**UUM JOURNAL OF LEGAL STUDIES**
*http://e-journal.uum.edu.my/index.php/uumjls*

How to cite this article:
Islam, M. T., Sahula, M., & Karim, M. E. (2022). Understanding GDPR: Its legal implications and relevance to South Asian privacy regimes. *UUM Journal of Legal Studies*, *13*(1), 45-76. https://doi.org/10.32890/uumjls2021.13.1.3

# UNDERSTANDING GDPR: ITS LEGAL IMPLICATIONS AND RELEVANCE TO SOUTH ASIAN PRIVACY REGIMES

**[1]Md. Toriqul Islam,**
**[2]Mariyam Sahula & [3]Mohammad Ershadul Karim**
Faculty of Law, University of Malaya, Malaysia

*[1]Corresponding author: toriqul.um.law@gmail.com*

Received: 11/10/2020 Revised: 26/3/2020 Accepted: 25/4/2021 Published: 31/1/2022

## ABSTRACT

Emerging as a buzzword, the General Data Protection Regulation (GDPR) has had immense implications on global data protection regimes. The GDPR appears as a worldwide standard for protecting personal data based on the omnibus legal substance, extensive extraterritorial scope, and influential market of the European Union (EU). It resulted in a global wave where countries are either adopting new legislation or modifying existing data privacy laws to comply with the GDPR. Historically, the South Asian region, abode to one-fifth of the world's people, has strong trade and economic ties with Europe. As reflected in current bilateral or multilateral trade agreements, the EU tends to be one of the largest trading partners of most South Asian countries. Therefore, it is understandable that the EU's norms, laws, policies, particularly the GDPR, would have

far-reaching impacts on South Asian countries. However, the issue has not been yet evaluated in legal academic settings that require an analysis of GDPR's overview and its impacts on South Asian privacy regimes. The findings of this doctrinal legal study, together with the sharing of a brief overview of the GDPR and South Asian privacy regimes, reiterate the influence of GDPR in this region. The findings of this research also have the prospects to enlighten the stakeholders in understanding the GDPR and its implications on global as well as South Asian privacy regimes. This article concludes with several suggestions and policy alternatives that policymakers can explore in South Asia and beyond in designing their potential personal data protection policy strategies.

**Keywords:** EU-South Asia Relations, GDPR, GDPR and South Asian Privacy Regimes, Implications of GDPR.

## INTRODUCTION

In this digital age, globally, most people, particularly, the young, enjoy the advantage of limitless access to the Internet (Ayub & Yusoff, 2020). This virtual reality is a double-edged sword that makes life easier, faster, and smarter, and simultaneously, entails potential privacy threats. Due to the increasing progress in surveillance, psychological and physical technology, and their usage by diverse actors from the early 1960s, privacy has become an ever-growing phenomenon (Westin, 2003). The discovery of the Internet; the World Wide Web (WWW), and the constant progress of ICT technologies have facilitated the collection, processing, and storing of large-scale personal data (Huth, 2017). Moreover, big data; cloud computing; data mining; artificial intelligence; machine learning; IoT technologies have revolutionised modern business models by processing personal data to an unprecedented level (Teixeira et al., 2019,). All these require comprehensive data protection regulations to secure the individuals' personal data, control cross-border data transfers, and regulate the businesses' conduct.

On these backgrounds, the EU launched the GDPR (GDPR, 2016), which appears as a clarion call for a unique global data privacy gold standard (Buttarelli, 2016). Generally, it is argued that from now, the

EU residents would know how businesses use their data, and how the EU can utilize the best opportunities of the data-based economy. To explain the GDPR's utility, it is further claimed that companies require clarity to extend business operations to safely extend throughout the region, while recent data breach incidents require more precise and stricter data protection regulations. In response, the EU performed the right job (Commission, 2018a).

Under Article 3, the GDPR applies against any data controller or processor with an establishment in the EU, who processes the EU residents' personal data, regardless of the place of data processing. It applies against foreign controllers or processors, who process the EU residents' personal data by offering goods or services and monitoring their behaviour. Therefore, the long arm of the GDPR extends to cover the entire world, including South Asia, holding the view that if you target or monitor the EU residents, you are targeted by the EU law (De Hert & Czerniawski, 2016). This extraterritorial application of the GDPR gives rise to tension worldwide, as its non-compliance leads to severe fines and penalties of up to €20 million or 4 percent of annual turnover, whichever is higher (GDPR, 2016).[1] Thus, the EU GDPR appears as one of the hot-button issues in the current global politics, policies, and business (Islam and Karim, 2020).

Many giant global corporations, such as Google, Facebook, Equifax, and Uber, have undergone massive sanctions because of non-compliance with the GDPR provisions. Arguably, like all other regions outside the EU, the South Asian businesses, persons, or entities are also under the scope of the GDPR, as many of them either offer goods or services to the EU residents or monitor their behaviour. This landscape may invoke people's interests in diverse aspects of the GDPR, including its basics; implications, and roles in shaping the standard for global and regional data privacy regimes. Against this backdrop, this article provides a brief introduction to the GDPR. It then explores the implications of the GDPR on global and South Asian personal data protection regulation. Later, an overview of the South Asian data privacy regimes and an evaluation of their adequacy in light of the GDPR are shared. Finally, the paper offers suggestions for improving the South Asian privacy regimes.

[1] Article, 83.

## UNDERSTANDING GDPR

The GDPR is an EU effort to protect the personal data of individuals in the EU region. The lifecycle of the GDPR began in January 2012 through a proposal of the European Commission (EC), which was approved on 27 April 2016, and finally, came into effect on 25 May 2018, followed by a long-term deliberation (Teixeira et al., 2019). It replaced the previous EU Directive 95/46/EC with several intense changes in almost everything, ranging from technology to advertising, and medicine to banking (Hern, 2018). Thus, the roles, influences, legal, textual, and contextual highness of the GDPR touch such a landmark, and diffuses globally in a manner that one must have a minimum understanding of the acronym 'GDPR' unless living in the rock (Langheinrich, 2018).

The GDPR is a vast, comprehensive, and complex document with a total of 11 chapters, 196 recitals, 99 articles, 88 pages, and '55,000 words' (GDPR, 2016). Possibly, the researchers do not have the spaces to engage with all aspects of the GDPR in sufficient depth and detail. GDPR's main issues include, among others, the definition of important terms, such as personal data, pseudonymised data, sensitive data, processing, the data controller, and data processor, along with territorial scope provisions; privacy principles; privacy impact assessment; appointment of DPO; privacy by design and default; consent; responsibilities of the controllers and processors; breach notification; establishment of the European Data Protection Board (EDPB), and new rights for the data subjects.

To begin with, Article 4 of the GDPR provides the definitions of key terms. Under this article, personal data means any information regarding an identified or identifiable natural person and includes some other information that can relate to him/ her in any way. Generally, personal data means and includes- the name; identification number; online identifier; location data; physical, genetic, or mental health, and the social, commercial, or cultural identity of the natural persons (GDPR, 2016).[2] Further, the personal data includes numerous personnel numbers, including the passport, driving licence, income tax, telephone, credit card, customer number; appearance; address; account information, and the number plate used by natural persons.

[2] Article 4(1).

The 'pseudonymised data' is a type of data, that can no longer link to a particular data subject without other attached information (GDPR, 2016).[3] For example, a 'pseudonymised data' is a mere name without connecting it to any additional information, data, or document, such as a passport. 'Special categories' or 'sensitive personal data' are data revealing one's ethnic or racial origin; philosophical, religious or political views and beliefs; trade union membership; genetic, biometric, or health data; sexual life or identity. These require ample protection and stringent conditions when processing (GDPR, 2016).[4] Data processing refers to certain personal data activities by automated or other means but mostly denotes collecting and disseminating personal data (GDPR, 2016).[5] The persons (natural or legal), including public officials, agencies, or bodies who decide the purposes and procedures of processing of the personal data are called the controllers (GDPR, 2016);[6] while persons who initiate the processing activities in favour of the controller are called the processors (GDPR, 2016).[7]

Undeniably, the previous EU Directive 95/46/EC's territorial scope was unclear, resulting in several high-profile cases. The GDPR includes clear-cut provisions setting several tests to address the problem, such as the establishment test, offering test, monitoring test, and public international law test. The GDPR extends to any EU establishment that processes the personal data of the EU individuals irrespective of the processing place; the foreign companies, that process personal data of the EU residents offering goods or services to them and monitor their behaviour (GDPR, 2016).[8] Finally, it includes the data processing activities of any controller or processor having no establishment in the EU but in other places where the laws of the EU Member States apply through public international law (GDPR, 2016).[9]

Like its predecessor, the GDPR contains six privacy principles, the compliance of which is the central component for a sound data protection regime, and the failure leads to the highest administrative

3 Article 4(5).
4 Article 9, and recitals 51-56.
5 Article 4(2).
6 Article 4(7).
7 Article 4(8).
8 Article 3(2)(a)(b).
9 Article 3(3), and recitals 22-25.

fines (ICO, 2018a). Under Article 5 of the GDPR, personal data shall be-

a. processed in a lawful, fair, and transparent manner (lawfulness, fairness and transparency principle);
b. collected for specific, explicit, and legitimate purposes, and not proceeded further in an incompatible manner to that of the initial purposes (purpose limitation principle);
c. adequate, relevant, and limited (data minimisation principle);
d. accurate and up-to-date, and if any irregularity, data will be erased or rectified immediately (accuracy principle);
e. stored for a definite period and to the extent, it is necessary for the initial purposes (storage limitation principle), and
f. processed, maintaining proper security, technical and organisational measures to save them from any damage, destruction, or accidental loss (integrity and confidentiality principle) (GDPR, 2016).[10]

The GDPR emphasises developing privacy impact assessment for processing large-scale sensitive data at a regional, national or international level. Also, data that causes high risks to data subjects' rights and freedoms; or operating new technologies; or data concerning biometric identity, criminal convictions, offences, or security measures. (GDPR, 2016).[11] Furthermore, the GDPR requires the appointment of a Data Protection Officer (DPO) by a public authority other than courts within the judicial capacity to deal with the large-scale personal data or special categories of data. The duties of the DPO include, among others, giving notice and advice to the data controller, processor, or any representative processing personal data. His responsibilities also include monitoring compatibility of the GDPR and domestic data protection legislation; raising awareness and conducting training; giving directions concerning data protection impact assessment, and extending cooperation to the supervisory authority (GDPR, 2016).[12]

To enhance personal data protection, the GDPR introduces a new principle, namely, privacy by design and default, which ensures that by default personal data cannot be accessed by an unspecified

[10] Article 5, and recital 39.
[11] Article 5, 35, 36, 57 and recital 75, 84, 89-96.
[12] See generally, GDPR, art 35, 37, 38, 39 and recital 91, 97.

number of natural persons without any human intervention (GDPR, 2016).[13] This regulatory principle considers privacy a critical element of any institution's design, maintenance, and operation of information systems. Besides, the GDPR affirms that mere silence, inaction, or pre-ticked boxes will never become consent, especially, for obtaining children's consent, and directs all entities not to use long and unreadable, but relatively simple terms for obtaining the consent of children (GDPR, 2016).[14] Moreover, parental consent is a prerequisite for processing personal data of children under 16, and this age may be 13 if EU Member States wish so (GDPR, 2016).[15] Ireland, for example, has fixed 13 as the age of consent (Kennedy, 2016).

The Regulation makes the controller responsible for implementing proper technical and organisational steps to ensure the purpose limitation; data minimisation; storage limitation, and accessibility (GDPR, 2016).[16] The obligations of data controllers and processors extend to joint data controllers and processors. They are duty-bound to conduct a data protection impact assessment before initiating a vulnerable processing activity (GDPR, 2016).[17] They are also responsible for appointing a DPO with expert knowledge on data protection laws and practices (GDPR, 2016).[18] The data breach notification is another crucial provision of the GDPR, which obliges controllers to notify the supervisory authority within 72 hours of any breach (GDPR, 2016),[19] and processors to inform controllers without undue delay (GDPR, 2016).[20] Besides, if a data breach is likely to cause high risks to the individuals' rights and freedoms, the controller is also responsible for informing the victim without delay (GDPR, 2016).[21]

The European Data Protection Board (EDPB) is established under GDPR, replacing the Article 29 Working Party, retaining a similar composition, i.e., heads of national supervisory authorities of Member States. Currently, the European Commission members are no

13 See generally, GDPR, art 25, and recital 78.
14 See, GDPR, recital 18.
15 Article 18.
16 Article 24.
17 Article 35.
18 Article 37.
19 Article 33(1).
20 Article 33(2).
21 Article 34.

longer part of the EDPB, although they can attend its meetings. The GDPR ensures the EDPB's independence and explicitly clarifies its duties, roles, and lability (EDPB, 2019). A lead supervisory authority, established in each Member State, monitors the compliance with the GDPR of each institution's principal establishment. (Makulilo, 2017).

The GDPR provides EU citizens with new rights such as (i) right to transparent information; (ii) right to rectify; (iii) right to erasure (right to be forgotten); (iv) right to restriction of processing; (v) right to data portability; (vi) right not to be subject to automated decision making and profiling.[22] Conversely, it imposes more obligations on controllers and processors, including data-retention; security; transborder issues, and communication with supervisory bodies (DLA Piper, 2020). In particular, GDPR allows exemptions, or derogations for public interest purposes, including archival, scientific, historical, or statistical research. It will also enable personal data processing, including promoting human rights and freedoms of data subjects.

The EU's data protection initiatives have been among the legal talk of the world's leading institutions and individuals. Eventually, this transplants the GDPR into other privacy protection mechanisms in the world (Schwartz, 2019). The GDPR represents the global diffusion of policy ideas and policy instruments of privacy, thus complementing the law and forms an integral part of entire regulatory regimes (Bennett and Raab, 2018).

## IMPLICATIONS OF GDPR

Due to overarching provisions, exclusive market power, and extensive extraterritorial scope, the GDPR appears as the global data privacy standard, the implications of which are undeniable. Admittedly, the GDPR has a tremendous impact on how data is managed within and outside the EU and contributes a significant role in shaping privacy legislation worldwide. The Regulation serves as the global data privacy law model practised worldwide. Albeit the net impact of the GDPR is two-folded, such as (1) transatlantic privacy convergence, and (2) rapid evolution as a global data privacy standard (Rustad & Koenig, 2018). Numerous countries worldwide, many US States, and most US-based processors are adopting policies in conformity with

[22] See generally, GDPR, arts 12-23.

GDPR (Rustad & Koenig, 2018). The emergence of a GDPR-styled privacy standard is found not only in the 'First World' but also in the 'Second World' and the 'Third World' countries (Rustad & Koenig, 2018).

The GDPR applies, in addition to offering a complete set of new rules requiring both technological and institutional responses, to almost all institutions worldwide that process EU citizens' personal data. Hence, if South Asian businesses with websites accessible to the EU residents offer them options for signing up for their services, South Asian businesses will be subject to GDPR, irrespective of whether or not the targeted EU residents will have to pay for these services. If South Asian companies track EU individuals' behaviour using cookies or logging IP addresses from their websites, the GDPR would not apply to them, unless it is unintentional. (KPMG, 2018).

Furthermore, South Asian businesses are likely to be bound by the GDPR for various reasons, such as the contractual obligations to the EU or their responsibilities to suppliers or contractual allies. Besides, the functions of data controllers or data processors are significant. Thus, South Asian companies will fall within the ambit of the GDPR, like all other companies outside the EU, for their data processing activities or the activities of their co-data controllers or processors. Furthermore, the GDPR allows foreign controllers or processors who fall within the scope of the GDPR to appoint their EU members to represent them in the EU. Non-compliance with the GDPR outside the EU, imposes a sanction on the representative. The same is the case for controllers or processors in South Asia.

Several intrinsic aspects of the GDPR affect the entire world, including (1) extraterritorial scope; (2) adequacy decision; (3) reputational damages, and (4) global diffusion, which may require a more detailed discussion.

The GDPR applies to any foreign controller or processor, who by offering goods or services or monitoring their behaviours, process the personal data of EU citizens. Thus, GDPR affects the entire world through these extraterritorial provisions, which break the traditional sovereignty immunity principles. The argument against extraterritoriality has been placed under fire by the advent of new global issues (Walsh, 2013). In *Lotus case* (1927), the International

Court of Justice asserted that the Member States were free to adopt principles best suited their conditions.[23] Similarly, in the case of Google Spain (2014), the European Court of Justice ruled that the US-based company Google Inc. had become profitable through the EU establishment's operations, Google Spain. Hence, the commercial links between the US controller, Google Inc., and the EU establishment, *Google Spain*, will be considered data processing by the EU establishment.

Indeed, in a changed global context, trends of customary international law are more supportive than prohibiting the territorial jurisdiction of States (Ryngaert, 2015) (Paul, 1991) *Hilton v. Guyot*, (1895). Thus, the claims over extraterritorial jurisdictions are justified; otherwise, a state does not extend its data protection regime to cover the foreign actors' behaviours. Also, it would not be able to render adequate protection for its citizens (Svantesson, 2014).

The GDPR, through the adequacy decision further expands its scope beyond the EU. As per Article 45 of the GDPR, if an adequate level of protection is assured, the transfer of EU residents' personal data to any third country or international institution is allowed. As a result, several countries, mostly the EU global trading partners, enact or amend the existing data privacy laws in compliance with the GDPR (Greenleaf, 2019a).

Currently, Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay have obtained complete adequacy decisions, and Canada the USA received partial adequacy (Commission, 2019c). The EC has recently granted Japan adequacy decisions (Commission, 2019d) and is working on South Korea's adequacy decision (ICO, 2018b). None of the South Asian countries is either on the list or considered. At the same time, India made two applications to obtain the EU favourable adequacy decision before and after amending the Information Technology Act 2000 but was unsuccessful (Greenleaf, 2019b).

The reputational damages caused by data breaches and subsequent harsh sanctions of the GDPR play a vital role in transplanting the provisions of the GDPR outside the EU. In 2019, the French DPA (CNIL) inflicted sanctions of €50 million on Google (Goldsmith, 2019); while the Information Commissioner's Office (ICO, UK)

[23] *FR v. Turk*, 1927 P.C.I.J. (ser. A) 10 (Supreme Court 1927).

imposed a fine of £500,000 on Facebook (ICO, 2018c). ICO also fined £500,000 on Equifax Ltd, a US-based credit risk assessment agency (ICO, 2018d); and the Dutch DPA [*Autoriteit Persoonsgegevens* (*AP*)] and ICO jointly fined $1.17 million on Uber, for a data breach incident, that happened in 2016 (Schulze, 2019b). All these incidents are compelling the giant corporations to reconsider GDPR compliance and associated reputational damages. Therefore, top US lawmakers, lobbyists, including Mark Zuckerberg, CEO of Facebook, Tim Cook, CEO of Apple, and Sundar Pichai, CEO of Google, urged to enact GDPR-like comprehensive Regulation in the USA (Schulze, 2019a). In 2018 California Consumer Privacy Act (CCPA) is the apparent result of such initiative.

For two primary reasons, (1) divergences in the domestic laws and (2) non-enforcement practices, there are still insoluble issues in the data regulations (Reed, 2004). Global integration of data controllers, processors and data subjects is a notion that can strike a balance between the interests of the trio. The GDPR, which emerges as a combination of international policy instruments, provides a notable expansion to the global system of policy convergence and positions itself as the international data privacy standard (Bennett, 2018). Thus, GDPR has been rapidly expanding beyond the EU, mainly in the African, Asian, Caribbean, and Latin American areas. (Greenleaf & Cottier, 2018).

Lawyers working with *Ius Laboris* indicate that at least 24 non-EU countries in which GDPR-related legal developments, decisions, or harmonisation trends occur (*Ius Laboris,* 2019). In 2019, the LGPD (Lei Geral de Proteção de Dados) of Brazil, was inspired by the GDPR (Lexology, 2019). India's draft Personal Data Protection Bill, 2019 contained several provisions of the GDPR, e.g. the right to erasure (section 18), and privacy by design (section 22), while, South Korea has revised its laws in line with the GDPR (Lexology, 2019). The nations of South Asia, however, should comply with this global trend. Research on South Asian privacy frameworks is, therefore, essential.

## DATA PRIVACY REGIMES OF SOUTH ASIA

In terms of political cultures; ethnicity; language; historical development and colonial history, Asian countries are highly diverse,

and these have been reflected in their approach to adopting data privacy measures. The global results in the enforcement of data privacy laws include both public and private enterprise. The Asian approach mainly covers only the private sectors as evidenced in Malaysia, Singapore, and India (Greenleaf, 2014d,). Certainly, Asian laws on data privacy are not equivalent to European data privacy structures, as data privacy is at the heart of Europe, not in Asia. As a legal and policy measure, privacy is not on the high priority list of any government in South Asia, like most parts of Asia (Prasad & Aravindakshan, 2020).

Further, the absence of any regional standard in Asia or any of its parts compared to the EU, Latin America, or Africa suggests that there is limited scope for adopting uniform principles, so, 'convergence' in Asia is not an excellent notion (Greenleaf, 2019b). Therefore, in the context of Asia, an analysis of data privacy legislation should proceed with domestic laws paying heed to all their remarkable diversity as the baseline, while considering the international factors in the context of what Greenleaf describes as the 'bottom-up' approach, unlike the 'top-down' European approach (Greenleaf, 2014d). We will give an overview of South Asian data privacy regimes in the following section.

**Afghanistan**

Currently, there is no law in the Islamic Republic of Afghanistan that is equivalent to the GDPR. The present 2004 Constitution of Afghanistan does not recognise the right to privacy, but it does recognise certain other privacy-related rights, including 'liberty and human dignity' (Article, 24); 'confidentiality of correspondence, conversations and communications' (Article 31); 'freedom of expression (Article, 34); 'protection of personal residence from unlawful trespassing' (Article, 38), and 'right to access to information from the state departments' (Article, 50). In March 2018, Afghanistan passed the Access to Information Law under Article 50 of the Constitution, which affirms, among others the denial of access to information to protect the right to privacy (Article, 16 (7)). Therefore, Afghanistan's privacy protection mechanism is fragile compared to other South Asian nations.

**Bangladesh**

Islam has strongly influenced the development of 'privacy' in Bangladesh, as it is primarily a Muslim country (Karim, 2005). In particular, numerous ancient and historical publications have shown that the arrival of Islam in ancient Bengal in the 13th century, the Muslim community began to preserve the culture of privacy, especially the privacy of home and female members, strictly (Karim, 2020).

Article 43 of the Bangladesh Constitution recognises the right to privacy in protecting home, correspondence and communication. In Parts II and III of the Constitution, several other constitutional guarantees may also be relevant to this right. For example, Articles 31 and 32 guarantee the absolute right to life and personal liberty, similar to Article 21 of the Indian Constitution.

Numerous other Bangladeshi laws have several isolated provisions relating to privacy. Section 509 of the Penal Code, 1860 affirms the protection of women's rights to modesty, decency, and privacy. While Section 63 of the Information and Communication Technology Act, 2006 (the ICT Act, 2006), contains provisions on privacy disclosure related offences and their penalties. Section 33 of the Digital Security Act 2018 (the DSA, 2018) forbids unlawful transfer and personal data retention. There is no law equivalent to GDPR, other than such scattered privacy-related provisions in various laws.

The draft Data Protection and Privacy Rules have released in 2019 containing numerous yet inconclusive privacy and data protection provisions. These include the definition of data;[24] data controllers;[25] personal data,[26] data processing;[27] "pseudonymisation";[28] profiling;[29] sensitive personal data;[30] and the scope.[31] In addition, the Rules provide for the data subjects' right;[32] principles of data collection

24 Section 2(f).
25 Section 2(h).
26 Section 2(l).
27 Section 2(n).
28 Section 2(o).
29 Section 2(q).
30 Section 2(s).
31 Section 3.
32 Section 5.

and processing;[33] transfer, storage and security of personal data;[34] duties of the controller, processor and data protection officer;[35] and supervision.[36] As it is a draft law, all provisions may be revised at any time by the Government.

Besides, this Draft Rules of 2019 cannot establish an adequate privacy regime in Bangladesh for numerous reasons, such as (1) it is not a standalone law, it was adopted to fulfil the objective Section 60 2(i) of the DSA, 2018; (2) the instrument does not contain necessary contents of a data protection law, and (3) it does not comply with any data protection standard (1st generation- OECD Privacy Guidelines, 1980, 2nd generation- Directive 95/46/EC, or 3rd generation- the GDPR, 2018). Therefore, Bangladesh's privacy regime is still in its infancy.

**Bhutan**

The 2008 Bhutan's Constitution explicitly affirms the right to privacy in Article 7 (clause 19), and included several privacy-related provisions. Such provisions are, 'the right to life, liberty and security of person' (Article, 7, Clause 1); 'freedom of speech, opinion and expression' (Article, 7, Clause 2); 'the right to information' (Article, 7, Clause 3); 'freedom of thought, conscience and religion' (Article, 7, Clause 4), and 'freedom of the press, radio, and television' (Article 7, Clause 5). The Information, Communications and Media Act (ICM) 2017 (entered into force in 2018) executes at least seven out of ten 'second generation' principles covering the ICT and media sector in Bhutan. Bhutan has taken one step forward in developing an adequate data protection regime (Greenleaf, 2019b).[37]

The ICM Act of Bhutan covers, among others the definition of personal data (Section 464 (76)); sensitive personal data (Section 464 (89)); general obligation on broadcasters to protect the privacy

[33] Section 16-33.

[34] Section 22-28.

[35] Section 30-35.

[36] Section 38-46.

[37] The 1st generation data privacy standard was set by the OECD Privacy Guidelines 1980, the 2nd generation standard was laid down by the Directive 95/46/EC, and the 3rd generation higher standard was set by the GDPR. See generally, Greenleaf G and Cottier B, 'Data Privacy Laws and Bills: Growth in Africa, GDPR Influence' (2018) 152 Privacy Laws & Business International Report, 11-13, UNSW Law Research Paper No. 18-52, 5.

of individuals (Section 179); responsibilities of government agencies concerning e-governance (Section 271). Chapter 17 of the Act deals with online and offline privacy protection issues, under 'privacy' (Sections 336-43); 'security of payment and personal information' (Sections 344-6); 'unsolicited e-mail' (Section 347), and 'communications with children' (Sections 348-51).

The issue of 'breach of confidentiality and privacy' is protected by Section 391 of the ICM Act. At the same time, Chapter 21 covers data protection, and Chapter 22 covers a wide range of offences and prescribes penalties. While not entirely self-governed, the Bill sets up an InfoComm and Media Authority in Bhutan (Greenleaf, 2019b), encourages authorities to investigate and resolve issues and ultimately, create a minimum data privacy regime in Bhutan (Greenleaf, 2019a).

**India**

The Constitution of India 1949 does not explicitly recognise the right to privacy. The Supreme Court of India held in several cases, including *Justice K.S. Puttaswamy (retd) & Anr vs Union of India and Ors* (2017) and *People's Union for Civil Liberties & Anor vs Union of India,* (1997) that privacy is a constitutionally protected right arising from Articles 19 (1) and 21 respectively. Many other documents include several clauses on privacy, e.g. the Information Technology Act 2000 (ITA 2000), containing several provisions covering the right to privacy and data protection. Due to inadequacy, it underwent substantial amendments in 2008. IT Rules 2011, contain privacy-related provisions, including personal data (Section 2 (1) (i)) and sensitive personal data (Section 3).

There is, however, no law equivalent to GDPR. So India has introduced a GDPR-styled Bill entitled 'Personal Data Protection Bill 2019'. It contains a wide range of requirements including notification, consent and purposes; data localisation; data fiduciary obligations; exemptions and penalties (S&R, 2020). However, there are significant criticisms to the Bill, such as allowing the central Government to exclude any government agency from the Bill's scope (Mandavia, 2019). On this point, Justice B. N. Srikrishna, drafter of the Bill, believed that it could convert India into an 'Orwellian State' (Mandavia, 2019), which Forbes India describes as 'blanket powers' at the hands of the Government (Arakali, 2019). The new PDP Bill 2019, amid

shortcomings and critiques, is a welcome start to India's path to an effective regime for protecting privacy.

**Maldives**

The Republic of Maldives ratified the ICCPR and endorsed the Optional Protocol to the ICCPR on 19 September 2006, which entered into force the same year (Assembly, 1966a). Accordingly, Article 17 of the ICCPR applies to its domestic laws. The 2008 Constitution of the Republic of the Maldives recognises the right to privacy in Article 24. It contains privacy-related provisions, including the right to life, liberty and security of the person (Article 21), the right to protection and respect for others' rights and freedoms (Article 67). The right to privacy is explicitly recognised in the Constitution, but not tried in a court of law.

The Right to Information Act 2014 (RIA 2014) is the only legislation that contains clauses relating to privacy protection issues. The Ministry of Economic Development drafted a Privacy and Data Protection Bill to promote small and medium enterprises; fostering e-commerce and establish procedures for storage, management, and protection of confidential consumer data. The Parliament has not yet reviewed the Bill. There is no legal document equivalent to the GDPR in the Maldives and, thus, within South Asia, Maldives has another weak data privacy framework.

**Nepal**

The 1990 Constitution, 2007 Interim Constitution, and the current 2015 Constitution of Nepal recognised the right to privacy in Article 28, while Article 27 guarantees the right to information. In Nepal, there is hardly any legislation equivalent to the GDPR except the Privacy Act, 2018 (2075). The Privacy Act contains a variety of provisions relating to the protection of privacy, including the definition of 'personal information', (Clause 1: Section 2 (c)); protection of privacy of body and family of a person (Clause 2); his/ her residence (Clause 3); property (Clause 4); document (Clause 5); data (Clause 6); correspondence (Clause 7) character (Clause 8); electronic means and privacy (Clause 9); protection of personal data (Clause 10); offences and sanctions (Clause 11).
However, in terms of overlaps in some sections of the Criminal

Code, 2017, there are critiques of Nepal's Privacy Act. For instance, conviction of an offence involving an illegal search of a person's body or property is punishable to 1 year and NPR 10,000 or both under the Criminal Code; while if charged under the Privacy Act, the penalty and fine would be up to 3 years and NPR 30,000 respectively or both for the same offence (Neupane, 2019).

Moreover, the Privacy Act hardly provides any room for detailed interpretation of personal data. If strictly interpreted, many essential concerns such as the e-mail address, IP address, social media ID or personal website will remain beyond the Act's scope. The enactment does not distinguish between the data controller and the processor; consequently, in many problems, such as data protection, data management, and liability for the breach of the right to privacy, this may cause difficulty (Neupane, 2019).

**Pakistan**

No explicit provision for the right to privacy exists in the Constitution of the Islamic Republic of Pakistan, 1973, except for the home's privacy (Article, 14 (1)). However, it includes several other clauses in various Articles, relevant to the protection of privacy, including the protection against unlawful interference with life, liberty, body, reputation or property of any individual (Article, 4 (2) (a)); the dignity of man (Article, 14 (1)); and freedom of speech and expression (Article, 4 (19)). The Pakistani Parliament passed the Electronic Crimes Act 2016 (PECA 2016) in 2016. It contains provisions relating to privacy rights, including the protection against unauthorised access to the central information infrastructure. Still, it includes unfavourable conditions in Section 37 to provide legal cover for invasive activities that weaken the constitutional protection of the right to privacy.

Except for the draft Personal Data Protection Bill (PDPB) 2018, there is no law equivalent to GDPR. It includes various provisions, including the definition of personal data (Section 2(g)); sensitive personal data (Section 2(n)); protection of personal data (Section 4); right of access to personal data (Section 12); right to correction of personal data (Section 15); processing sensitive personal data (Section 23), and several others to ensure the protection of personal data and privacy. There are various criticisms against the Pakistani draft Bill, including

the proposed title itself, such as Section 1(1) of the Bill terms the Bill as the Personal Data Protection Act, 2017. The Act should be the year of its adoption. Compared with GDPR, the PDPB applies only to personal data processing relating to commercial transactions, limiting Bill's material scope. The definition of sensitive personal data is also restricted as biometric and genetic data are not included. The draft Bill uses the word 'individual' to describe 'data subject' that may cause an uncertainty as it is not clear if the individual refers to natural persons or juristic persons, or both (Privacy International, 2018).

**Sri Lanka**

Sri Lanka, which ratified the ICCPR on 11 June 1980 and entered into force on 11 September 1980, is a democratic socialist country (Assembly, 1966b). In 1997 the country endorsed the ICCPR Optional Protocol allowing complaints to UNHRC regarding its incompetence in upholding Article 17. Even though UNHRC received complaints against Sri Lanka, few were considered (UNHRC, 2006). Previously, the right to privacy was no recognised in the Constitution of Sri Lanka. Still, by the 19th amendment, 2015 Article 14A was incorporated into the present Constitution, containing the right as an exception to the right to access information.

The Computer Crimes Act 2007 (CCA) contains various crimes that apply to the 'data protection' and compensatory clauses that constitute civil liability for privacy violations. However, the data subject need not comply with the action until the criminal proceeding commencement. The Act applies to data protection as it includes unlawful entry issues; unapproved modifications; unlawfully obtained information; unauthorised interference, and other related crimes (Section, 3, 4, 5 and 8). There is no law equivalent to GDPR other than the Personal Data Protection Bill, which, after deliberations with the stakeholders, modified the previous Data Protection Framework (released on 12 June 2019).

However, the enactment will occur within three years of the day of its certification by the speaker (Babele, 2019). The provisions of the draft Bill, from the scope, the principles of privacy, and the duties of the data controllers, are more or less influenced by the EU GDPR. There are also significant discrepancies with GDPR, such as that this draft Bill does not include any provision on sensitive personal data.

Compared to the GDPR, Sri Lanka's draft Bill is significantly less comprehensive and imposes fewer penalties than the GDPR.

From the discussion above, it is evident that there is less progress in the South Asia region regarding data privacy laws. Greenleaf (2019b) argued that South Asia's data privacy regimes have not matured enough, but have just started with significant shortcomings. In most cases, contrary to international norms, South Asian countries do not have adequate data privacy legislation. Both Bhutan and Nepal have special laws with weaknesses in South Asia, while India, Pakistan, and Sri Lanka are seeking to pass data protection bills. Bangladesh is committed to adopting a data protection law shortly, while there is no substantial progress in Afghanistan and Maldives.

The EU's approach to data protection laws, currently promoted by the GDPR, is the right option for the South Asian region. It is compelling based on widespread economic and trade relations between the EU and South Asia.

## EU-SOUTH ASIA RELATIONS

In the last three and a half decades, South Asia has played a crucial role in developing a constant economic growth and reform process worldwide (IMF, 2019). The intra-regional businesses in South Asia are comparatively smaller due to the lack of cooperation and integration, despite ample opportunities, potential, resources and workforce (WB, 2016). South Asia can move forward by raising revenues; diminishing financial deficits; increasing trade, and liberalising private and foreign direct investment (IMF, 2019).

Based on results of some recent surveys, the World Economic Forum (WEF) finds some areas where South Asia can focus. Initiatives such as increasing cooperation, greater connectivity, adoption of ICT, and innovation skills (WEF, 2018a) have been proposed to develop economic resilience in the region (WEF, 2019b). Therefore, the secret to the South Asia region's success lies in promoting economic cooperation and an integration process that can materialise by establishing a secure and safe ICT infrastructure and comprehensive GDPR compliant data protection regimes.

Based on EU market power, the GDPR affects most South Asian nations since it appears among the largest trading partners for almost all countries in the region (Wu and Goldsmith, 2006). For example, the EU is Bangladesh's leading trading partner, sharing a total of 24 percent of the country's total foreign trade (European Commission, 2015). Bangladesh is the 35th largest trading partner in goods, according to the same report. In terms of revenue, more than half of Bangladesh's total exports go to the EU (European Union, 2016a). After China, the EU is Pakistan's second-largest trading partner and overall trade between the EU and Pakistan were nearly EUR 12.6 billion in 2018. The EU received a total of 35 percent of Pakistan's exports (Fact Sheets, 2019). Similarly, the EU is Sri Lanka's second-highest trading partner after India, with bilateral trade in goods reaching EUR 4.5 billion in 2018. The EU grants Sri Lanka with EUR 1.3 billion surplus trade (Fact Sheets, 2019).

Once again, the EU is the Maldives' fourth-largest trading partner, accounting for 10 percent of its overall trade in goods in 2017 (Fact Sheets, 2019). The EU is one of India's most important sources of investment, with inward and outward stocks of EUR 11 and 76.7 billion in 2017, and bilateral trade in goods amounted to EUR 90 billion in 2018, along with a massive surplus of almost EUR 2 billion for India (Fact Sheets, 2019). The EU has signed a 'Contribution to Agriculture and Rural Development (CARD)' agreement with Nepal worth about EUR 40 million (Fact Sheets, 2019). The EU is one of Nepal's leading development partners and donors, with a three-fold rise in its development budget to EUR 360 million for 2014-2020.

The EU has had a very active presence in Bhutan since 1982 and plays a broad role in eradicating its poverty; fostering democratic processes and good governance; promoting natural assets and sustainable agriculture (Fact Sheets, 2019). The EU is allocating EUR 42 million through its Multi-Indicative Plan 2014-2020 to support the Bhutanese people (Fact Sheets, 2019). The same document describes that Afghanistan is the largest EU donation receiving country in South Asia, and the EU allocated EUR 1.4 billion between 2014 and 2020, 20 percent of which is for financial incentives associated with the reform activities. (Fact Sheets, 2019). To conclude, since South Asia has had undeniable trade relations with the EU, South Asia would be

deeply affected by EU laws and policies. The EU GDPR, therefore, has enormous consequences for South Asian data privacy regimes. This paper, thus, provides the following recommendations for reinforcing South Asia's data privacy regimes.

## SUGGESTIONS AND RECOMMENDATIONS

It is not easy to assess a specific jurisdiction or region's data protection regime, since there is no universally agreed standard for evaluating the adequacy. Although there is no sturdy rule to assess the standard of the data privacy regimes, many measures, such as (1) the definitional test, (2) the contextual surroundings, (3) principles of privacy, and (4) enforcement mechanisms, will assess the adequacy of a data protection law (Greenleaf, 2014d).

Definitional test means, whether legal regimes of South Asian laws, can be identified as data privacy laws by their definition. By contextual surroundings means, whether there is any legally binding treaty for all nations of South Asia. Also, whether the right to privacy is recognised in the Constitutions horizontally, i.e. covering both the public and private sectors. Both regional and international data protection instruments contain many privacy protection principles, from OECD Guidelines 1980 to GDPR 2018. Therefore, this test makes it possible to evaluate the privacy regimes if they align with global standards. Finally, enforcement test determines whether South Asia's privacy regimes hold similar enforcement mechanisms as enumerated in a standard data protection legislation.

The South Asian privacy regimes do not qualify for the tests mentioned earlier, despite some constitutional recognitions, clauses in domestic laws, and rulings favouring privacy. It is also clear that South Asia has a weaker culture compared to the West, including other regions such as Africa, the Caribbean, and ASEAN on the Asian continent. Undoubtedly, the culture is changing, as evidenced by recent initiatives taken by some countries in the region, such as specialised legislation in Bhutan and Nepal; the adoption of draft data protection bills by India, Pakistan and Sri Lanka, and the pledge by Bangladesh to prepare a draft soon.

Private individuals should be vigilant of their privacy interests in every sphere of digital communication and transaction. Businesses in the region need to adopt several best practices, including training their employees on data security; investing in fitting security technologies; complying with the existing data privacy laws; regularly conducting the vulnerability analysis, and developing a data breach response plan (Berecki, 2019).

The governments of the region have to adopt and implement multi-layered policy measures. These include taking privacy on priority; conducting privacy impact assessment; identifying vulnerable sectors etc. They also have to enact comprehensive data privacy laws and raise awareness among the public.

It is essential to acknowledge privacy as a matter of grave concern. Governments should conduct privacy impact assessments in major privacy vulnerable sectors, such as healthcare; accommodation; public sectors; retail, and finance (Ekran, 2019). Governments may try examining countrywide implications of privacy violations through random sampling. If results show significant consequences for a data breach cost, they should make awareness about the issue.

Subsequently, governments may undertake several interim measures, such as notifying vulnerable sectors of data breaches or industries to take care of their clients' personal data. The governments may also publish a list of vulnerable sectors and instruct them to get a government licence before processing the resident's personal data. In Malaysia, for instance, 13 types of organisations are expected to register under the Personal Data Protection Act, 2010 (PDPA, 2010). It is essential to have constitutional provisions affirming the right to privacy to ascertain the determination of securing the citizens' privacy rights. By the 19th amendment of its Constitution in 2015, Sri Lanka inserted Article 14A to incorporate privacy provision.

Most notably, policymakers in the region should consider implementing robust data protection legislation in response to the challenges raised by the growing use and advancement of ICT technology, biometric plans, national ID card programs, and intensive national surveillance systems employed in the region. Given the digital divide between the US and EU in terms of privacy regulation and Chinese regional

control, South Asian countries can adopt a fourth/moderate approach resulting from best practices.

The dominance of the GDPR is evident from its impacts on global and regional entities, its data privacy regimes, and the broad South Asian trade relations with the EU. It implies that the GDPR is the ideal option for setting up a new privacy framework reforming South Asian region's prevailing ones. The United Nations also endorses the view for countries that are seeking to enact new data protection laws. The UN Special Rapporteur on 'the right to privacy' (2019), for instance, recently noted that by following equivalent or special provisions of the Regulation, the protection of personal data should remain within the priority list of governments in the countries, not parties to the GDPR (Cannataci, 2019).

Policymakers can raise public awareness by circulating privacy issues, laws and policies. If they do not know their rights, data protection policies and protected internet browsing, individuals could be at risk of data loss. Beyond these, the judiciary can play pivotal roles to infuse trust, security and confidence by curbing diverse sorts of cyber threats, such as malware attack, denial-of-service attack, botnets, spam, privacy threats, identity theft, phishing, hacking, cracking or attacking critical infrastructure, and strengthening cybersecurity by taking steps against those activities (Abdul Ghani, 2020).

Finally, through the SAARC Working Group on Telecommunications and ICT (Islam and Karim, 2019), South Asia can adopt regional efforts, including the awareness campaign; adopting declaration; and signing treaties. As we see, over decades, the notion of 'privacy' has steadily evolved in the world and progressed through phase-by-phase developments. For example, by many of its pioneering efforts and instruments the EU have established the right to privacy at EU level. Such EU instruments include the European Convention on Human Rights and Fundamental Freedoms, 1950 (Article, 8); the Convention 108 [Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981 of the Council of Europe (CoE)]; Directive 95/46/EC, 1995, and GDPR. The African, Caribbean, and Latin American countries have also introduced regional initiatives of a similar kind. Even Asia's ASEAN nations

have a sub-regional privacy agreement (Greenleaf, 2019b), so the South Asian region can follow the patterns.

## CONCLUSION

The EU has a long history of contributing to the advancement of scholarship and global privacy law. The EU is leading the global data privacy framework, beginning with the European Convention on Human Rights 1950, and subsequent CoE Convention 108, Convention 108+, Directive 95/46/EC, and GDPR. EU dominance was explicit in the area of data privacy law after the introduction of GDPR in 2018. Owing to its omnibus legal substance, GDPR is the world's most comprehensive, robust, and all-inclusive data protection instrument in the world (Schwartz, 2019). Due to the 'Brussels Effect' (Bradford, 2012); influential market power (Wu and Goldsmith, 2006); comprehensive extraterritorial scope, and an the adequacy decision, GDPR emerges as the global standard for data protection regimes.

The GDPR extends its long arm to include all entities outside the EU borders that process EU residents' personal data either by offering the goods or services or monitoring their behaviour (GDPR, 2016).[38] To continue diverse relationships with the EU nations, particularly, the trade relation, it has become necessary for the rest of the world to have an adequate protection level for the data subjects' rights. There has been a global trend to enact the GDPR styled data privacy law to achieve the EU's adequacy status. Consequently, in shaping the data privacy regimes, the GDPR is followed worldwide, and South Asian countries cannot deny it.

GDPR can impose compliance on South Asian data controllers and processors and the processing of EU residents' personal data to fulfil the condition of 'establishment' or offer goods and services or monitor their behaviours (Article 3). GDPR compliance means that South

Asian countries should revise their data privacy legislations in line with this Regulation. Unfortunately, South Asian countries, mostly,

[38] See generally, GDPR, art 3.

Afghanistan, Bangladesh, and the Maldives, have failed to make any significant attempt to develop adequate mechanisms to protect privacy. While businesses and other entities in South Asia process EU residents' personal data, they should plan their data processing activities to comply with GDPR; otherwise, they may be subject to severe penalties for non-compliance.

Above all, functioning as a union of 27 countries, the EU is the world's leading single market and, along with the US and China, one of the three most prominent global trade players (European Union, 2017b). The EU had the second-largest share of exports and imports of goods in the world in 2016 (European Union, 2017b). Besides, the EU retains both coercive and persuasive instruments and means of shaping international affairs (Damro, 2015). The positions, laws and policies of the EU ultimately impact the entire world and South Asia with this influential market power. All South Asian countries have developed potential trade ties with the EU. Consequently, the EU GDPR has immense consequences for existing global data privacy regulations, and South Asia is no exception.

Paying heed to all those facts, the researchers believe that the region will move forward by developing successful privacy protection regimes in line with the provisions of the GDPR. In doing so, all South Asian countries attempting to prepare the Data Privacy Bill, and all those that have already implemented it should amend their Bills before actually enacting them, strictly adhering to the provisions of the GDPR. It could help South Asia achieve the EU adequacy standard; improve trade relations with the EEA countries; protect the region's personal data and data-based economy; open doors to other industries such as outsourcing, and ultimately contribute to the region's economic development.

## ACKNOWLEDGMENT

This research has not received any specific grant from any funding agency in the public, commercial, or non-profit sectors.

## REFERENCES

Abdul Ghani, A., I. M. (2020) Challenges for legal education in the era of I.R.4.0. *UUM Journal of Legal Studies*, *11*(2), 27-51.

Arakali, H. (2019, December 13). The personal data protection Bill could be a serious threat to Indians' Privacy. *Forbs India.* http://www.forbesindia.com/article/leaderboard/the-personal-data-protection-bill-could-be-a-serious-threat-to-indians-privacy/56623/1

Assembly, G. (1966a, December 16). International Covenant on Civil and Political Rights (ICCPR). https://treaties.un.org/doc/Publication/MTDSG/Volume%20I/Chapter%20IV/IV-4.en.pdf

Assembly, G. (1966b). *International Covenant on Civil and Political Rights* (ICCPR). https://treaties.un.org/doc/Publication/MTDSG/Volume%20I/Chapter%20IV/IV-4.en.pdf

Ayub, Z. A., & Yusoff, Z. M. (2020). Right of online informational privacy of children in Malaysia: A statutory perspective. *UUM Journal of Legal Studies, 9*, 222.

Babele, A. (2019, October 10). Sri Lanka introduces final draft of personal data protection Bill. *Medianama.* https://www.medianama.com/2019/10/223-sri-lanka-final-draft-of-data-protection-legislation/

Bradford, A. (2012). The Brussel's effect. *Northwestern University Law Review, 107*, 1.

Bennett, C. J. (2018). The European general data protection regulation: An instrument for the globalisation of privacy standards? *Information Polity, 23*(2), 244.

Bennett, C. J., & Raab, C. D. (2018). Revisiting the governance of privacy: Contemporary policy instruments in global perspective. *Regulation & Governance*.

Berecki, B. (2019, February 4). 5 Best Practices for Data Breach Prevention in 2019. endpointprotector.com/blog/5-best-practices-for-data-breach-prevention-in-2019/

Buttarelli, G. (2016). The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law, 6*(2).

Cannataci J. (2019, October 17). *Report of the Special Rapporteur on the Right to Privacy.* A/HRC/40/63, para 107, p. 16. https://rm.coe.int/40th-hrc-session-report-of-the-special-rapporteur-on-the-right-to-priv/1680933f08

Commission, EU. (2018a, June 24). *Statement by Vice-President Ansip and Commissioner Jourová Ahead of the Entry into Application of the General Data Protection Regulation*. https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_18_3889.

Commission, EU. (2000b, August 11). *Hague Conference on Private International Law*. https://assets.hcch.net/upload/wop/jdgmpd11.pdf

Commission, EU. (2019c). *Adequacy decisions*. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Commission, EU. (2019d January 23). *European Commission adopts adequacy decision on Japan, Creating the world's largest area of safe data flows*. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421

Council, EU. (2000b). *The Brussels I Regulation 2000: Regulation (EC) No 44/2001 of 22 December 2000 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters*. http://www.dutchcivillaw.com/legislation/brusselsone.htm

Damro, C. (2012). Market power Europe. *Journal of European Public Policy, 19*(5), 682-699.

De Hert, P. & Czerniawski, M. (2016). Expanding the European data protection scope beyond territory: Article 3 of the general data protection regulation in its wider context. *International Data Privacy Law,* 6 (3), 230-43.

DLA Piper. (2020, February 8). *EU general data protection regulation - Key changes*. https://www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/

EDPB. ( 2019). *First Overview on the implementation of the GDPR and the roles and means of the National Supervisory Authorities*. file:///C:/Users/user/Downloads/19_2019_edpb_written_report_to_libe_en.pdf

Ekran. (2019, June 27). *5 industries most at risk of data breaches*. https://www.ekransystem.com/en/blog/5-industries-most-risk-of-data-breaches

European Commission. (2015) *Countries and regions, Bangladesh: Trade Picture*. https://ec.europa.eu/trade/policy/countries-and regions/countries/bangladesh/#:~:text=The%20EU%20is%20Bangladesh's%20main,EU's%20total%20imports%20from%20Bangladesh

European Union. (2016a). *Relations between the EU and Bangladesh*. https://eeas.europa.eu/delegations/bangladesh/926/bangladesh-and-eu_en

European Union. (2017b). *The Economy*. https://europa.eu/european-union/about-eu/figures/economy_en

Fact Sheets, EU: South Asia. (2019). https://www.europarl.europa.eu/factsheets/en/sheet/181/south-asia.

Goldsmith, J. (2019, January 21). *France slaps Google with €50M fine for privacy violation under GDPR*. https://www.forbes.com/sites/jillgoldsmith/2019/01/21/france-slaps-google-with-e50m-fine-for-privacy-violation-under-gdpr/#2722b09a79ec

Greenleaf, G. (2019a). Global Data Privacy Laws 2019: 132 National Laws & Many Bills. *Privacy Laws & Business International Report*, 157 (14-18), 7.

Greenleaf, G. (2019b). Asia's Data Privacy Dilemmas 2014–19: National Divergences, Cross-Border Gridlock. *Revista Uruguaya de Protección de Datos Personales (Revista PDP)* 49-73 UNSWLRS 103, 60.

Greenleaf, G. (2019c). *Countries with Data Privacy Laws – By Year 1973-2019* (May 10, 2019). SSRN: https://ssrn.com/abstract=3386510 or https://doi.org/10.2139/ssrn.3386510

Greenleaf, G. (2014d). *Asian Data Privacy Laws: Trade & human rights perspectives.* Oxford: Oxford University Press, 10.

Greenleaf, G. (2012e). The Influence of European data privacy standards outside Europe: Implications for Globalisation of Convention 108. *International Data Privacy Law,* 2(2), 68.

Greenleaf, G. & Cottier, B. (2018). Data privacy laws and Bills: Growth in Africa, GDPR influence. *Privacy Laws & Business International Report,* 152 (18-52), 5.

Hague Conference on Private International Law. (1967). *Hague Conference: Supplementary Protocol to the Hague Convention on the Recognition and Enforcement of Foreign Judgments*. assets.hcch.net/docs/7e92b6a1-1eff-4567-ae95-9b8e93104c9e.pdf

Hern A. (2018, May 21). What Is GDPR and how will it affect you? *The Guardian*. https://www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect you

Huth, D. (2017). A pattern catalogue for GDPR compliant data protection. In *PoEM Doctoral Consortium*, 34-40.

ICO. (2018a, May 25). *The Principles*. Information Commissioner's Office, UK. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

ICO. (2018b, May 25). *International Transfers*. Information Commissioner's Office, UK. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers#adequacy-decision

ICO. (2018c, October 25*). ICO issues maximum £500,000 fine to Facebook for failing to protect users personal information*. Information Commissioner's Office, UK. https://ico.org.uk/facebook-fine-20181025?utm_source=twitter&utm_medium=iconews&utm_term=7e7dd63a-2bfd-407c-b985-c21fa7b16b6c&utm_content=&utm_campaign=%C2%A0

ICO. (2018d, September 20). *Equifax Ltd*. Information Commissioner's Office, UK. https://ico.org.uk/action-weve-taken/enforcement/equifax-ltd/

IMF. (2019, November 4). Building on South Asia's Economic success. *IMF Country Focus.* https://www.imf.org/en/News/Articles/2019/11/01/NA110219-building-on-south-asias-economic-success

Islam, M. T., & Karim, M. E. (2019, September/ October). *UPDATE: A Research Guide on the South Asian Association for Regional Cooperation* (SAARC). https://www.nyulawglobal.org/globalex/SAARC1.html#_Information_and_Poverty

Islam, M. T., & Karim, M. E. (2020). Extraterritorial application of the GDPR: An International Law Perspective. *IIUM Law Journal, 28*(2), 531-565.

*Ius Laboris* (2019, September 17). The impact of the GDPR Outside the EU. https://theword.iuslaboris.com/hrlaw/whats-new/the-impact-of-the-gdpr-outside-the-eu

Jiali, M. (2012). SAARC: Achievements and challenges. *Policy Perspectives*, 161-65.

Karim, ME. (2005) Citizen's right to privacy: Reflection in the International Instruments and National Laws. *9 Bangladesh Journal of Law*, 54.

Karim, ME. (2020) *Cyber law in Bangladesh*. Wolters Kluwer, 223.

Kennedy J. Ireland's Government agrees 'digital age of consent' should be 13. (2020). https://www.siliconrepublic.com/comms/digital-age-of-consent-ireland

KPMG. (2018, April 11). *Extraterritorial scope of the GDPR: The impact of the GDPR on organisations in Asia*. https://assets.kpmg/content/dam/kpmg/sg/pdf/2018/04/impact-of-gdpr-in-asia.pdf

Kuner, C. (2010). Data protection law and international jurisdiction on the internet (Part 2). *International Journal of Law and Information Technology, 18* (3), 227-47.

Langheinrich, M. (2018). The golden age of privacy? *IEEE Pervasive Computing, 17* (4), 4-8.

Lexology. (2019, June 5). *Happy birthday GDPR. At one year on, what have we learned*? https://www.lexology.com/library/detail.aspx?g=649cd552-7853-4abc-81c6-37af2c8dd415

Makulilo, AB. (2017). The GDPR implications for data protection and privacy protection in Africa. 1 *International Journal of Data Protection Officer, Privacy Officer & Privacy Counsel*, 15-16.

Mandavia, M. (2019, December 10). Data protection Bill: Centre has the power to exempt any government agency. *The Economic Times*. https://economictimes.indiatimes.com/tech/internet/data-protection-bill-centre-has-the-power-to-exempt-any-government-agency-from-application-of-act/articleshow/72454669.cms

Neupane. (2019, February 2018). *Introduction to the Privacy Act 2018*. https://www.neupanelegal.com/news-detail/introduction-to-the-privacy-act-2018.html

Paul, Joel R. (1991). Comity in International Law. *Harvard International Law Journal,* 32, 1.

PDPA. (2010). *Personal Data Protection Act 2010*. (Act No. 709, Malaysia).

Prasad, S. K., & Aravindakshan, S. (2020). Playing catch up–privacy regimes in South Asia. *The International Journal of Human Rights*, 1-2.

Privacy International. (2018, August). *Personal Data Protection Bill, 2018: Civil Society submission to the Ministry of Information Technology and Telecommunications*. https://digitalrightsfoundation.pk/wp-content/uploads/2018/08/DP-Comments-Brief-Final-8.8.18-1.pdf

Reed, C. (2004). *Internet law: Text and materials*: Cambridge University Press, 271.

GDPR (2016). Regulation (EU) 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. *Official Journal of the European Union, 59*(1-88), 294.

Report, S. B. (2019, November 27). *Data protection act soon: Jabbar*. https://www.thedailystar.net/business/data-protection-act-in-bangladesh-soon-1832320

Rustad, M. L., & Koenig, T. H. (2018). Towards a global data privacy standard. *Florida Law Review, 71*, 18-16.

Ryngaert, C. (2015). *Jurisdiction in International Law.* USA: Oxford University Press.

Schulze, E. (2019a, May 23). The US wants to copy Europe's strict data privacy law – But only some of It. *The CNBC.* https://www.cnbc.com/2019/05/23/gdpr-one-year-on-ceos-politicians-push-for-us-federal-privacy-law.html

Schulze, E. (2019b, November 27). *Uber fined nearly $1.2 million by British and Dutch authorities for 2016 data breach*. The CNBC. https://www.cnbc.com/2018/11/27/uber-fined-more-than-1-million-dollars-by-uk-and-dutch-authorities.html

Schwartz, P. M. (2019). Global Data Privacy: The EU Way. *New York University Law Review, 94*, 4.

S&R Associates. (2020, January 7). India: The Personal Data Protection Bill, 2019. *Mondaq*. http://www.mondaq.com/india/x/880766/data+protection/The+Personal+Data+Protection+2019

Svantesson, D. J. B. (2014). The extraterritoriality of EU Data Privacy Law-Its theoretical justification and its practical effect on US businesses. *Stanford Journal of International Law, 50*(1), 55.

Teixeira, G. A., da Silva, M. M., & Pereira, R. (2019). The critical success factors of GDPR implementation: A systematic literature review. *Digital Policy, Regulation and Governance*, *21*(4), 402.

UNHRC. (2006, September 14). Decisions of the Human Rights Committee Declaring Communications Inadmissible under the Optional Protocol to the International Covenant on Civil and Political Rights. http://www.worldlii.org/int/cases/UNHRC/2006/48.html

Walsh, R. (2013). Extraterritorial confusion: The complex relationship between Bowman and Morrison and a revised approach to extraterritoriality. *Valparaiso University Law Review, 47* (2), 629.

WB. (2016, May 24). The Potential of Intra-regional trade for South Asia. *World Bank Infographic*. https://www.worldbank.org/en/news/infographic/2016/05/24/the-potential-of-intra-regional-trade-for-south-asia

WEF. (2018a). The Global Competitiveness Report 2018: South Asia. *World Economic Forum.* http://reports.weforum.org/global-competitiveness-report-2018/south-asia/

WEF. (2019b, October 2). The South Asia Risks Landscape. *World Economic Forum.* https://www.weforum.org/whitepapers/the-south-asia-risks-landscape

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*(2), 431-53.

Wu, T. & Goldsmith, J. (2006). *Who controls the internet? Illusions of a borderless world*. New York: Oxford University Press.

Zarsky, Tal Z. (2017). Incompatible: The GDPR in the age of big data. *Seton Hall Law Review, 47*(4), 995.