ATLANTIS PRESS

*Advances in Economics, Business and Management Research, volume 130*

**3rd International Conference on Law and Governance (ICLAVE 2019)**

# Extraterritoriality of Data Protection: GDPR and Its Possible Enforcement in Indonesia

Indriana Pramesti[1*], Arie Afriansyah[2]

[1]*Master's Student at Faculty of Law Universitas Indonesia, Jakarta, Indonesia*
[2]*Researcher and Lecturer at Faculty of Law Universitas Indonesia, Jakarta, Indonesia*
**Corresponding Author. Email: pramesti.indriana@gmail.com*

**ABSTRACT**

The expansion of communication technology entails the free flows of data beyond and across borders. Jurisdiction based on territoriality is seen by an increasing number of countries to be longer sufficient when it comes to data transfer governance, and data privacy in particular. The European Union's General Data Protection Regulation or GDPR is by far the most innovative and comprehensive set of data rules, which, aside from imposing high standards of data protection, introduces extraterritorial application to controller and processor outside the EU. Questions are raised regarding the legality of EU legislator decision to regulate non-EU actors and activities. But the biggest question remains: how such regulation can be enforced in third countries. This paper examines the enforcement of extraterritorial application of GDPR, in particular the provision of Art. 3 (1) and Art. 3 (2), by reviewing from the perspective of international law as well as domestic law. Alternative strategies deployed by EU regulators to promote compliance with the GDPR will also be discussed. Prescriptive jurisdiction and enforcement jurisdiction will be distinguished so as to give clarity on the extent of power a state has in terms of application of laws. States are permitted under International law to prescribe, in its own jurisdiction, legislation that regulate matters outside of its own territory. However, they are limited by the international law to enforce such regulation in the territory of other country without said country's consent. As Indonesia is not a party to any treaty governing enforcement of judgement and actions of foreign authority nor it permits, based on its laws, the same, it is unlikely that court decision or sanctions from European authority can be enforced in Indonesia. However, alternative strategies deployed by the EU regulators, particularly the data adequacy requirement may drive compliance among Indonesian entity.

***Keywords:*** *data protection, GDPR, extraterritoriality, data protection law enforcement, jurisdiction*

## 1. INTRODUCTION

Central to the growth of information technology are the collection transmission, management, processing and exchange of data. Often dubbed as the new wealth (others have likened it to 'oil' of the internet), the flows of data are now a crucial element in national economic planning. Indonesia, for example, has set an ambitious plan to be the biggest digital economy in ASEAN with e-commerce growing to US$130 billion by 2020. It also aims to boost GDP growth at an additional 2% per annum by increasing access to broadband and data [1].

However, cases of misuse of personal data by Facebook, Google, British Airways, and Marriot, among others, have sparked concern regarding the security of privacy and consumer protection. One of the most interesting development in the global data protection framework is the EU GDPR. Entered into force since 25 May 2018, it is an upgrade from the previous regulation (Directive 95/46/EC) on the safeguard of personal data. It is also the first time a regional data protection regulation giving impact on a global scale. The extraterritorial effect is the result of Article 3 of the GDPR, which requires establishment in the EU linked to data processing activity taking place anywhere as well as entities established outside of the EU offering goods or services to individuals in the EU or monitor their behaviour to comply with the rules [2].

The GDPR is the most innovative and the most comprehensive framework of data protection in the world. GDPR embarks from the recognition of privacy as a part of human rights [3]. It introduces the principles of data protection in daily business activities. GDPR has transformed how business handles consumer information and a provide a greater control for individual to determine who can process their data and for what purpose. GDPR calls for a reformation of data processing flows, from the collection, processing, transfer, storage to the removal of data. The businesses are obligated, among others, to appoint a representative in the EU, maintain the record of processing activities, implement security in accordance with the standard, and report any breach of data to supervisory authority and data owner [4-7].

Following the promulgation of GDPR, multinational companies are forced to adopt GDPR standard in their operation[8]. To comply with the GDPR, It is reported that 74% of companies spent US$100,000 on average to prepare for the GDPR and the remaining 20% spent a staggering amount of US$ 1 million. From these numbers, only 6% spent less than US$50,000 [9]. It seems that the companies have foreseen the potential costs of GDPR that many of them with less financial and human resources have opted to avoid its application altogether. Forbes reported that there is an increase of US websites that prevent them from being accessed by people in the EU [10].

But despite such onerous obligations and a threat hefty sanction for non-compliance, the main question remains: is the GDPR enforceable? The current world order is built on territorial principle as the accepted limit to jurisdictional basis [11], even though more countries have expanded their jurisdiction to regulate matters that transcends geographical boundary particularly in criminal law (anti-trust, anti-corruption) and internet governance [12]. It is understood that the GDPR is embarking from the 'effects dotrine', which imposes jurisdiction based on the effect of a conduct to a state [13]. And while the trend for legislative jurisdiction to prescribe the law has shifted to more extraterritorial in nature, the enforcement of such extraterritorial reach is still based on the concept of sovereignty and non-interference. Consequently, any measures including court decision in the EU cannot be enforced in third countries, except with their agreement.

The study finds that the GDPR expressly seeks to regulate processing activities and operators that are located outside of the EU. Such extension of prescriptive jurisdiction is permitted under international law which operates on the basis of territoriality and sovereignty. But this is where the power stops, because when it comes to the enforcement, the states are bound by the international law to not interfere with the matters in the territory of other state. As established in the Lotus case, the conventional means of law enforcement in third country such as investigation, seizure of assets and imposition of fines can only be conducted by the permission and endorsement of said third country. There are two basis on which a state can enforce foreign judgment or executive actions. First is the existence of treaty agreeing mutual consent to recognize such foreign judgment or executive actions. Indonesia is not a party to any treaty governing this matter and as such is not bound to recognize or enforce any judgment or executive action for non-compliance of GDPR. Second is if the domestic law provides any ground that enable the state to recognize and enforce foreign judgment, such as the principle of comity known in the U.S. Indonesia does not recognize such principle nor does its law permitted the enforcement of foreign judgement or any other executive action in Indonesia. By now, it is clear that enforcement of GDPR by way of conventional measures such as fines and seizure to Indonesian entity remains unlikely. However, EU regulator seems to have come up with several alternative strategies, such as prohibition of transfer of data to countries without adequate protection of data (data adequacy requirement), and optimization of reputation risk and market destroying measures as a tool for enforcement. Some measures have, to some extent, compelled the compliance of Indonesian companies. One of the indicators being the adoption of corporate rules which subjected them to GDPR.

### *1.1. Related Work*

Current scholarship have discussed at length the legal basis or justification of the application of extraterritoriality in data protection regulation, both from theoretical and jurisprudential perspective [14]. Others have explored the development of extraterritorial application of EU data protection law [15]. Several also have discussed the problems enforcement jurisdiction of the GDPR to non-EU countries and alternative approach to enforcement [16]. However, these literatures are written from the American and European perspective which may have similarities and differences with the Indonesian legal system.

### *1.2. Our Contribution*

This article contributes to the present scholarship by analysing the enforcement of GDPR, especially with regards to Art. 3 (1) and 3 (2), in Indonesia.

### *1.3. Paper Structure*

This article will be written with the following structure. First, the paper will present an overview to extraterritorial provisions under the GDPR. Second, it will present the theory on prescriptive jurisdiction and its application in the case of extraterritoriality of GDPR. Third, it will analyse the enforcement jurisdiction of GDPR in Indonesia by examining both international and national law. This part will also provide commentary on the alternative approach for enforcement offered by other scholars and assess their possible implementation in Indonesia. Last, are conclusions to the analysis conducted in the previous sections.

## 2. OVERVIEW OF PROVISIONS ON EXTRATERRITORIALITY UNDER THE GDPR

The key feature of GDPR is the increase in territorial scope as stipulated under Article 3 of the GDPR. It reflects a desire to pursue a level playing field for companies, both EU and non-EU, that target the EU markets [17]. The GDPR now shall be applicable to (i) establishment of processor and controller in the EU, regardless of where the data is processed (establishment criterion) and (ii) processor and controller outside the EU that offers goods

and services to data subjects in the EU [18] or monitor their behaviour (targeting criterion) [19]. The following will discuss briefly the scope of each of the categories.

## A. Art. 3 (1) of the GDPR

For ease of reading, it is best to firstly establish when a 'controller' or a 'processor' is deemed as an 'establishment' in the EU. An establishment is referred to as 'effective and real exercise of activities through stable arrangements', whether or not it takes the form of legal personality registered in the EU. Although a 'stable arrangement' is loosely defined, the European Data Protection Board (EDPB) through Guidelines 3/2018 notes that it is impossible to conclude the existence of establishment in the EU merely for having a web that is accessible in the EU [20].

Further, such establishment shall also be considered within the 'context of activities' of an establishment in the processing of personal data. Meaning, the activities carried out by establishment in the EU must have a connection to the processing of personal data by entity outside of the EU. A revenue-raising and marketing activity can be one of the indicator of processing activity in the 'context of activities' carried out by EU establishment [21].

GDPR shall also be applicable in the instance where data controller or processor is established in the EU regardless where the processing activities actually takes place. Similar to the above, the activity of data controller or processor in the EU that is linked to processing activity abroad that trigger the application of GDPR [22].

Where a controller appoint processor outside of the EU or when processor in the EU subcontracted processing works, in whole or in part, to processor outside of the EU, would then the processor located outside of the EU subject to GDPR? Article 28 (3) requires obtaining guarantees from processor that it will implement technical and organizational measure to meet the requirements under GDPR. Such compliance with GDPR is not the result of direct application of GDPR to the processor, but instead by virtue of contract between the controller or processor in the EU with processor outside the EU. Guidelines 3/2018 clarifies that the controller then should ensure that the processor not subject to GDPR complies with GDPR requirements as stipulated in the contract [23]. Question remains as to whether or not, in the case of breach of processor's obligation that result in violation of GDPR, the controller would be liable under the GDPR for such breach since it is obligated to ensure processor's compliance in the first place [24].

Other scenario includes a non-EU controller and EU processor. In this instance, the question whether or not the non-EU controller is processing in the context of the establishment in the EU (in this case the EU processor), matters little. This is because in both situation, the processor, due to its location in the EU, will always be subject to processor obligation under the GDPR [25]. As for the controller, Guidelines 3/2018 clarifies that processor and controller shall be distinguished, meaning that the EU processor working for non-EU controller cannot be construed as an EU establishment of the controller under Art. 3 (1) [26]. Non-EU controller, if it appoints a processor in the EU, will not be subject to controller obligations under the GDPR by virtue of Art. 3 (1). That being said, it can still be subject to GDPR if falling under Art. 3 (2).

## B. Article 3 (2) of the GDPR

Art. 3 (2) focuses on the activities being carried out, namely the offering of goods or services to data subjects in the EU or the monitoring of their behaviour that takes place in the EU. The construction of data subject under Art. 3 (2) is built around their location and is not confined by their citizenship or residency [27]. Meaning, this provision also applies when the data subject is in the EU for only a short period of time, e.g. tourist [28]. Conversely, this does not apply to processing of personal data of EU citizens or residence who happens to be outside of the EU.

The element 'offering goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the Union' shall be determined by assessing whether or not such offer of goods or services is directed at a person in the EU [29]. By 'directed at a person in the EU' it meant to say that the goods or services outside of EU that is not specifically or intentionally marketed to data subjects in the EU, even though the goods and services can still be accessed by persons in the EU, shall be ruled out from its application.

The intention to offer goods or services to persons in the EU is indicated by establishment of customer relation. Guideline 3 suggest that the following factors can be used as indicator of the existence of such activity: [30]

(i) The EU or its member state(s) is expressly mentioned;
(ii) The data controller or processor pays a search engine operator to enable consumer in the EU to access its site or there are marketing and advertisement campaigns directed at an EU country audience;
(iii) The international nature of the activity at issue, e.g. tourism;
(iv) The mention of dedicated contact to be reached from an EU country;
(v) The use of a top-level domain name other than that where the processor or controller is established;
(vi) Travel instructions from EU country to the place where the service is provided;
(vii) The mention of an international clientele based in EU;

(viii) The use of language or a currency other than that used in the trader's country, especially a language or currency of one or more EU Member states;
(ix) The data controller offers delivering goods in EU country.

Other activities included in the scope of Art. 3 (2) is the monitoring of data subject's behaviour as far as their behaviour takes place within the EU [31]. The determination on when data processing would be deemed as 'monitoring' shall take into account the purpose of the controller to subject such data to behavioural analysis or technique [32].

## C. Extraterritoriality: Prescriptive Jurisdiction

### *The basis of jurisdiction*

This section should begin with visiting the concept of jurisdiction. Jurisdiction is a term loosely defined, its conception will depend on the angle from which it is observed. Broadly speaking, jurisdiction both grants power to government institution and then limits said power. The type of jurisdictions can be distinguished in two, namely prescriptive jurisdiction and enforcement jurisdiction. Prescriptive jurisdiction points to the area where a state can prescribe law or decisions to a certain activities, persons, things or situation [33]. On the other hand, borrowing from the definition provided by the American Law Institute, enforcement jurisdiction refers to the power to 'enforce or compel compliance or to punish non-compliance with its laws or regulations, whether through the courts or by use of executive, administrative, police, or other non-judicial action' [34]. This section focuses on the power of the state to regulate data protection to subjects and actions occurring outside its territory or prescriptive jurisdiction while the enforcement jurisdiction will be dealt with in the later section.

The literature regarding jurisdiction always refer to the territorial jurisdiction as the most universally accepted limit to jurisdiction. According to this principle, state's jurisdiction covers only those, either subjects, actions, relations, or situations, located or carried out in their defined geographical territory. The territorial jurisdiction used to be regarded as the most practical approach in delimiting a state's power because it was, and still is, closely linked to the concept of 'sovereignty'. Ryngaert remarks that the concept is heavily influenced by the Westphalia Treaty which seeks to divide and organize the world into 'a system of territorially delimited nation-States that have full and exclusive sovereignty over their own territory, and no sovereignty over other States' territory' [35]. This implies a state's full authority to govern any matters in its territory and that such authority should be respected by other states. Any assertion one makes upon matters outside of their territory would be deemed as offensive because it has the potential of violating the principles of non-intervention and equality of all state [36]. As the world progress, however, the insistence on the concept of territoriality has the negative turn of hindering the development of laws over matters that are increasingly non-territorial in nature. Several countries now turn to the extraterritorial jurisdiction, especially in the sphere of criminal law and cyberspace law. The U.S., for example, has long applied legislation with regards to criminal conduct beyond its territorial border through Foreign Corrupt Practices Act 1977 and anti-money laundering provisions under 18 United States Code, sections 1956 and 1957. In terms of cyberspace, Singapore has passed Personal Data Protection Act 2012 which prohibits the collection and use of data of an individual by an organization without said individual's consent, where the term 'organization' broadly encompasses both individual and other entity, whether or not formed or recognised under the law of Singapore or having an office or a place of business, in Singapore [37]. And then of course there is GDPR, which scope of applicability has been outlined at length at previous section. This move is followed by an increasing number of countries including Brazil [38] and India [39].

So what calls for such expansion of jurisdiction? Dan J.B. Svantesson, referring to a Canadian paper, wrote there are four reasons for applying extraterritoriality in criminal law which might be useful to analyse motives in other context of law, namely: "(1) to regulate extraterritorial conduct with strong connection to the state; (2) to control the 'public face' of [the state claiming jurisdiction]; (3) to avoid lawless territory; and (4) to implement international agreements regarding particular offenses [or other matters]." [40] Svantesson added other motives for acting extraterritorially may embark from the belief that such action may contribute in the making of world order or is desired by the people of the first or that other state [41].

### *The legality of prescriptive jurisdiction applying law extraterritorially*

To address the legality or justification of the application of law extraterritorially, it would be worthwhile to visit the teachings from the U.S scholars and judges considering their contribution to the theories of jurisdictions, which mostly were delivered in relation to the enforcement of the Sherman Act. The Sherman Act, passed in 1890, was the first federal act prohibiting trusts. According William S. Dodge, the statute was silent with regards to its extraterritorial scope, but interestingly, three different approaches had been applied to cases involving the statute: the 'territorial' approach, the 'effects' approach, and the 'balancing' approach [42].

The territorial approach was adopted by Justice Holmes in American Banana Co. v. United Fruit Co. ("Banana") and

later in 1991 was invoked in E.E.O.C. v. Arabian American Oil Co. [43] In Banana, the court was questioned on the applicability of the Sherman Act on actions that were done outside of the territory of the U.S. In it, Justice Holmes argued that 'the general and almost universal rule is that the character of an act as lawful or unlawful must be determined wholly by the law of the country where the act is done' [44]. It must be noted that despite such stance, Justice Holmes acknowledged the power of the legislator to extend the scope of the Sherman Act but even so, where the act itself is silent and there is a doubt on such extraterritorial application, the operation and effect of an act must be construed to be limited based on the territorial limit customarily observed by the lawmakers [45].

Judge Learned Hand took a different position in United State v. Alumunium Co. of America ("Alcoa"). In it, Judge Hand refused the application of Sherman Act over alleged cartel practice concerning the trade of aluminum ingots. The Alcoa was the largest trader of aluminium ingots and when several big players formed a cartel in Switzerland to buy a portion of Alcoa's assets outside of the United States, the Justice Department tried to interfere with the plan. Judge Hand found that there were no link to the U.S. but then added to his consideration the possible effect of the cartel to the U.S as the ground for enforcing the Sherman Act to the cartel. Judge Hand ultimately rejected the claim. However, his approach was vastly different to that of Justice Holmes'. He introduces the element of 'effects' as the basis for applying the act extraterritorially which considers the enforcement of an act based on whether a conduct has any consequences to the States [46]. Judge Hand's effect approach drawn many criticism for its disregard of other nations' interest, [47] which then prompted the development of the balancing approach. It was Kingman Brewster who first suggested the application of 'jurisdictional rule of reason', that is a number of variables which must be assessed in determining the extraterritorial application of the Sherman Act. The suggestion was finally adopted in *Timberlane Lumber Co. v. Bank of America ("Timberlane")* and the Restatement (Third) of Foreign Relations Law [48]. Under section 403 of the Restatement (Third), prescriptive jurisdiction to legislate statute with extraterritorial extent may be exercised but it shall consider the comparative interest balancing, that is, "the importance of regulation to the regulating state" compared to "the extent to which another state may have an interest in regulating the activity" [49]. This assessment must take into account the list of factors rendering the exercise of prescriptive jurisdiction unreasonable under Section 403 (2).

The above describes U.S. Court's evolving attitude towards question on prescriptive jurisdiction of extraterritorial scope. At the end, the prescriptive jurisdiction is still confined within reasons such as the 'effect' of an action to the state while also respecting other nation's interest on the case at hand. However, it can be seen that it is no longer strictly adhering to the territorial principle and opens up possibility of extraterritorial regulation where the basis of such application exists. And it appears that the EU legislator has adopted more or less the same stance as Judge Hand by applying the targeting criteria set out under Art. 3 (2) GDPR.

But what about the legality of such assertion of jurisdiction under international law? At the level of international law, the jurisdiction of a state to exert power outside of its territorial jurisdiction was addressed in The Lotus Case: France vs Turkey, 1927 ("Lotus"). The case concerned the collision on the high seas between a French vessel, S.S. Lotus, and a Turkish vessel, which killed eight Turkish National. In Lotus, the Permanent Court of International Justice was questioned whether Turkey was violating the international law when it tried the officer of the Lotus, a French national, over manslaughter occurring in high seas and punish him under its national law [50].

The Court confirmed that a state's jurisdiction 'cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention' [51]. However, upon further reading, the Courts laid down another principle: that a state, within its territory, is not prohibited under international law to exercise jurisdiction which relates to persons, property and acts outside of their territory [52]. This leaves the states with a great discretion to determine the scope of their prescriptive and adjudicative jurisdiction because it hinges on its own sovereignty [53].

Now, it is clear that the European Union legislator has a legal basis under international law to extend the application of the GDPR to data processing and data processor and data controller outside of the EU. This broad prescriptive jurisdiction, however, is not equipped with the extraterritorial enforcement jurisdiction. Referring to other principle set out under Lotus, a state do not have any power or jurisdiction outside of its own territory. Meaning, forms of enforcement measures, such as fine, investigation, and seizure, in relation to the non-compliance with the GDPR cannot be carried out in a third country without the latter's consent [54]. This problem and its relevance to GDPR's enforcement in Indonesia will be addressed in greater depth in the next section.

## D. Extraterritoriality: Enforcement Jurisdiction in Indonesia

The general international law on enforcement jurisdiction enshrined in the Lotus case that a state "may not exercise its power in any form in the territory of another State" is uncontested, even when it is also acknowledged that a state has the power the prescribe law extraterritorially [55]. This has been the main concerns when the EU legislator

drafted the framework for data protection. Following the Lotus case, law enforcement through judicial or administrative power in third country such as investigation, seizure of assets and imposition of fines can only be conducted by the permission and endorsement of said third country. Christopher Kuner went as far as saying that all enforcement of measure, even for demand of information, an investigation, a seizure or a fine would be in contravention with international law, [56] even though in practice there have been fines levied against non-EU processor for non-compliance with the GDPR.

The first part discusses the legal basis for Indonesia to enforce foreign judgement and measures, namely through international convention and the principle of comity. This part will show that conventional law enforcement in Indonesia would be difficult for the lack of basis and precedence allowing Indonesian court or other authorities to implement foreign judgement and orders.

Other scholars have pointed out that the EU lawmakers are well aware of this limitation and therefore seems to have devise a number of workarounds. As noted by Benjamin Greze: *"It may not be necessary to enforce privacy regulation against every company that fails to comply. Selective enforcement may be sufficient to send a message to all delinquent companies that they should get their houses in order."* [57]

Such alternative approach to law enforcement will be discussed in the later part.

## 1. The Conventional Approach

The conventional approach in this context refers to the enforcement of judicial or executive power of foreign countries that may only take place through the support and assistance of adjudicative or executive branch of the state where the target or action is located.

### *Treaty*

Currently, the international regime addressing the enforcement of foreign judgment is contained in the Hague Convention on the Recognition and Enforcement of Foreign Judgements in Civil and Commercial Matters 1971 (the Hague Convention). Only a handful of countries are members, namely Albania, Cyprus, Kuwait, Portugal and Netherlands. Meanwhile, the newly adopted 2019 Convention on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters has yet to enter into force [58]. In 2005, there were also Hague Choice of Court Convention which entered into force in 2015. Those convention hasn’t been widely accepted by the majority of countries, including Indonesia.

In terms of treaty of specific commitments, the Data Protection Convention 108 [59] developed by the Council of Europe, is the only convention regulating data protection in international level. Even though opens for signing and ratification to non-Europeans, the majority of the members is of the members of Council of Europe (47 countries). Uruguay becomes the first non-EU country to join, followed by Mauritius, Senegal and Tunisia [60].

As of now, the EU and Indonesia also have yet to form any bilateral arrangement setting forth mutual enforcement of any domestic laws and regulation or data protection regulation in particular. In the absence of treaty commitment, Indonesia is not bound by international law to recognize and enforce judgement delivered by EU in relation to the non-compliance with the GDPR.

### *Domestic Law*

It is entirely within a state's sovereignty to determine whether or not it will enforce a decision or order issued by foreign judicial or executive bodies. Now, some jurisdiction, such the U.S., recognize foreign acts by virtue of the principle of 'comity'. The comity principle was first developed Dutch jurist Ulrich Huber which later heavily influenced scholars in both common law and civil law system [61].

The principle of comity originates from the idea how rights acquired in foreign countries can be maintained in the territory of other states for commercial purposes [62]. Hubert was evading the inconvenience caused non-recognition of transaction lawfully concluded under foreign law in other countries by suggesting that 'Sovereigns will so act by way of comity that rights acquired within the limits of a government retain their force everywhere' [63] .Conversely, the sovereign is also permitted to deny the effect of foreign law if it is deemed necessary to protect its interest. This principle governs the international relations of a state, but it is entirely within the realm of domestic law and is not derived from international law. According to William S. Dodge's, principle of comity lays down the basis for a state to determine 'for itself how much recognition or restraint to give in deference to foreign government actors.' [66] Further he asserts that the principle of comity should not only be confined as 'recognition' but 'deference' extended to foreign government actors, including in the instances where such foreign actor delivered judgements or when it is present as party in disputes processed before its courts [76].

The principle of comity, however, is absent from Indonesian legal system. And so far we have yet to see any precedence where Indonesian court recognize and enforce foreign judgement. Indonesian legal practitioner, M. Yahya Harahap, refers to Art. 436 Reglement op de Burgerlijke rechtvordering (Rv) as the legal basis for the enforcement of foreign judgement in Indonesia. According to the provision, a foreign judgement cannot be recognized and enforced in Indonesia unless the law prescribe otherwise [66]. Until now, the only exception to the rule is the foreign decision relating to calculation and distribution

of losses arising from ships under Art. 724 of Indonesia Commercial Code (Kitab Undang-Undang Hukum Dagang). Other than that, foreign judgement shall remain unenforceable in Indonesia.

## 2. Other (Alternative) Strategies Implemented by the EU

Now, it has been clearly established that the enforcement jurisdiction to Indonesian entities by way conventional approach is unlikely. However, recent cases indicates compliance with Data Protection Authority's ("DPA") order by non-EU companies despite the lack of enforcement jurisdiction. One of the example of compliance to DPA order can be seen in AggregateIQ Data Services Ltd (AIQ) v. UK's Information Commissioner's Office (ICO). AIQ is one of the company embroiled in the Facebook scandal relating to political campaign in Brexit [67]. ICO's enforcement notice ordered AIQ to cease with the processing of personal data of UK and EU citizens for political campaign within 30 days of the notice date and threat AIQ with a fine of up to 20 million euros or 4% of annual worldwide revenue should it fail to comply with the notice. What's interesting is that even though at first AIQ appeal the enforcement notice, at the end it decided to comply with it.

From the case it seems that the enforceability of sanctions by court or DPA is not the only factor that determine the success of the enforcement of GDPR to non-EU entities. As stated by Christopher Kuner 'it is the risk of enforceable sanctions has by far the greatest effect in influencing the behaviour of data controllers' [68]. Other scholars have suggested that factors like reputation risk may have a great contribution to the self-compliance of the data controller and processors outside of EU. Factors that may help the case of GDPR compliance will be discussed below.

### *Data adequacy requirement*

Other attempt to promote compliance comes in the form of data adequacy decision. Art. 45 of the GDPR provides that the transfer of personal data to a third country or an international organisation may take place only if the European Commission ("EC") decided that the third country has an adequate level of protection. This data adequacy requirement is additional measure to Art. 3 (2) of GDPR. Although both provisions relates to the processing of data by non-EU entities, they target different actors. Art. 3(2) of the GDPR directly addresses the non-EU legal entity who process personal data or monitor the behaviour of data subjects, and requires them to answer to DPA. Under Art. 45, it is not the non-EU operator that are regulated, rather it places restrictions on the side of EU operator and prohibits them to transfer personal data to parties in third countries which have yet to meet the standards outlined therein. Its enforcement is targeted not on foreign parties, but towards domestic actors that is fully within their territorial sovereignty.

At the time that the General Data Protection Regulation became applicable, only Andorra, Argentina, Canada (only commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, Japan and USA are decided to be adequate [69]. So far, Indonesia has yet to be declared as data protection adequate by the EC. And it would likely be a long journey until it meets the standard. Currently, the general legal framework for personal data protection in Indonesia is contained in Law No. 11 of 2008 on Electronic Information and Transaction, Minister of Communication and Informatics Regulation No. 20 of 2016 on the Protection of Personal Data in Electronic System (MOCI Regulation 20) [70]. The government also has issued Government Regulation No. 71 of 2019 regarding Administration Of Electronic Systems And Transactions.

If there is no adequacy decision for a country, the protection of data must be assured through "binding corporate rules". Binding corporate rules is internal rules for data transfers within multinational companies. They allow multinational companies to transfer personal data internationally within the same corporate group to countries that do not provide adequate level of protection.

The European countries are among the top investors in Indonesia, with 2,789 ongoing projects in 2017, worth up to USD 3,167 million, dispersed over a variety of sectors, including electricity, gas and water to hotel and restaurant [71]. Complying with the data adequacy requirements, a number of Indonesian companies with European affiliations including KPMG, PT Shell Indonesia, PT Total Oil Indonesia, and PT Continental Tyres Indonesia have posted notice of adoption of binding corporate rules in their website.

### *Risks associated with non-compliance*

Reputation risk is the top risk associated with non-compliance for its elusive nature: the damage is difficult to quantify and it may adversely impact the business in a number of ways, such as stock price decline and loss of consumers' trust, not to mention the cost of dealing with reputation damage [72]. Moreover, in data protection area, this type of 'punishment' is likely deployed to the fullest extent as an enforcement tool for non-compliance. Data protection regulators usually disseminate study findings, press release or press conference to authority's actions to non-compliance [73]. Recently, the UK ICO has made public the non-compliance of British Airways, even when the it has yet to determine the figure of the fine to be imposed to the airlines [74]. The announcement of UK ICO of its intention to issue the fine under the GDPR were widely reported throughout mass media both in and outside of EU.

The significance of reputational risk management would be subject to the corporate values and the market size of the company. In countries where customers trust is at the core of business principles such as Japan, the reputation management would be seen as priority and accordingly, the company is likely willing to spend more time and money to maintain compliance with GDPR [75]. The demands of the market also plays a role in motivating compliance. In April 2018, after the massive scandal involving Cambridge Analytica, Mark Zuckerberg announce that the standard set by GDPR will be applied to all of Facebook users worldwide [76]. This came after public outcry of distrusts towards Facebook and petition to apply GDPR, not only from the EU but also from other parts of the world. As illustrated in Transatlantic Consumer Dialogue open letter to Facebook: "We write to you on behalf of leading consumer and privacy organizations (…) to urge you to adopt the [GDPR] as a baseline standard for all Facebook services. There is simply no reason for your company to provide less than the best legal standards currently available to protect the privacy of Facebook users." [77]

Aside from the reputation risk, the operator should also be aware of the risk of market destroying measure taken by the EU regulator. Note that the EU has the authority to block websites that violates the GDPR from being accessed in the EU.

It is difficult to quantify or say for certain how much this factor affects the compliance of Indonesian entity to the GDPR, mainly because internal risk management policies of companies are usually not publicized. Additionally, so far there has been no precedent where a European agency impose sanctions to an Indonesian entity and therefore the attitude of Indonesian companies towards GDPR sanctions cannot be known.

## 3. CONCLUSION

As a response to the increasing role of information technology and possibility of abuse of data by actors outside of the EU border, the GDPR introduces the expansion of jurisdiction to broadly regulate operator established in the EU, regardless of where the data is processed as well as operator outside the EU that offers goods and services to data subjects in the EU or monitor their behaviour. Following the territorial principle and the concept of sovereignty which is the benchmark for jurisdiction delimitation accepted amongst nation, the EU legislators has the full jurisdiction under the International law to determine to which situation, actions, or persons it deems necessary to regulate. And indeed, the attitude towards extraterritorial prescriptive jurisdiction has been steadily shifting, and more states are now more open to the idea of adopting a data protection laws that applies extraterritorially.

However, such broad prescriptive jurisdiction is not equipped with the power to enforce in the territory of other states. As established in the Lotus case, the general international law on enforcement jurisdiction that a state "may not exercise its power in any form in the territory of another State" is uncontested, even when it is also acknowledge that a state has the power the prescribe law extraterritorially. Therefore, if a state wishes to enforce judicial or executive actions towards persons, things, or matter in another state's territory, it must with the approval and endorsement of the third country. The consent of a state to enforce foreign judicial or executive actions can be made on the basis of treaty, which is obligatory for the states to comply with, and based on their own domestic regulation. Indonesia is not a party to any treaty that obligated it to recognize or enforce foreign judicial or executive order. Therefore, Indonesia is not bound under international law to recognize and enforce judgement delivered by EU in relation to the non-compliance with the GDPR. A state may enforce a foreign judgment out of deference to foreign government actors, or the principle of comity. However, Indonesian legal system does not recognize such principle. Nor does Indonesian law facilitate the enforcement and recognition of GDPR in Indonesia.

The enforcement of GDPR in non-EU countries, including Indonesia, has been greatly undermined by the limit of enforcement jurisdiction. However, there are other strategies that may compel compliance of Indonesian entities. One that seems to be clearly working as of now is the data adequacy requirement which acts as a safeguard to prevent non-compliance by entities outside of the EU. Other strategies, such as reputational risk and risk of market destroying measure may also play a part in ensuring compliance albeit the degree of its impact is currently unknown. Further assessment, presumably from an empirical or statistical angle, will be necessary to identity compliance based on this factor.

## ACKNOWLEDGMENT

This work was supported by Publikasi Internasional Terindeks Mahasiswa Magister (PITMA B) of Universitas Indonesia.

## REFERENCES

[1] Asia Cloud Computing Association, ‘Cross-Border Data Flows: A Review of the Regulatory Enablers, Blockers, and Key Sectoral Opportunities in Five Asian Economies: India, Indonesia, Japan, the Philippines, and Vietnam,’ (2018), pg. 5.

[2] Art. 3 GDPR.

[3] European Convention on Human Rights 1950.

[4] Art. 27 of GDPR.

[5] Art. 30 of GDPR.

[6] Art. 32 of GDPR.

[7] Art. 33 and 34 of GDPR.

[8] Eduardo Ustaran as quoted by David Benady, "GDPR: Europe is taking the lead in data protection," https://www.raconteur.net/hr/gdpr-europe-lead-data-protection (accessed 12 June 2019).

[9] Nicole Lindsey, "Understanding the GDPR Cost of Continuous Compliance," CPO Magazine, https://www.cpomagazine.com/data-protection/understanding-the-gdpr-cost-of-continuous-compliance/ (accessed 20 September 2019.

[10] Forbes Technology Council, "15 Unexpected Consequences of GDPR," Forbes, https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/#1ff037ae94ad (accessed 19 September 2019).

[11] Raplh Christian Michaels, "Jurisdiction, Foundations", Forthcoming in Elgar Encyclopedia of Private International Law, https://www.researchgate.net/publication/311409795 (accessed 9 October 2019), pg. 2.

[12] Dan Jerker B. Svantesson, "A Jurisprudential Justification for Extraterritoriality in (Private) International Law" Santa Clara Journal of International Law Volume 13 Issue 2 (17 September 2015), pg. 524.

[13] Adèle Azzi, "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation," JIPITEC 126 para 126 (2018), pg. 131.

[14] See Dan Jerker B. Svantesson, "A Jurisprudential..", pg. 523.

[15] Shakila Bu-Pasha, "Cross Border Issue under EU Data Protection Law with Regards to Personal Data Protection." Journal of Information and Technology Law 26 (2017), https://doi.org/10.1080/13600834.2017.1330740 (accessed on 20 June 2019).

[16] See Adèle Azzi, "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation," JIPITEC 126 para 126 (2018) and Benjamin Greze, " The Extra-Territorrial Enforcement of the GDPR: a Genuine Issue and the Quest for Alternatives," International Data Privacy Law, Vol. 9, No. 2 (2019), pg. 112.

[17] European Data Protection Board, "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for Public Consultation" adopted on 16 November 2018.

[18] As an example, an organization established in Indonesia offering a service to EU individual by requiring the consumer to filling in their personal data will be subject to GDPR. Similarly, any monitoring activities of EU citizen, such as tracking and cookies, by an entity located outside of EU will also be subject to GDPR.

[19] Art. 3 of GDPR.

[20] European Data Protection Board (EDPB), "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for Public Consultation" adopted on 16 November 2018, pg. 5.

[21] *Ibid*, pg. 7.

[22] *Ibid*.

[23] *Ibid*, pg. 10.

[24] Art. 28 (3) of GDPR lists provisions that must be stipulated in the contract, one of them being the processor should make available to the controller all information necessary to demonstrate compliance with this article and allow for audits conducted or mandated by the controller.

[25] EDPB, "Guidelines 3/2018", pg. 10.

[26] *Ibid*.

[27] *Ibid*, pg. 13.

[28] *Ibid*, pg. 13.

[29] According to Recital 23 of GDPR "in order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union".

[30] Guidelines 3/2018 refers to Pammer v Reederei Karl Schlüter GmbH & Co and Hotel Alpenhof v Heller (Joined cases C-585/08 and C-144/09). In that case, the judge comtemplated the determination of "directing an

activity" in the EU. Also see Recital 23 of GDPR, which mentions factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union in determining whether or not the controller envisages offering goods or services to data subjects in the EU.

[31] Recital 24 of the GDPR elaborates that: "in order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes."

[32] *Ibid*, pg. 18. Examples of monitoring activities include: behavioural advertisement, geo-localisation activities, in particular for marketing purposes, online tracking through the use of cookies or other tracking techniques such as fingerprinting, personalised diet and health analytics services online, CCTV, market surveys and other behavioural studies based on individual profiles, monitoring or regular reporting on an individual's health status (see Guidelines 3/2018, pg. 18).

[33] Cedric Ryngaert, "The Concept of Jurisdiction in International Law", Utrecht University, https://unijuris.sites.uu.nl/wp-content/uploads/sites/9/2014/12/The-Concept-of-Jurisdiction-in-International-Law.pdf (accessed 9 October 2019), pg. 4.

[34] The American Law Institute, Restatement of the Law Third: The Foreign Relations Law Institute, (Philadelphia: The American Law Institute, 1987), para. 401 (a).

[35] Cedric Ryngaert, "The Concept of Jurisdiction in International Law", Utrecht University, https://unijuris.sites.uu.nl/wp-content/uploads/sites/9/2014/12/The-Concept-of-Jurisdiction-in-International-Law.pdf (accessed 9 October 2019), pg. 2.

[36] *Ibid*, pg. 3

[37] Singapore, Personal Data Protection Act (Act No. 26/2012).

[38] See Renato Leite Monteiro, " The new Brazilian General Data Protection Law — a detailed analysis" IAPP, https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/ (accessed 9 October 2019).).

[39] Saikat Datta, "India Gears Up for Historic Data Protection Law" Asia Times, https://www.asiatimes.com/2019/06/article/india-gears-up-for-historic-data-protection-law/ (accessed 9 October 2019).

[40] Dan Jerker B. Svantesson, "A Jurisprudential…", pg. 524. See also Steve Coughlan et al., "Global Reach, Local Grasp: Constructing Extraterritorial Jurisdiction in the Age of Globalization," 6 Canadian Journal of Law and Technology (2007).

[41] Ibid, pg. 13.

[42] William S. Dodge, "Extraterritoriality and Conflict-of-Laws Theory: An Argument for Judicial Unilateralism," Harvard International Law Journal Vol. 39 (1998), pg. 1.

[43] *Ibid*, pg. 121.

[44] Quoted by William S. Dodge, *ibid*, pg. 122.

[45] *Ibid*.

[46] *Ibid*, pg. 125.

[47] *Ibid*, pg. 127.

[48] Restatement of the Law Third, Restatement of the Foreign Relations Law (Restatement Third) of the United States is a volume that developed by American Law Institute tells what the law in a general area is, how it is changing, and what direction the authors think this change should take. See Black's Law Dictionary 1180 (5th ed. 1979). Although restatements are not binding as law, they have been accorded such high respect by the courts. Restatement Third describe the legal aspects of international relations and domestic law of the U.S. that relates to the relation of U.S. and other countries. See Kathleen Hixson, "Extraterritorial Jurisdiction Under the Third Restatement of Foreign Relations Law of the United States," Fordham International Law Journal Vol. 12 Issue 1 Article 6 (1988), pg. 128.

[49] Restatement (Third) of Foreign Relations Law Section 403(2)(c), (g) (1987).

[50] Permanent Court of International Justice, The Case of the S.S. "Lotus" (1927), pg. 5.

[51] *Ibid*, pg. 18.

[52] *Ibid*, pg. 19. According Par. 46 of the decision: " It does not, however, follow that international law prohibits a State from exercising jurisdiction in its own territory, in respect of any case which relates to acts which have taken place abroad, and in which it cannot rely on some permissive rule of international law. Such a view would only be tenable if international law contained a general prohibition to States to extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory, and if, as an exception to this general prohibition, it allowed States to do so in certain specific cases. But this is certainly not the case under international law as it stands at present. Far from laying down a general prohibition to the effect that States may not extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory, it leaves them in this respect a wide measure of discretion, which is only limited in certain cases by prohibitive rules; as regards other cases, every State remains free to adopt the principles which it regards as best and most suitable."

[53] *Ibid*.

[54] Benjamin Greze, " The extra-territorial enforcement of the GDPR…" pg. 115.

[55] Cedric Ryngaert, "The Concept of Jurisdiction in International Law", Utrecht University, https://unijuris.sites.uu.nl/wp-content/uploads/sites/9/2014/12/The-Concept-of-Jurisdiction-in-International-Law.pdf (accessed 9 October 2019), pg. 121.

[56] Benjamin Greze, "The extra-territorial enforcement of the GDPR…," pg. 115.

[57] Benjamin Greze in " The extra-territorial enforcement of the GDPR…", pg. 112, quoting David Wright and Paul De Hert, 'Introduction to Enforcing Privacy' in David Wright and Paul De Hert (eds), Enforcing Privacy: Regulatory, Legal and Technical Approaches, (Springer, Switzerland 2016), pg. 4.

[58] The 2019 Hague Convention requires will enter into force once at least two states have ratified it. At present only Uruguay has signed the Convention. HCCH, "It's done: the 2019 HCCH Judgments Convention has been adopted!," HCCH, https://www.hcch.net/en/news-archive/details/?varevent=687 (accessed 20 September 2019).

[59] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (28 January 1981).

[60] Lydia F de la Torre, "What is "Convention 108"?" Medium, https://medium.com/golden-data/what-is-coe-108-3708915e9846 (accessed 20 September 2019).

[61] William S. Dodge, "International Comity in American Law," Columbia Law Review Vol. 115 No. 8 (December 2015), pg. 2085.

[62] *Ibid*, pg. 2085.

[63] *Ibid*, pg. 2086.

[64] *Ibid*, pg. 2077.

[65] *Ibid*, pg. 2078.

[66] Yahya Harahap, Hukum Acara Perdata, Jakarta: Sinar Grafika, 2007, pg. 220-221.

[67] Herzeg Fox & Neeman, "UK: First Enforcemenet Action Under the GDPR by the ICO" Mondaq, http://www.mondaq.com/uk/x/772214/data+protection/First+Enforcement+Action+Under+The+GDPR+By+The+ICO (accessed 20 September 2019).

[68] Benjamin Greze, " The extra-territorial enforcement of the GDPR…," pg. 112 quoting Christopher Kuner, "Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law" 5 (4) IDPL (2015), pg. 235, 245.

[69] Intersoft Consulting, "GDPR: Third Countries" Intersoft Consulting, https://gdpr-info.eu/issues/third-countries/ (accessed 10 October 2019).

[70] Data protection obligations and mechanisms imposed on the administrator of electronic system is discussed in greater detail under MOCI Regulation 20. The regulation does not make a distinction between data controller or processor, and instead seeks to regulate electronic system administrator in general. Similar to GDPR, it also outlines the principles in the protection of personal data, including, among others, treatment of personal data as privacy and utilization of personal data based on approval. Art. 2 of MOCI Regulation 20.

[71] Delegation of the European Union to Indonesia and Brunei Darussalam, "European Union Trade and Investment with Indonesia 2018," pg. 26.

[72] Jeffrey Batt, "Reputational Risk and the GDPR: What's at Stake and How to Handle It," Brink News, https://www.brinknews.com/reputational-risk-and-the-gdpr-whats-at-stake-and-how-to-handle-it/ (accessed 11 October 2019).

[73] Benjamin Greze, "The extra-territorial enforcement of the GDPR…," pg. 112.

[74] Danny Palmer, "GDPR: British Airways faces record £183m fine for customer data breach", ZDNET, https://www.zdnet.com/article/gdpr-british-airways-faces-record-183m-fine-for-customer-data-breach/ (accessed 11 October 2019).

[75] Benjamin Greze, "The extra-territorial enforcement of the GDPR…," pg. 112.

[76] Adèle Azzi, "The Challenges…", pg. 135.

[77] *Ibid.*