding international agreement backed by the Government of Bangladesh, incorporating the SCCs, between the BFIU and partner authorities from the EU could be a safer option compared to an agency-to-agency MoU. This is because the level of legislative reform will be needed to ensure "appropriate safeguards" of EU personal data, and "enforceable rights and effective legal remedies for EU data subjects" could only be guaranteed by a government.

Conclusion

The purpose of this study was to understand the data privacy issues an information-intensive state authority like an FIU must pay attention to when dealing with countries with stronger data protection regimes. FIUs are key players in a jurisdiction's AML/CFT reporting framework. For the receipt, analysis, and transmission of reports of suspicions, they need timely and unrestricted access to financial data. The analysis adds value to information, and this function can be efficient only when FIU has adequate access to relevant data both at home and abroad. However, an FIU may face restrictions in accessing financial data initially collected and processed by a foreign authority on privacy grounds. This may seriously undermine its ability to fight against money laundering.

In the context of Bangladesh, the BFIU is facing this challenge. Despite BFIU's high level of enthusiasm and commitment to engaging in international cooperation with its partners, its access to information held by some foreign partners remains limited. A series of recent events points to the weaker privacy framework in Bangladesh as the key reason why international partner agencies show reluctance in intelligence exchange with BFIU. This study examined the methods BFIU usually uses to import financial intelligence from its foreign counterparts and assessed their suitability in the context of intelligence exchange between BFIU and a partner agency in the EU.

The research's findings suggest that BFIU's current approach to international intelligence exchange is inadequate to meet the requirements of the EU data protection regime. One of the goals of EU GDPR is to protect individuals' fundamental rights, and freedoms, particularly their right to protection of their personal data. An FIU from the EU is obliged under GDPR to ensure EU financial intelligence is protected, particularly when it leaves EU territory. However, under the current regulatory and institutional framework on privacy, BFIU is unable to guarantee the appropriate safeguards, the opportunity to seek redress before an independent dispute resolution body, and effective legal remedies if EU data subjects' rights are violated in Bangladesh.

A recent debate on illegal fund transfers from Bangladesh to various Swiss banks has revealed two important facts. BFIU faces stiff challenges in international intelligence exchange, and the lack of adequate privacy protection is the key reason behind this problem. Experience with Switzerland – a non-EU and non-GDPR country that recognises the EU SCCs to legitimise transfers of personal data from Switzerland to countries without an adequate level of data protection – indicates that BFIU will face an even tougher challenge in data import from an EU jurisdiction.

Under these circumstances, this Article raises important questions about the suitability of agency-to-agency MoU which are not backed by any meaningful regulatory and institutional framework on privacy to satisfy the conditions of importing EU personal data in Bangladesh. The Article argues that this deficiency in data protection is part of a more general lack of privacy protection in Bangladesh. Therefore, the growing number of MoU with foreign partners may not yield the expected results under the constant risks of facing privacy-related legal challenges. A political commitment from the highest level of the government is necessary to convince BFIU's European counterparts to conclude legally binding agreements. However, it would be interesting to pursue studies on the possibility of

seeking an adequacy decision for BFIU only, because it is a more durable solution compared to appropriate safeguards. "A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or *one or more specified sectors* [emphasis added] within that third country [. . .] ensures an adequate level of protection" {Regulation 2016/679, art. 45 (1)}.

References

APG (2016), "Anti-money laundering and counter-terrorist financing measures Bangladesh mutual evaluation report", available at: www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/APG-MER-Bangladesh-2016.pdf (accessed 24 August 2022).

APG (2019), "3rd Follow-up report, mutual evaluation of Bangladesh", available at: www.fatf-gafi.org/media/fatf/content/images/APG-Follow-Up-Report-Bangladesh-2019.pdf (accessed 19 September 2022).

Bangladesh Financial Intelligence Unit (2022), "International", available at: www.bfiu.org.bd/index.php/mou/international (accessed 21 September 2022).

Byron, R. and Hasan, M. (2022), "Bangladeshi individuals, banks: Deposits with Swiss banks rise 55pc", The Daily Star, 17 June, available at: www.thedailystar.net/business/economy/banks/news/bangladeshi-individuals-banks-deposits-swiss-banks-rise-55pc-3049316 (accessed 19 September 2022).

Charter of Fundamental Rights of the European Union (2012), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT (accessed 29 November 2022).

Drechsler, L. (2020), "The Achilles heel of EU data protection in a law enforcement context: International transfers under appropriate safeguards in the law enforcement directive", *Cybercrime: New Threats, New Responses (Proceedings of the XVth International Conference on Internet, Law and Politics, Universitat Oberta de Catalunya, Barcelona, 1-2 July, e-book, Huygens Editorial*, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3664125 (accessed 19 September 2022).

Drechsler, L. (2021), "Wanted: LED adequacy decisions. How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context", *International Data Privacy Law*, Vol. 11 No. 2, pp. 182-195, doi: 10.1093/idpl/ipaa019.

Ejaz, R. (2022), "Dhaka-Berne talks to exchange information on money deposited with Swiss banks", The Daily Prothom Alo, 16 August, available at: www.prothomalo.com/bangladesh/fqzu8z9jij (accessed 19 September 2022).

European Commission COM (2019), "371, Report from the commission to the European parliament and the council assessing the framework for cooperation between financial intelligence units", available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52019DC0371 (accessed 27 September 2022).

European Data Protection Board (2020), "Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies", available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_en.pdf (accessed 19 September 2022).

European Union (2021), "Relations with the EU, the European Union and Bangladesh", available at: www.eeas.europa.eu/node/400062_bs?s=164 (accessed 15 July 2022).

European Union (2022), "EU and Bangladesh hold 10th joint commission meeting", available at: www.eeas.europa.eu/eeas/eu-and-bangladesh-hold-10th-joint-commission-meeting_en (accessed 16 July 2022).

Group, E. (2013), "Egmont group of financial intelligence units principles for information exchange between financial intelligence units", available at: https://egmontgroup.org/wp-content/uploads/

2021/09/Egmont-Group-of-Financial-Intelligence-Units-Principles-for-Information-Exchange-Between-Financial-Intelligence-Units.pdf (accessed 12 July 2022).

Group, E. (2022), "About the Egmont Group", available at: https://egmontgroup.org/about/ (accessed 27 September 2022).

McNeill, J.H. (1994), "International agreements: recent US-UK practice concerning the memorandum of understanding", *American Journal of International Law*, Vol. 88 No. 4, pp. 821-826, doi: 10.2307/2204146.

Quintel, T. (2022), "Data protection rules applicable to financial intelligence units: still no clarity in sight", *ERA Forum*, Vol. 23 No. 1, pp. 53-74, doi: 10.1007/s12027-021-00697-z.

Riaz, A. (2021), "How Bangladesh's digital security act is creating a culture of fear", available at: https://carnegieendowment.org/2021/12/09/how-bangladesh-s-digital-security-act-is-creating-culture-of-fear-pub-85951 (accessed 16 July 2022).

Shaw, M.N. (2014), "International law", Cambridge University Press, citing United States-United Kingdom Arbitration concerning Heathrow Airport User Charges (USA/UK), Award on the First Question (1992) 24 RIAA 3, para 6.7, p. 657.

Star Digital Report (2022a), "Bangladesh didn't seek specific info on citizens' deposits to Swiss banks", The Daily Star, August 10, available at: www.thedailystar.net/news/bangladesh/news/bangladesh-didnt-seek-specific-info-citizens-deposits-swiss-banks-3091781 (accessed 27 September 2022).

Star Digital Report (2022b), "Statements of Swiss ambassador, Bangladesh govt, ACC contradictory: HC", The Daily Star, August 14, available at: www.thedailystar.net/news/bangladesh/news/statements-swiss-ambassador-bangladesh-govt-acc-contradictory-hc-3094726 (accessed 27 September 2022).

The Daily Observer (2022), "BFIU says Tk 8.66b dirty money seized in July-April", 20 June, available at: www.observerbd.com/news.php?id=371226 (accessed 27 September 2022).

The Daily Prothom Alo (2022a), "Foreigners don't share intelligence on money laundering: foreign minister", 27 July, available at: www.prothomalo.com/politics/0q1rka1al9 (accessed 19 September 2022).

The Daily Prothom Alo (2022b), "What are the options to access Swiss banks information?", 18 August, available at: www.prothomalo.com/business/bank/d7lspqz42v (accessed 19 September 2022).

The Daily Star (2022), "Swiss envoy's statement that Bangladesh didn't seek info on bank accounts is untrue", 11 August, available at: www.thedailystar.net/news/bangladesh/diplomacy/news/swiss-envoys-statement-bangladesh-didnt-seek-info-bank-accounts-lie-3092796 (accessed 19 September 2022).

Further reading

Bangladesh Financial Intelligence Unit (2021), "Annual report 2020-21", available at: www.bb.org.bd/pub/annual/bfiu/2020-2021.pdf (accessed 19 September 2022).

Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559 (July 16, 2020)available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62018CJ0311 (accessed 27 September 2022).

Case C-362/14 Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650 (6 October 2015) available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362 (accessed 27 September 2022).

Charter of Fundamental Rights of the European Union, 2012/C 326/391 available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (accessed 27 September 2022).

Commission (2019), "Report from the commission to the European parliament and the council – assessing the framework for cooperation between financial intelligence units", 24 July, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52019DC0371 (accessed 19 September 2022).

Constitution of the People's Republic of Bangladesh, ACT No. of 1972) available at: http://bdlaws.minlaw.gov.bd/act-367.html (accessed 27 September 2022).

Digital Security Act (DSA), 2018 (Bangladesh).

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

Information and Communication Technology (ICT) Act 2006 (Bangladesh).

Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434 (accessed 27 September 2022).

Corresponding author
Md. Zahurul Haq can be contacted at: zahurul.haq@gmail.com

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: **permissions@emeraldinsight.com**