

What Is Next for Digital Trade in a Post-Brexit Britain? – Examining the Regulation of Data Flows Under G.A.T.S. & Possible Implications of G.D.P.R. on Britain as a Third Country

ABHISHEK RANA* & RISHABHA MEENA**

* Abhishek Rana is a Lecturer at the Jindal Global Law School, O.P. Jindal Global University, India. He is also a visiting faculty in W.T.O. law at the Indian Society of International Law.

** Rishabha Meena is a Research Fellow at the Centre for Trade and Investment Law at the Indian Institute of Foreign Trade.

The authors would like to thank Neha Mishra and Svetlana Yakovleva for their precious comments on earlier drafts. They also wish to specify that all errors remain theirs alone.

✉ * abhishekrana@jgu.edu.in ** rishabh.149620@gmail.com

ABSTRACT

Data, much like other currencies, flows cross-border -from one jurisdiction to the other. However, it is hard to regulate the privacy aspects surrounding such free-flowing data by rules strictly based on jurisdiction. This article thereby begins by discussing the importance of data protection regulations like the General Data Protection Regulation (G.D.P.R.), followed by a brief analysis of the General Agreement on Trade in Services' pivotal role in regulating data flows and digital trade, and how it can be further used in checking the World Trade Organisation consistency of various data protection requirements resorted by the European Union (E.U.) so far under the G.D.P.R.. Lastly, the note examines how, post the Brexit transition period, the situation will change for the United Kingdom (U.K.) as it has become a third country for the E.U. data protection regime, with the authors critiquing the various models, including the recent Draft U.K.-E.U. Comprehensive Free Trade Agreement, that may help the U.K. in attaining an "adequacy" status, which is requisite for the continuation of an unconstrained digital trade with the E.U. .

KEYWORDS

*World Trade Organization; General Data Protection Regulation; Brexit;
General Agreement on Trade in Services; Data*



TABLE OF CONTENTS

| | |
|--|----|
| Introduction | 7 |
| 1. Data Protection & Digital Trade Governed by G.D.P.R. | 10 |
| 2. Regulating Data Flows & Data Privacy Measures Under G.A.T.S. | 12 |
| 2.1 Assessment of G.D.P.R. with E.U.'s Schedule of Commitment | 13 |
| 2.2. Exceptions to Non-Discrimination and Market Access Commitment | 17 |
| 3. Digital Trade Post-Transition Period: Exploring the Viable Models for the U.K. | 20 |
| 3.1 Option that the U.K. Could Have Explored | 20 |
| 3.1.1 U.K. as an E.E.A. Member: Exemption from Data Adequacy Requirement, but a Loss of Sovereignty | 20 |
| 3.2 Models that Are Being Explored | 22 |
| 3.2.1 U.K.-E.U. C.F.T.A.: a Bilateral Approach to (digital) Trade | 22 |
| 3.2.2 Full Adequacy Finding Under the G.D.P.R.: a Hard Nut to Crack | 24 |
| Conclusion | 27 |

INTRODUCTION

In the modern era, the privacy of a person is an essential facet of human rights law which necessitates legal protection,¹ and it has been enshrined in multiple international instruments covering fundamental human rights.² For instance, under Article 17 of the International Covenant on Civil and Political Rights, a person cannot be subjected to “arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation”.³ In furtherance of the same, several countries have either amended their existing legislations or have brought in new regulations to deal with the issue of privacy.⁴ The debates around data privacy, apart from being addressed from a human rights perspective, can also be understood from an international economic law lens as privacy aspects heavily influence the international trade of data; although the domestic data protection regimes of the World Trade Organisation’s [hereinafter W.T.O.] Members have tried to act as barriers to such free flow of digital trade.⁵

¹ Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

² International Covenant on Civil and Political Rights, art. 17, Dec. 16, 1966, UNTS vol. 999, 171 (hereinafter ICCPR); See Human Rights Committee, General Comment No. 16 (Thirty-second session, 1994), Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, UN Doc. HRI/GEN/1/Rev.1, 21 (1994).

³ ICCPR, Art. 17.

⁴ Australia is governed by “Australian privacy principles”, see Privacy Act 1988 (Cth) sch 1; Canada is governed by the Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5; India is governed by the Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 while the Personal Data Protection Bill, 2019, No. 373 is yet to become an Act.

⁵ Svetlana Yakovleva & Kristina Irion, *The Best of Both Worlds? Free Trade in Services and EU Law on Privacy and Data Protection*, 2 EUR. DATA PROT. L. REV.191 (2016). See Rolf H. Weber, *Regulatory Autonomy and Privacy Standards under the G.A.T.S.*, 7 ASIAN J. WTO & INT’L HEALTH L & POL’Y 25 (2012).

Even the “global organisations” that are operating their businesses in multiple countries, the privacy aspect of their business is generally governed by the domestic legislation(s) of the state in which their individual offices are based.⁶ However, situations requiring a transfer of data from one country to another, in due course, may lead to different legal systems coming into conflict with each other, especially in determining the adequate standard of data protection.⁷ This issue might entail another analogous debate on whether data protectionism hinders globalisation⁸ but the authors have not dealt with that question in this article.

Amongst the various existing data protection laws around the world, the European Union’s [hereinafter E.U.] General Data Protection Regulation [hereinafter G.D.P.R.] is one of the most comprehensive ones, and has become a global standard for most of the countries.⁹ The G.D.P.R. goes far beyond merely being domestic legislation as it has implications on other countries as well, wherein the underlying detailed and specific regulatory standards can be imposed on non-E.U. or European Economic Area [hereinafter E.E.A.] based companies, involved in gathering or transfer of data. While the EU and E.E.A. member states enjoy an unrestricted flow of data, it becomes a tricky situation when one Member from the Union decides to pull out. On March 29, 2017, the United Kingdom [hereinafter U.K.] decided to withdraw its membership from the E.U. . Brexit saw the fall of two experienced Conservative Party leaders who were initially pro-E.U. . After Britain officially left the E.U. (“Brexit”) on January 31, 2020, it entered a transition period – as per which it remains a part of the E.U. customs union; although it no longer is a part of the political institutions of the E.U. . The concerned Withdrawal Agreement has allowed E.U. law to be implemented in Britain until December 31, 2020.

Post this transition period, the digital trade that is currently being overseen by the G.D.P.R. for data protection purposes, is going to get hampered. There will be an automatic ban on any “default transfer” of personal data from the E.U. members to the U.K.. Consequentially, the legal entities existing in different E.U. member states will no longer be able to transfer personal data as per the earlier U.K.-E.U. relationship. The transfer of data will only become possible when the U.K. is able to show adequate level of protection; or there are appropriate protection measures like Binding Corporate Rules [hereinafter B.C.R.s] or Standard Contractual Clauses [hereinafter S.C.C.s]; or other conditions which are part of Chapter V of G.D.P.R. which deals with transfer of personal

⁶ Robert L. Totterdale, *Globalization and Data Privacy: An Exploratory Study*, INT’L J. INFO. SEC & PRIV., Spring 2010, at 19.

⁷ *Id.*

⁸ Dan Gunderman, *Are Data Privacy Regulations Hindering Globalization*, CYBER SECURITY HUB (Dec. 7, 2018) <https://www.cshub.com/data/news/are-data-privacy-regulations-hindering-globalization>.

⁹ Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771 (2019).

data to third countries or international organisations. Some of these requirements which form part of Chapter V, in the long run, are speculated to be a significant obstruction in digital trade flows for all the third countries, and not just the U.K., as it would require the third countries to align their data protection laws¹⁰ as per the G.D.P.R., and also factor in other privacy related aspects that are part of the legal framework of the E.U. .¹¹

This note, in Part II, traces the importance of G.D.P.R., and reflects on how it will impact the digital trade flows between the E.U. and third countries as some of its provisions impose obligations relating to the E.U. data subjects even on the companies based outside the E.U. . Part III provides a basic understanding of the General Agreement on Trade in Services' [hereinafter G.A.T.S.] framework responsible for regulating the trade in services and provisions essential to govern the transboundary flow of data. It assesses the G.A.T.S. consistency of various G.D.P.R. provisions providing for the usage of either data protection measures such as S.C.C.s and B.C.R.s or availing an "adequacy status" for the third countries. Part IV delves into the options available to the U.K. for regulating and protecting the transfer of data post-transition period with the E.U./E.E.A. . The authors analyse the two possible options that the U.K. is currently exploring for a smoother future exchange of data, while also taking into account other non-trade concerns that might come with these options. The two options that have been critically analysed include: (i) the recent Draft E.U.-U.K. Comprehensive Free Trade Agreement [hereinafter E.U.-U.K. C.F.T.A.] released in May 2020, which while excludes data adequacy, interestingly includes "digital trade" under the draft agreement; or (ii) U.K. showing an adequate level of data protection under its domestic legislation, which can later meet the equivalence of data standards set by the E.U. . Finally, the note recommends the best option that the U.K. might have moving forward, and what steps the private parties can take to protect their data in case there is a delay in finalising a possible arrangement between the post-transition period U.K. and the E.U. .

¹⁰ The requirement of an equivalent level of data protection or alignment of law has been imposed by G.D.P.R. because a lower-level data protection in the transferee country poses threat and risks to the privacy of the individual. LEE A. BYGRAVE, *DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC AND LIMITS* 79 (2002).

¹¹ Graham Greenleaf, "European" *Data Privacy Standards Implemented in Laws Outside Europe* 149 *Privacy Laws & Business International Report* 21-23 (2017) Additionally, it is not only G.D.P.R. with which the UK has to comply with. Under Article 45(2), the UK is also required to take into account the national security laws, defence laws, human rights laws, etc; C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd.*, 2020 E.C.R.

1. DATA PROTECTION & DIGITAL TRADE GOVERNED BY G.D.P.R.

The E.U.'s data protection regime since the 1990s has been extensively regulated and was always applied uniformly for all types of personal information; unlike in the United States [hereinafter U.S.] where generally sector-specific data privacy guidelines exist for the regulation of personal information - varying from industry-to-industry.¹² So, with the introduction of the revolutionary G.D.P.R.,¹³ replacing 1995 Data Protection Directive,¹⁴ all the legal entities and undertakings¹⁵ (majorly businesses and public bodies) covered under this regulation were given two years to prepare themselves for the changes,¹⁶ with the G.D.P.R. finally entering into force on May 25, 2018.

G.D.P.R. led to an introduction of specific new rules along with the augmentation of the already existing regulations,¹⁷ with heavy penalties if the requirements as per the regulations are not complied with. The Data Protection Authorities have the power to impose strict sanctions in the form of progressive fines up to €20m or up to 4% of an undertaking's worldwide annual turnover.¹⁸ Another vital distinction to note here is that the E.U.-wide data protection law is in the form of a regulation,¹⁹ and not a directive, making it directly applicable to the member states without a need to be incorporated into their domestic laws.²⁰ Thus, G.D.P.R.'s enforcement affected nearly every company in the E.U., but the ones who are affected by it the most are responsible for holding, controlling, and processing²¹ the data of the consumers,²² and it majorly includes the parties in a digital economy, viz. the technology firms and the marketers, along with the

¹² Kurt Wimmer & Joseph Jones, *Brexit and Implications for Privacy*, 40 *FORDHAM INT'L L.J.* 1553 (2017). However, in case of California, there is no sector specific laws for data protection. The California Consumer Privacy Act 2018 is single legislation governing data protection which applies to all types of business upon fulfilment of certain criteria.

¹³ Council Regulation 2016/679/EC of the European Parliament and of the Council on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data and Repealing Directive 95/46/EC, 2016 O.J. (L119) 1 [hereinafter G.D.P.R.].

¹⁴ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281).

¹⁵ Mario Rosentau, *The General Data Protection Regulation and Its Violation of EU Treaties*, *JURIDICA INT'L*, March 2018, at 36, 38.

¹⁶ Matt Burgess, *What is GDPR? The summary guide to GDPR compliance in the UK*, *WIRED.CO.UK* (Mar. 24, 2020), <https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018>.

¹⁷ Wimmer & Jones, *supra* note 12, at 1555.

¹⁸ Alex Hern, *What is GDPR and how will it affect you?*, *THE GUARDIAN* (May, 21, 2018), <https://www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you>.

¹⁹ Section 2 of the European Communities Act 1972 provides that all the EU regulations and treaties are applicable to the U.K. without express incorporation under a domestic law.

²⁰ Wimmer & Jones, *supra* note 12, at 1555.

²¹ G.D.P.R. makes a differentiation between "controller" and "processor" of data.

²² Wimmer & Jones, *supra* note 12, at 1554.

data brokers who help in connecting such technology firms to marketers.²³ These companies are presumed to incur the maximum amount of legal and technical costs.²⁴

G.D.P.R. continues to allow for a free transfer of personal data between the E.U./E.E.A. member states, insofar as the rules for the protection of such data are followed. Data can also be transferred to third countries, but only in certain circumstances, which generally includes either (i) transfer of data to a third country whose data protection regime has been considered by the European Commission to be “adequate” (deciphered to mean “essentially equivalent” to the data protection regime in the E.U.²⁵) or (ii) relying on other safety measures (like S.C.C.s or B.C.R.s)²⁶ with a business organization existing in a third country that has not yet obtained ‘adequacy status’.²⁷ Personal data can be transferred to third countries outside the E.U./E.E.A. without these usually relied upon options too, in special situations and single cases.²⁸

The E.U. members have long enjoyed the benefits of having an unimpeded transfer of data, especially with the E.U. proactively signing different arrangements with third countries ranging from the concept of sharing of law enforcement data²⁹ (e.g., under the E.U.-U.S. “Umbrella” Agreement)³⁰ to other data sharing courses of action (e.g., the E.U.-Canada Passenger Name Record Agreement).³¹ However, after the transition period, the U.K. will turn into a “third country” for data regulation in the E.U., which implies that the personal data is bound to be severely confined.³² Therefore, to guarantee the transfer of such personal data with few limitations or restrictions between the E.U. and the U.K., the U.K. government will have to assess whether it can accede to

²³ *Id.*

²⁴ Rosentau, *supra* note 15, at 38.

²⁵ C-362-14, Max Schrems v. Data Protection Commissioner, 2015 E.C.R. 73,74.

²⁶ Jeffrey N. Berman, *GDPR - What are the Model Contract Clauses?*, BFLAW.COM (Dec. 20, 2018), <https://www.bfvlaw.com/gdpr-what-are-the-model-contract-clauses/>.

²⁷ As of now, Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework) have been granted the adequate standard.

²⁸ Such special situations and single cases are applicable when the data subject has given consent to such transfer even after knowing all the risks; usually in circumstances where such a transfer is necessary like in the instance of public interest. However, these cases become applicable only when (i) there is a single occasion; (ii) it concerns limited data subjects; and (iii) takes place after weighing of interest. GDPR art. 49; *Transfer of data to a third country*, DATAINSPEKTIONEN.SE, <https://www.datainspektionen.se/other-lang/in-english/the-general-data-protection-regulation-gdpr/transfer-of-data-to-a-third-country/>.

²⁹ Wimmer & Jones, *supra* note 12, at 1556-1557.

³⁰ Agreement between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offences, 2016 O.J. (L 336/3) 3-13.

³¹ Draft agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data. See Proposal for a Council Decision on the Conclusion of the Agreement Between Canada and the European Union on the Transfer and Processing of Passenger Name Record Data, COM (2013) 528 final (July 18, 2013).

³² Stuart Anderson, *Brexit Data Confusion*, INT’L J. DATA PROT. OFF., PRIV. OFF. & PRIV. COUNS, 2018, Volume 2 at 10.

the existing arrangements or manage to get a separate bilateral agreement. It is vital to maintain and potentially reproduce the current arrangements as it would let the critical flow of personal data to continue, and would further help in settling any international legal disputes that may arise from time to time when the companies have to honour the requests for data to be shared for law enforcement purposes.³³

2. REGULATING DATA FLOWS & DATA PRIVACY MEASURES UNDER G.A.T.S.

The W.T.O.'s establishment, on 1 January 1995³⁴, led to an emergence of an effective administrative and juridical system in the rules of global trading. The multilateral agreements under the W.T.O., which are attached as Annexes to the Marrakesh Agreement, not only dealt with trade in goods³⁵, but also in services³⁶ and intellectual property rights³⁷. It was the modernisation, ubiquitous digitisation, and free flow of data through the internet which unravelled the need for regulating trade in digital economic sectors³⁸ with the help of G.A.T.S. .³⁹ Thus, G.A.T.S. has dealt with such issues primarily through five obligations and commitments, viz. (i) violation of the Most-Favored Nation [hereinafter M.F.N.] treatment⁴⁰, (ii) violation of the Market Access [hereinafter M.A.] commitments⁴¹, (iii) violation of National Treatment [hereinafter N.T.]⁴², (iv) domestic regulations⁴³ and (v) general⁴⁴ and security⁴⁵ exceptions to M.F.N., N.T. and M.A. commitments.

³³ Wimmer & Jones, *supra* note 12, at 1559.

³⁴ Marrakesh Agreement Establishing the World Trade Organization, Apr. 15 1994, 1867 UNTS 3, 1868 UNTS 3, 1869 UNTS 3.

³⁵ General Agreement on Tariffs and Trade 1994, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1867 U.N.T.S. 187, 33 I.L.M. 1153 (1994) [hereinafter GATT 1994].

³⁶ See General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167 (1994) [hereinafter G.A.T.S.].

³⁷ Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994) [hereinafter TRIPS Agreement].

³⁸ Margaret Byrne Sedgewick, *Transborder Data Privacy as Trade*, 105 CAL. L. REV 1513, 1542 (2017).

³⁹ G.A.T.S. in its Article I:2 mentions about governing "trade in services" through four modes of supply, which are "cross border supply" (mode 1), "consumption abroad" (mode 2), "commercial presence" (mode 3), and "presence of natural persons" (mode 4); See Weber, *supra* n. 5.

⁴⁰ G.A.T.S., *supra* note 36.

⁴¹ *Id.* Art. XVI.

⁴² *Id.* Art. XVII.

⁴³ *Id.* Art. VI.

⁴⁴ *Id.* Art. XVI.

⁴⁵ *Id.* Art. XVII.

In this part, the authors explore the consistency of various regulations of G.D.P.R. in light of the commitments undertaken by the E.U. under G.A.T.S., as these regulations form the basis of international data transfer with third countries.

2.1 ASSESSMENT OF G.D.P.R. WITH E.U.'S SCHEDULE OF COMMITMENT

The G.A.T.S. borrowed the basic principles of non-discrimination and market access, amongst others, from the General Agreement on Tariffs and Trade [hereinafter G.A.T.T.] 1947, and in so doing applied these principles in service sectors such as finance, communication, digital market, education, tourism, licensing, *et cetera*.⁴⁶ In principle, any limitations amounting to zero quota or total ban put forth on the transfer of any data to other Members or third countries will constitute a restriction on M.A. .⁴⁷

However, services that are covered under G.A.T.S. are not automatically opened to competition, except in the case of general commitments like most favoured nation treatment. W.T.O. Members guarantee the access to their domestic markets only for those sectors or modes of supplies that have been specified in their “schedule of commitments”, and further accepted by individual Members with or without limitations.⁴⁸ This schedule is legally binding and an integral part of the G.A.T.S.,⁴⁹ where each Member specifies in which sector, in relation to what service, and to what extent the commitment taken shall bind them. Members can select to either be fully bound⁵⁰ or be bound with limitations.⁵¹ Therefore, it becomes vital to, firstly, classify the category in which the data transfer services would fall; secondly, identify the mode through which such services are supplied; and lastly, assess the consistency of the data regulation provisions in accordance with the commitments undertaken in the national treatment and market access categories. These requirements together “*create the tapestry of fundamental principles used by most nations to regulate international trade*” in data services.⁵²

⁴⁶ *Id.* Art. I; See also *The most dynamic segment of International Trade: Trade in Services*, WTO.ORG (2015) https://www.wto.org/english/thewto_e/20y_e/services_brochure2015_e.pdf.

⁴⁷ *Understanding on commitments in financial services*, https://www.wto.org/english/tratop_e/serv_e/21-fin_e.htm. This principle can be applied to all types of services involving data transfer.

⁴⁸ See *Schedules of specific commitments and lists of Article II exemptions*, WTO.ORG, https://www.wto.org/english/tratop_e/serv_e/serv_commitments_e.htm.

⁴⁹ Svetlana Yakovleva & Kristina Irion, *The Best of Both Worlds - Free Trade in Services and EU Law on Privacy and Data Protection*, 2 EUR. DATA PROT. L. REV. 191, 192 (2016).

⁵⁰ A full commitment of market access means a prohibition to maintain, predominantly qualitative, market access barriers included in the exhaustive list of Art. XVI: 2. Yakovleva & Irion, *supra* note 5, at 191.

⁵¹ If a party wants to preserve certain market access barriers banned by Art. XVI:2 in sectors and in relation to modes of supply where it undertook a specific market access commitment, such limitations should be included in the Services Schedule in the column ‘Limitations on Market Access’. See *Guide to reading the GATS schedules of specific commitments and the list of Article II (MFN) exemptions*, WTO.ORG, https://www.wto.org/english/tratop_e/serv_e/guide1_e.htm.

⁵² Joshua D. Blume, *Reading the Trade Tea Leaves: A Comparative Analysis of Potential United States WTO - GATS claims against Privacy, Localization, and Cybersecurity Laws*, 49 GEO. J. INT. L. REV. 801, 807 (2018).

So, to determine the type of service under which data transfer through digital trade would fall under, we take a cue from the 1993 Scheduling Guidelines⁵³ that illustrated the need for a classification of sectors and sub-sectors based on the Services Sectoral Classification List,⁵⁴ which is further based on the United Nations Central Product Classification⁵⁵. While classifying a particular service, the focus must be laid on the teleological interpretation of the character of that service, the purpose that is being achieved,⁵⁶ and any other component that would give an essential characteristic to that particular service.⁵⁷ From the explanatory notes for the services in the U.N. Central Product Classification, it is evident that the data & message transmission services consist of network services that transfer data, receive and send electronic messages, and manipulate the information in databases.⁵⁸ The critical feature of telecommunication services is the transmission and reception of signals by electromagnetic waves.⁵⁹ Since data transfer requires the transmission and reception of signals,⁶⁰ data transfer services are classified under the telecommunication ones.

Secondly, under Article I:2 of G.A.T.S., services are supplied through four different modes, viz. cross-border (mode 1), consumption abroad (mode 2), commercial presence (mode 3), and movement of natural persons (mode 4). The supply of services from territory of one W.T.O. Member to the territory of another W.T.O. Member, without the presence of the service supplier in the territory of the service receiver, is the cross-border supply of service.⁶¹ Therefore, the international data transfer is cross-border of service as the transfer occurs without the presence of the service provider in the destination country.

Thirdly, the W.T.O. Members also undertake specific commitments for M.A. and N.T. under Article XVI and Article XVII of the G.A.T.S. respectively, with the W.T.O. consistency of a measure determined based on the commitments taken. A Member, therefore, can rely on one of the three forms, by opting for “none” (no limitations to be

⁵³ See Group of Negotiations on Services, Uruguay Round, Scheduling of Initial Commitments in trade in Services, Explanatory Note, GATT Doc. MTN.GNS/W/164 ¶ 4 (Sept. 3, 1994).

⁵⁴ GATT Secretariat, *Services Sectoral Classification List*, GATT Doc. MTN.GNS/W/120 (July 10, 1991).

⁵⁵ U.N. Dep't of Int'l Econ. & Soc. Affairs, Provisional Central Product Classification, U.N. Doc. ST/ESA/STAT/SER.M/77 (2002).

⁵⁶ See ROLF H. WEBER & MIRA BURRI, *CLASSIFICATION OF SERVICES IN THE DIGITAL ECONOMY* 93 (2013).

⁵⁷ See Ines Willemyns, *GATS Classification of Digital Services - Does 'The Cloud' Have a Silver Lining?*, 53 J. WORLD TRADE 59, 76 (2019).

⁵⁸ U.N. Dep't of Int'l Econ & Soc. Affairs, Provisional Central Product Classification, 140 Part II, U.N. Doc. ST/ESA/STAT/SER.M/77, U.N. Sales No. E.91.XVII.7 (1991), Part III, 223.

⁵⁹ G.A.T.S, Annex on Telecommunication Service.

⁶⁰ See *Data Transmission - Parallel v. Serial*, QUANTIL, <https://www.quantil.com/content-delivery-insights/content-acceleration/data-transmission/>.

⁶¹ Panel Report, *Mexico - Measures Affecting Telecommunications Services*, ¶ 7.28, WTO Doc. WT/DS204/R (adopted June 1, 2004) [hereinafter Panel Report, Mexico - Telecommunications].

imposed),⁶² “unbound” (any type of limitations can be imposed),⁶³ or bound (specific type of limitations are agreed upon to be imposed) in its Schedule of Commitments. In the case of G.D.P.R., the E.U. has not undertaken any commitments for the cross-border mode of supply in the telecommunication services by inscribing “none” under the concerned Schedule,⁶⁴ which means that it is now prohibited from imposing any restriction(s). Therefore, the requirements such as S.C.C.s⁶⁵ or B.C.R.s⁶⁶ or even the adequacy status becomes difficult to justify.

Article XVI:2 G.A.T.S., dealing with M.A., provides for a list of measures that should not be maintained in sectors where a country has undertaken full M.A. commitments.⁶⁷ Thus, the M.A. commitments which are not indicated in a Member’s schedule of commitments, like the setting up of high privacy standards; or by providing any particular benefits on providing source code; or registration requirements for data collection⁶⁸, would end up being violative of Article XVI:2(a) and (c) of the G.A.T.S. .⁶⁹ It was in the *U.S. - Gambling*⁷⁰ dispute where the Appellate Body held that the remote supply of betting and gambling is to be categorised as *cross-border electronic delivery of services*, with the disputed measure of limiting the number of service suppliers held to be a quantitative restriction on cross border supply, thereby violative of the M.A. principle.⁷¹ Also, considering the ratio in *Mexico - Telecom*, where the Panel held that the routing requirement for international telecommunication is inconsistent with Article XVI:2 (a), (b), and (c).⁷² Therefore, since the E.U. has inscribed “none” in the “limitations on market access” column, it means that the G.D.P.R. cannot have an effect of zero quota

⁶² Panel Report, *United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, ¶ 6.279, WTO Doc. WT/DS285/R (adopted Nov. 10, 2004) [hereinafter Panel Report, *US — Gambling*].

⁶³ See MITSUO MATSUSHITA ET AL., *THE WORLD TRADE ORGANIZATION LAW, PRACTICE, AND POLICY* 598 (3rd ed. 2015).

⁶⁴ G.A.T.S., *supra* note 36.

⁶⁵ The Standard Contractual Clauses [hereinafter S.C.C.s] are the standard sets of contractual terms and conditions governing data transfer between the EU or E.E.A. and the non-E.U. entities which must be present in the contract between these two entities (if the non-E.U. countries has not obtained adequacy status). It ensures the compliance with the G.D.P.R. requirements by the non-E.U. entities at private individual level. See *Standard contractual clauses for data transfers between EU and non-EU countries (European Commission)*, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

⁶⁶ Binding Corporate Rules are legally binding and enforceable internal rules and policies to govern international data transfers within the organization having its branches in the EU and outside the EU, where the country in which non-EU branch of the organization is located has not obtained adequacy status. See *Binding Corporate Rules - The General Data Protection Regulation*, PWC (2019), <<https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf>.

⁶⁷ Panel Report, *United States - Gambling*, *supra* note 62, § 6.298.

⁶⁸ Weber, *supra* note 5, at 25. Rolf H. Weber, *Regulatory Autonomy and Privacy Standards under the GATS*, 7 *ASIAN J. WTO & INT’L HEALTH L & POL’Y* 25 (2012).

⁶⁹ *Id.*

⁷⁰ Appellate Body Report, *United States Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WTO Doc. WT/DS285/AB/R (Apr. 7, 2005) [hereinafter Appellate Body Report, *US - Gambling*].

⁷¹ Yakovleva & Irion, *supra* note 5, at 212.

⁷² Panel Report, *Mexico - Telecommunications*, *supra* note 61, § 7.85.

or a complete prohibition. However, the requirements such as S.C.C.s, B.C.R.s, and other safety measures as required by the E.U. can be argued to be inconsistent with the E.U.'s obligations,⁷³ given that such high privacy standards may act as quantitative restrictions having the effect of limiting the supply of services – especially in the sectors like finance and banking, transport services (in terms of storing passenger data), global accounting firms, etc. In the recent 2020 decision of *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Schrems II)*, the Court validated the S.C.C.s but imposed an obligation on the data exporter to ensure the safeguard of data which being exported to a third country which must take into account the legal system of the importing country and the data access by the third country.⁷⁴ The non-fulfilment of aforementioned requirements would consequently lead to non-delivery of services, thereby naturally limiting the number of service suppliers, which can be successfully challenged under Articles XVI:2(a) and XVI:2(c) of G.A.T.S. .⁷⁵

Meanwhile, the requirement of N.T. under G.A.T.S. is violated when a W.T.O. Member provides less favorable treatment to foreign services than the domestic services.⁷⁶ However, contrary to the G.A.T.T., N.T. is not a mandatory obligation, but a conditional one, with its violation based on the limitations existing in a Member's Schedule of Commitments.⁷⁷ Article XVII G.A.T.S. requires Members to accord “like” foreign services and service suppliers with either *de jure* or *de facto* “treatment no less favourable” than their domestic counterparts.⁷⁸ In determining whether the product is “like” or not, the Dispute Settlement Body [hereinafter D.S.B.] has adjudicated on the four parameters given by working parties on Border Tax Adjustment.⁷⁹ An interesting case study on the national treatment provision under G.A.T.S is *China-Publications and Audiovisual Products*.⁸⁰ The measure at dispute herein were the restrictions placed on the

⁷³ Blume, *supra* note 52, at 822-23; see also DANIEL CROSBY, ANALYSIS OF DATA LOCALIZATION MEASURES UNDER WTO SERVICES TRADE RULES AND COMMITMENTS 7 (2016). (E15 Initiative Policy Brief, 2016).

⁷⁴ Case C-311/18 *Data Protection Commissioner v. Facebook Ireland Ltd.*, para. 104-105 (2020).

⁷⁵ Weber, *supra* note 5, at 33.

⁷⁶ G.A.T.S., *supra* note 36.

⁷⁷ Panel Report, *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, ¶7.950, WTO Doc. WT/DS363/R and Corr.1 (Jan.19, 2010) [hereinafter Panel Report, *China- Publications and Audiovisual Products*].

⁷⁸ See Aditya Mattoo, *Services Globalization in an Age of Insecurity: Rethinking Trade Cooperation* (World Bank Group Policy Research Working Paper 8579, 2018).

⁷⁹ Four parameters given in the working party report include – (i) whether the product is “similar”, (ii) product’s end-uses, (iii) consumers’ tastes and habits, (iv) product’s properties, nature and quality. See General Agreement on Tariffs and Trade, *Report by the working parties on Border Tax Adjustments*, L/3464, (adopted Dec.2, 1970) [hereinafter G.A.T.T.].

⁸⁰ Appellate Body Report, *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment*, WTO Doc. WT/DS363/AB/R (Dec. 21, 2009) [hereinafter Appellate Body Report, *China- Publications and Audiovisual Products*]. After US-Gambling Appellate Body Report, *China- Publications and Audiovisual Products* Appellate Body Report is the only case that dealt with public morality under General Security Exception.

foreign-invested enterprises in China relating to the importation and distribution of *foreign* publications, electronic publications, and audiovisual products. The Chinese government imposed harsh and onerous content review requirements on foreign products in comparison to their like domestic products. The Appellate Body held that such Chinese measures are inconsistent with Article XVII as China undertook no commitments under the concerned sector, and thereby such application of content review requirement was held to be violative of Article XVII.⁸¹

Similarly, it can be contended that international data transfer rules under the G.D.P.R. may lead to a potential violation of N.T. principle as the non-E.U. entities have to comply with additional requirements such as adequacy status, B.C.R.s or S.C.C.s, and other special situations which may cause additional burdens, economic as well as administrative, on the foreign services. However, footnote 10 to Article XVII creates an exception by excluding any inherent competitive disadvantages which result from the foreign character of the relevant services or service suppliers as a ground for violation of the N.T.;⁸² hence, the E.U. can justify such requirements under Footnote 10. Also, the level of data protection has a significant influence on the “likeness” analysis of the domestic and foreign services which may make them “unlike”,⁸³ and the E.U. can easily rely on the argument that the services provided by the E.U. and foreign services are not alike.

2.2. EXCEPTIONS TO NON-DISCRIMINATION AND MARKET ACCESS COMMITMENT

The exceptions clause in the W.T.O. agreements exists to allow the Members to adopt such measures that are otherwise W.T.O. inconsistent with the objective of enabling the members to pursue their policy objectives that are legitimate and important.⁸⁴ The general exceptions clause under Article XIV of G.A.T.S. and Article XX of G.A.T.T. provide

⁸¹ See Panel Report, *China- Publications and Audiovisual Products*, ¶ 7.1097, 7.1142, 7.1170, WTO Doc. WT/DS363/R and Corr.1 (Jan.19, 2010).

⁸² See G.A.T.S., Apr. 15, 1994, Art. XVII, 1869 U.N.T.S. 183.

⁸³ For instance, the data localization requirements in Europe for the business to business services has modified the competitive relationship between the services and service supplier because of the evolution of localization requirements into recurrent requirement of the enterprise customers. So, services coming from countries which have the adequate level of protection would receive favourable treatment; however, such services would not be considered “like” for the national treatment test. See Svetlana Yakovleva & Kristina Irion, *The Best of Both Worlds? Free Trade in Services and EU Law on Privacy and Data Protection*, 2 EUR. DATA PROT. L. REV. 191, 204 (2016). It must be noted that national treatment requirement would depend on claim brought under different sector having a connection with data transfer (such financial services, etc) and hence no specific analysis is given to any one service over another. Blume, *supra* note 52, at 807.

⁸⁴ See Appellate Body Report, *US - Gambling*, *supra* note 70, § 290-291.

different grounds for when the W.T.O. Members can get away from their agreed obligations and commitments. Under the G.A.T.S., these general exceptions can be invoked to: (a) protect public morals or maintain public orders, (b) protect human, animal or plant life or health, (c) secure compliance with laws or regulations which are not inconsistent with the provisions of G.A.T.S.,⁸⁵ (d) collection or imposition of direct taxes, and (e) differential treatment due to the agreement on avoidance of double taxation. Article XIV(c)(ii) G.A.T.S. is crucial here, specifically in the case of G.D.P.R., as this particular exception can be invoked if it is necessary to secure compliance with such laws or regulations that exist for “*the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.*”⁸⁶ Article XIV of G.A.T.S., much like Article XX of G.A.T.T., consists of several tests to check the legality of the measure. The authors believe that G.D.P.R. can be justified under the general exceptions only if it falls either under Article XIV(a) or Article XIV(c)(ii), but under these exceptions, the members are still required to prove the “necessity”, which is based on “weighing and balancing” test involving the importance of the values being protected, the extent of the measure’s contribution, and trade restrictiveness of the measure.⁸⁷ Apart from this, if any Member wants to claim a general exception, they would also have to fulfil the conditions in the Chapeau which requires that the *application of the measure must not constitute “arbitrary” or “unjustifiable” discrimination where the same conditions prevail, and a “disguised restriction on trade in services”*. It ensures that the Members’ right to avail exceptions is exercised in a reasonable manner and does not frustrate the rights accorded to other Members under the substantive rules of the G.A.T.S. .⁸⁸

In the *U.S. - Gambling* dispute, the U.S. invoked the “public morals” exception under the Wire Act by claiming that the measures taken are necessary to prevent⁸⁹ and protect the nation’s public morals and further maintain public order.⁹⁰ The pre-requisite for the justification of invoking a general exception clause is that it should be done strictly in a situation “*. . . where a genuine and sufficiently serious threat is posed to one of the fundamental interests of the society*”.⁹¹

⁸⁵ See G.A.T.S., *supra* note 36.

⁸⁶ *Id.* Art. XIV(c)(ii); For a fully-fledged analysis of how this may occur, see generally KRISTINA IRION, SVETLANA YAKOVLEVA & MARIJA BARTL, *TRADE AND PRIVACY: COMPLICATED BEDFELLOWS? HOW TO ACHIEVE DATA PROTECTION-PROOF FREE TRADE AGREEMENTS* 27-33 (2016). see generally Weber, *supra* note 5, at 32-34

⁸⁷ See Appellate Body Report, *US - Gambling*, *supra* note 70, § 306.

⁸⁸ See also *id.* § 338-369.

⁸⁹ See The measure at issue was “the total prohibition on the cross- border supply of gambling and betting services”. See Appellate Body Report, *US - Gambling*, *supra* note 70, § 10-11.

⁹⁰ See *id.* § 316.

⁹¹ Yves Poullet, *Transborder Data Flows and Extraterritoriality: The European Position*, 2 J. INT’L COM. L. & TECH. 141 (2007).

“Public order” points towards the need for safeguarding fundamental interests of the nation⁹² which are highly subjective and dependent on many peculiar factors, giving Members a free hand to determine the appropriate level of protection for themselves.⁹³ The term “order” is read with footnote 5 of G.A.T.S., and it can also be termed as the preservation of the fundamental interests of society.⁹⁴ The U.S., in the gambling dispute, successfully established the prima facie case of “necessity” within the meaning of Article XIV(a) by showing that there were no other reasonably available measures.⁹⁵ Nevertheless, they failed the chapeau test because the measure did not apply equally on the domestic and the foreign service suppliers.⁹⁶ The authors believe that the restrictions under the G.D.P.R. can also rely on the same public morals and public order exception as these restrictions are currently being promoted as a means to enhance data security, i.e. protecting the privacy and security of personal information,⁹⁷ which is one of the fundamental interests of society.

Meanwhile, the exception under Article XIV(c)(ii) remains highly relevant for any measure seeking to secure protection of privacy of individuals under the G.A.T.S. .⁹⁸ It remains imperative that the three-fold test is fully satisfied before any Member relies on the said defence,⁹⁹ which involves (i) the identification of laws and regulations with which the measure is expected to secure compliance; (ii) such laws and regulations must not be inconsistent with the W.T.O. norms; and (iii) the measure is imposed to ensure compliance with those laws and regulations.¹⁰⁰ Further, a Member can impose any measure consistent with W.T.O. norms to achieve “zero-risk” level of protection.¹⁰¹ Once the three-fold test is satisfied, the Member would still have to show “necessity” and pass other criteria under the Chapeau. One such essential requirement under the Chapeau is that of the “like condition” comparison. Since the third party requirements under the G.D.P.R. are based on the fact that the data protection regime, including the national security system, in the E.U. and the third country is not at the same level¹⁰² which is a

⁹² See Panel Report, *European Union and its member States – Certain Measures Relating to the Energy Sector*, ¶ 296, WTO Doc. WT/DS476/R/Add.1 (circulated Aug. 10, 2018) [adoption/appeal pending].

⁹³ See generally Appellate Body Report, *US – Gambling*, supra note 70, §6.461.

⁹⁴ See Appellate Body Report, *Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef*, ¶176, WTO Doc. WT/DS161/AB/R, WT/DS169/AB/R (adopted Jan. 10, 2001) [hereinafter Appellate Body Report, *Korea – Beef*].

⁹⁵ See e.g., Appellate Body Report, *US – Gambling*, supra note 70, § 326.

⁹⁶ See e.g., *id.* § 372.

⁹⁷ See also Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J., 677, 718 (2015).

⁹⁸ See also G.A.T.S., supra note 36.

⁹⁹ See Panel Report, *United States – Measures Relating to Shrimp from Thailand*, ¶7.7174, WTO Doc. WT/DS343/R (adopted Feb. 29, 2008).

¹⁰⁰ *Id.*

¹⁰¹ See e.g., Appellate Body Report, *Korea-Beef*, supra note 94, §181.

¹⁰² See Peter Swire, *Foreign Intelligence and Other Issues in the Initial Opinion in Schrems II*, LAWFARE (Dec.23, 2019), <https://www.lawfareblog.com/foreign-intelligence-and-other-issues-initial-opinion-schrems-ii>.

vital consideration under the G.D.P.R. .¹⁰³ Therefore, it is established that the conditions prevailing in these two countries are not alike, and the arbitrariness and justifiability of the measures shall not be challenged. Therefore, there is a strong possibility that a complaint in the near future may be brought before the D.S.B. against the E.U., pertaining to the high regulatory standards imposed by the G.D.P.R., which go against the E.U.'s schedule of commitments under G.A.T.S. . Nevertheless, the E.U. can continue to rely on the justification of its measures under the general exceptions provided by Article XIV of G.A.T.S. .¹⁰⁴

3. DIGITAL TRADE POST-TRANSITION PERIOD: EXPLORING THE VIABLE MODELS FOR THE U.K.

Once the U.K. becomes a “third country” from the context of G.D.P.R., that is where the things change. In order to obtain an adequate data protection level, the U.K. will have to, first, seek approval from the European Commission, like other third countries. Apart from opting for the adequacy ruling, there are other options available that the U.K. can rely upon to regulate its future digital trade with the E.U. . So far, it was seen that the U.K. was inclined towards opting for the adequacy status approach; however, recently, the U.K. has also planned to negotiate a comprehensive free trade agreement with the E.U. .

3.1 OPTION THAT THE U.K. COULD HAVE EXPLORED

3.1.1 U.K. AS AN E.E.A. MEMBER: EXEMPTION FROM DATA ADEQUACY REQUIREMENT, BUT A LOSS OF SOVEREIGNTY

A few scholars had attempted to explore the E.E.A. Agreement model for the post-Brexit U.K., not essentially considering it from a data transfer aspect. It was noticed that since E.U. laws are directly applicable to E.E.A. Members without specific incorporation by their members,¹⁰⁵ and G.D.P.R. already applies to all the E.E.A. Members,¹⁰⁶ if the U.K.

¹⁰³ See generally *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data*, COM(2020) 66 final (Feb. 19, 2020) [hereinafter *European Strategy for Data*].

¹⁰⁴ See Federica Velli, *The Issue of Data Protection in EU Trade Commitments: Cross-Border Data Transfers in GATS and Bilateral Free Trade Agreements*, 4 EUR. PAPERS 881 (2019).

¹⁰⁵ See Consolidated Version of the Treaty on the Functioning of the European Union art. 15, May 9, 2008, 2008 O.J. (C 115) 47 [hereinafter T.F.E.U.].

¹⁰⁶ See generally Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement, 2018 O.J. (L 183).

joins E.E.A., then the U.K. is not required to be treated like third countries in the post-transition period. In the context of Britain,¹⁰⁷ the most important issue is whether the U.K. would remain a member of the E.E.A. after its withdrawal from the E.U. .

The E.E.A. Agreement aims to build economic cooperation by promoting cross-border trade between the E.U. and the E.E.A. member States (i.e. Iceland, Liechtenstein and Norway), with equal competitive opportunities.¹⁰⁸ Although the E.E.A. members are not part of the E.U., they still get to enjoy cooperation with the E.U. member states in the field of economy, security and society.¹⁰⁹ Meanwhile, it is important to note that the automatic application of the E.U. legislation on the E.E.A. Members is bound to raise concerns by being equivalent to challenging a nation's sovereign powers as the E.E.A. members are not given the opportunity to participate in the discussions of all the E.U. legislations, but instead are required to incorporate it.¹¹⁰

One group of scholars opined that the U.K.'s withdrawal from the E.U. will imply its withdrawal from the E.E.A. too, because the E.E.A. Agreement applies to the territories to which the E.U.'s treaty apply.¹¹¹ The other group of scholars argue that the U.K.'s termination of the E.U. membership does not affect its membership at the E.E.A.¹¹² until and unless it gives a 12 months' notice under Article 127 of the E.E.A. Agreement¹¹³ as the existence of the U.K. in the E.E.A. is based on its autonomous status, rather than based on its membership with the E.U. .¹¹⁴ Nevertheless, exploring an E.E.A. member would have had many disadvantages for the U.K. in the areas other than the digital trade, some of them being the common reasons behind the Brexit vote.

Seeking data transfer through the E.E.A. mode would mean a transfer of power from the U.K. to a central E.U. agency, and direct application of E.U. law in the U.K. without participation in the enactment of the legislation(s),¹¹⁵ which is an obvious threat to the

¹⁰⁷ See also Lord Owen, *The Legal Way to Exit the EU by 31st October is Through a Transition in the E.E.A.*, BREXIT CENTRAL (Oct. 8, 2019), <https://brexitcentral.com/the-legal-way-to-exit-the-eu-by-31st-october-is-through-a-transition-in-the-e.e.a./>.

¹⁰⁸ See Agreement on the European Economic Area, art. 2(c), art. 10, Jan. 3, 1994, 1994 O.J. (L 001) 3 [hereinafter E.E.A. Agreement].

¹⁰⁹ See *Utenfor Og Innenfor: Norges Avtaler. Med EU (Outside and Inside: Norway's Agreements with the EU)* NOU 64-76 (Ministry of Foreign Affairs, 2012).

¹¹⁰ See John Erik Fossum, *Representation Under Hegemony? On Norway's Relationship to the EU*, in *THE EUROPEAN UNION'S NON-MEMBERS: INDEPENDENCE UNDER HEGEMONY?* 153, 155-56 (Erik O. Eriksen & John Erik Fossum eds., 2015).

¹¹¹ See Dóra Sif Tynes & Elisabeth Lian Haugsdal, *In, Out or In-Between? The U.K. as a Contracting Party to the Agreement on the European Economic Area*, 41 EUR. L.REV. 753, 763 (2016).

¹¹² See Ulrich G. Schroeter & Heinrich Nemeček, *The (Uncertain) Impact of Brexit on the United Kingdom's Membership in the European Economic Area*, 27 EUR. BUS. L. REV. 921, 922 (2016).

¹¹³ See David Allen Green, *Brexit: Can and Should the U.K. Remain in the EEA?*, FIN. TIMES (Aug. 2, 2017), <https://www.ft.com/content/16b50be8-161c-38d3-83b8-14b04faa9580>.

¹¹⁴ See Schroeter & Nemeček, *supra* note 112, at 921.

¹¹⁵ See DESMOND DINAN, *EUROPE RECAST: A HISTORY OF EUROPEAN UNION 19-25* (Red Globe Press 2014) (2004).

sovereignty of the U.K.¹¹⁶ Secondly, the applicability of the burdensome E.U. regulations has cost the UK approximately \$880 million,¹¹⁷ and similarly, the cost of joining the E.E.A. would also be high. Therefore, joining (remaining in) the E.E.A. would not be in the best interests of a post-Brexit Britain¹¹⁸ merely because it may continue to benefit the U.K. in cases of data privacy due to G.D.P.R. .

3.2 MODELS THAT ARE BEING EXPLORED

3.2.1 U.K.-E.U. C.F.T.A.: A BILATERAL APPROACH TO (DIGITAL) TRADE

A draft U.K.-E.U. Comprehensive Free Trade Agreement [hereinafter U.K.-E.U. C.F.T.A.], that came out in May 2020, seems to be the U.K.'s new plan post the transition period. While parties are currently negotiating on the same; they continue to have major differences on matters concerning level playing field provisions, competition, and state aid, and the overall governance structure of the agreement.¹¹⁹ This approach of the U.K. is a tad bit similar to the Switzerland's approach in establishing its relationship with the E.U. where they closely integrated, and continue to cooperate on bilateral levels on a sectoral basis,¹²⁰ having concluded multiple agreements.¹²¹ However, U.K. C.F.T.A.'s approach is essentially for seeking greater autonomy for the U.K.,¹²² so that the U.K. will retain its sovereign right; and "whatever happens", the U.K. will not negotiate on any matters in which it loses its control over its laws and politics.¹²³ In furtherance of the same, the U.K. has also maintained its position on not being bound by the decision(s) of

¹¹⁶ See generally Ralph C. Bryant, *Brexit: Make Hard Choices but Don't Confuse Sovereignty with Autonomy*, BROOKINGS (Dec. 21, 2018), <https://www.brookings.edu/blog/up-front/2018/12/21/brexit-make-hard-choices-but-dont-confuse-sovereignty-with-autonomy/>.

¹¹⁷ See Timothy B. Lee, *Brexit: the 7 most important arguments for Britain to leave the EU*, VOX (Jun. 25, 2016), <https://www.vox.com/2016/6/22/11992106/brexit-arguments>.

¹¹⁸ See MJ Pérez Crespo, *After Brexit... The Best of Both Worlds? Rebutting the Norwegian and Swiss Models as Long-Term Options for the U.K.* 36(1) YEARBOOK OF EUROPEAN LAW 94, 108 (2017).

¹¹⁹ *What does the U.K.'s draft EU FTA text tell us about the negotiations?*, WIREDGOV (May 21, 2020), <https://www.wiredgov.net/wg/news.nsf/articles/What+does+the+UKs+draft+EU+FTA+text+tell+us+about+the+negotiations+21052020112500>.

¹²⁰ *Id.* at 11.

¹²¹ See *e.g.*, Bilateral Agreement I EU- Swis, Jun. 21, 1999, 2002 O.J. (L 114). The areas covered by the Bilateral Agreement I were (i) free movement of persons; (ii) overland transport; (iii) air transport; (iv) public procurement markets; (v) participation in EU research program; (vi) agriculture; (vii) technical barriers to trade; Bilateral Agreement II EU- Swis, Oct. 26, 2004, 2004 O.J. (L 114). The areas covered by this Bilateral Agreement II were (i) taxation of savings; (ii) fight against fraud; (iii) Schengen/Dublin; (iv) processed agricultural products; (v) statistics; (vi) pension; (vii) environment; (viii) audio-visual industry; (ix) education and occupational training.

¹²² See MARIUS VAHL & NINA GROLIMUND, *INTEGRATION WITHOUT MEMBERSHIP: SWITZERLAND'S BILATERAL AGREEMENTS WITH THE EUROPEAN UNION* 3 (2006).

¹²³ See HM Government, *The Future Relationship with the EU-The UK's Approach to Negotiations*, CP211, ¶ 5 (Feb. 2020) [hereinafter Negotiations Document].

the European Court of Justice [hereinafter E.C.J.].¹²⁴ Taking into consideration the bilateral nature of the agreement, the U.K. remains to be at the same bargaining position as that of the E.U. .¹²⁵

This model may pose certain structural challenges like (i) negotiating such a big agreement with multiple arrangements on different subjects will be a lengthy and complex process, but would invariably allow the U.K. to retain its sovereignty; (ii) the U.K. would be less bothered by implementation of all the E.U. laws, and would only have to comply with those laws which would be agreed upon in the bilateral agreement between them; and (iii) the U.K. would not be bound by an interpretation of the E.C.J. in cases of dispute between its bilateral agreement with the E.U., as it is in the case of Switzerland.

In context of the data transfer, the U.K. has declared that data protection will not be a part of U.K.-E.U. C.F.T.A. as the U.K. considers it separate from a more comprehensive future relationship,¹²⁶ yet it is crucial to note that the U.K.-E.U. C.F.T.A. does provide a separate chapter on digital trade.¹²⁷ Also, the draft U.K.-E.U. C.F.T.A. specifically talks about emerging technology which is inextricably related to the G.D.P.R. as the G.D.P.R. has been “designed to cover new technologies”.¹²⁸

The importance of digital trade and adequacy decision has been noted by the European Commission, especially in the context of Brexit, by stating that Brexit is “... an enabling factor for trade, including digital trade, and an essential prerequisite for a close and ambitious cooperation in the area of law enforcement and security”.¹²⁹ Noting the importance of data protection in digital trade,¹³⁰ which has also been considered by the E.U., the authors feel that data adequacy should be a part of the U.K.-E.U. C.F.T.A., as the exclusion of data privacy laws would have implications on areas such as banking and financial services, e-commerce, etc. which are part of the U.K.-E.U. C.F.T.A..¹³¹ However, Europe’s data strategy clearly stipulates that the *only* way for data protection,

¹²⁴ *Id.* ¶ 6.

¹²⁵ See RENÉ SCHWOK & CENNI NAJY, UK RETURNING TO EFTA: DIVORCE AT 40 AND GOING BACK TO MOM AND DAD? ¶ 40 (2012).

¹²⁶ See Negotiations Document, *supra* note 123, ¶ 60.

¹²⁷ See generally Draft UK-EU Comprehensive Free Trade Agreement, March 18, 2020, UKTF (2020) 14 [hereinafter C.F.T.A.].

¹²⁸ See Draft UK-EU Comprehensive Free Trade Agreement, March 18, 2020, UKTF (2020) 14 [hereinafter C.F.T.A.]; *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation*, COM (2020) 264 final (Jun. 24, 2020) [hereinafter E.U.’s Approach].

¹²⁹ E.U.’s Approach, *supra* note 128, at 11.

¹³⁰ See generally Aaditya Mattoo & Joshua P. Meltzer, *Resolving the conflict between Privacy and Digital Trade*, Vox (May 23, 2018), <https://voxeu.org/article/resolving-conflict-between-privacy-and-digital-trade>.

¹³¹ See For instance, Article 18.13 specifically talks about personal information protection and hence exclusion of adequacy status issue from the EU-UK FTA would cause additional burden to the UK.

irrespective of its importance in digital trade, is adequacy decision or other existing mechanisms in the G.D.P.R., rather than subjecting data protection under the free trade agreement,¹³² and the process for obtaining the adequacy decision has been initiated by the U.K.,¹³³ however the E.U. has casted doubts in this regard.¹³⁴ It is crucial to note that while adequacy decision are yet to be finalised, data transfer between the U.K. and the E.U. is currently taking place under the Trade and Cooperation Agreement signed on 24 December 2020, which has provided a six-month bridging period to allow the continued flow of data.

3.2.2 FULL ADEQUACY FINDING UNDER THE G.D.P.R.: A HARD NUT TO CRACK

The transboundary transfer of data from one W.T.O. Member to another is analogous to the free flow of trade in (electronic) services. In situations involving the transfer of data from the E.U. to a third country, it is essential to consider whether that third country is a “secured” country (i.e. the country that has been afforded adequacy status) or an “unsecured” country under the G.D.P.R.¹³⁵ Article 45 of the G.D.P.R.¹³⁶ provides that secured countries are the ones where the national laws provide an essentially equivalent level of protection to the data as that in the E.U., and have in that way successfully achieved adequacy decision. The E.C.J. gave a landmark decision in the *Schrems v Data Protection Commissioner* [hereinafter *Schrems I*] case concerning Article 25 of the E.U. Data Protection Directive, which is broader than Article 45 of the G.D.P.R., wherein the Court held that there must be an evaluation of the third country’s data protection laws and its application.¹³⁷ In other words, *Schrems I* case advocated the essential equivalency test. In addition to these requirements, Article 45 should also evaluate whether third country’s laws on national security, human rights, etc. are similar to the E.U. laws,¹³⁸ and while determining such adequacy of the data protection law, the European Commission must take into account the existence and effective functioning of one or more independent

¹³² See European Strategy for Data, *supra* note 103.

¹³³ See, e.g. *What does Adequacy mean?*, ICO <https://ico.org.uk/for-organisations/data-protection-at-the-end-of-the-transition-period/what-does-adequacy-mean>.

¹³⁴ See Letter from Andrea Jelinek, Chair of the European Data Protection Board (EDPB) to Member States, (Jun. 15, 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.

¹³⁵ See G.D.P.R., *Third Countries*, INTERSOFT CONSULTING, <https://gdpr-info.eu/issues/third-countries>.

¹³⁶ See G.D.P.R., *supra* note 13, Art. 45. Article 45 of the G.D.P.R. imposes an obligation on the member states to ensure that the data can be transferred to a country outside the EU only if that country ensures an adequate level of protection.

¹³⁷ See Case C-362/14, *Max Schrems v. Data Protection Commissioner*, ECLI:EU:C:2015:650, ¶ 75 (Oct. 6, 2015).

¹³⁸ See, e.g., PRASHANT MALI, *GDPR ARTICLES WITH COMMENTARY & EU CASE LAWS* 109 (2019).

supervisory authorities, the rule of law, relevant legislation, respect for human rights and fundamental freedoms, and the international commitments the third country or international organisation has entered into.¹³⁹

Meanwhile, unsecured countries are considered as the ones which have not achieved an ‘adequacy decision’, and in the absence of that adequacy decision, the international transfer of data can take place through B.C.R.s,¹⁴⁰ S.C.C.s,¹⁴¹ or as per the procedures under Article 46 or Article 49 of the G.D.P.R. . The data transfer that happens through S.C.C. between private parties can also ensure data protection if assurances are made to comply with the G.D.P.R.’s approved Code of Conduct.¹⁴² These model Code of Conduct must be approved¹⁴³ and monitored¹⁴⁴ by a supervisory authority under the G.D.P.R.; and it must be noted that these corporate rules or standard data protection clauses are available only for arrangements among the parties without any direct intervention by the State as a regulatory authority, while an adequacy status is given to a State without the involvement of private parties. The comparison between the B.C.R.s and S.C.C.s suggests that B.C.R.s might be overall more effective than the S.C.C.s as the former can be tailored as per the requirements of a corporation which will differ with the kind of business operations being carried out. B.C.R.s can be comparatively costly as they require an approval from a competent data protection authority [hereinafter D.P.A.], and then the decision of the D.P.A. is sent to the European Data Protection Board [hereinafter E.D.P.B.], and it is only after the opinion of E.D.P.B., the D.P.A. approves the concerned B.C.R.s. However, in the case of a S.C.C., *firstly*, the S.C.C. is approved by the Commission which can be used by the parties without any approval from any authority - making it less costly than the B.C.R.s; however, in case of an ad-hoc S.C.C., there is a similar approval mechanism as in the case of B.C.R.s.¹⁴⁵ Also, the scope of B.C.R.s is limited to only intra-corporate transfer as opposed to the S.C.C.s, which have a wider scope. It is also observed that there exist possibilities when compliance with “adequacy decision” is not needed in certain circumstances, viz. (i) if the data subjects have consented to it; (ii) the transfer pertains to a legal or a contractual claim; or (iii) in the public interest.¹⁴⁶

¹³⁹ See G.D.P.R., *supra* note 13, Art. 45.

¹⁴⁰ Binding Corporate Rules are the rules dealing with international data transfer within intra-organizations located in different countries. See generally *International personal data transfers: binding corporate rules (BCRs) under the GDPR*, I-Scoop, <https://www.i-scoop.eu/gdpr/binding-corporate-rules-bcrs-gdpr>.

¹⁴¹ See generally G.D.P.R., *supra* note 13, Art. 46.

¹⁴² See *id.* Art. 40; see also *GDPR and approved codes of conduct – demonstrating compliance*, I-Scoop, <https://www.i-scoop.eu/gdpr/gdpr-codes-conduct>.

¹⁴³ G.D.P.R., *supra* note 13, Art. 55.

¹⁴⁴ *Id.* Art. 41.

¹⁴⁵ See, e.g., Patrick Van Eecke et al., *EU: Binding Corporate Rules are Generating Greater Interest*, DLA PIPER (Oct. 16, 2019), <https://blogs.dlapiper.com/privacymatters/eu-binding-corporate-rules-are-generating-greater-interest>.

¹⁴⁶ G.D.P.R., *supra* note 13, Art. 49.

The authors note that the option of moving forward with an “adequacy decision” approach seems to be the easiest amongst all the others discussed above,¹⁴⁷ and is being pursued by the U.K. to retain its sovereignty. It has also been argued that seeking an “adequacy decision” in the case of the U.K. is merely a formal requirement as U.K. was already a member of the E.U.,¹⁴⁸ and they would be better off with a fully-fledged comprehensive E.U.-U.K. data agreement.¹⁴⁹ The advantage of this bilateral data only arrangement approach would be that it cannot be revoked by the European Commission or invalidated by the E.C.J. as would be in the case of an “adequacy decision”,¹⁵⁰ and it makes this bilateral data only arrangement more beneficial since we understand that a sudden revocation or invalidation of an adequacy decision would freeze the E.U. – U.K. digital trade, eventually hampering the U.K.’s economy.

Furthermore, the U.K. Information Commission Office [hereinafter I.C.O.]¹⁵¹ has already implemented the G.D.P.R., with the promulgation of the Data Protection Act 2018.¹⁵² Nevertheless, despite the compatibility that exists between the U.K. Data Protection Act and E.U.’s G.D.P.R., there exists a doubt on specific grounds as to whether the UK will be able to achieve its adequacy decision without any problems. So, in *Secretary of State for the Home Department v Watson*, the E.C.J. held that the collection of data and its retention by the security services in all cases without having any exception, even for the collection and/or retention of data for combating crime,¹⁵³ violates the fundamental right to privacy of a person.¹⁵⁴ A possible hindrance in accomplishing the essential equivalence test by the U.K. exists concerning their “Investigatory Powers Act, 2016”. The High Court and the European Court of Human Rights have held that the powers granted to the U.K.’s security forces and intelligence services to intercept, hold, and examine any data would end up violating the privacy rights of individuals, and hence put the likelihood of getting an adequacy decision by the E.U. into question.¹⁵⁵

¹⁴⁷ See Warwick Ashford, *UK surveillance laws a potential ‘sticking point’ post-Brexit*, COMPUTERWEEKLY.COM (Apr. 19, 2018), <https://www.computerweekly.com/news/252439434/UK-surveillance-laws-a-potential-sticking-point-post-Brexit>.

¹⁴⁸ See Department of Exiting the EU, *Framework for the UK-EU Partnership Data Protection* (2018), 16.

¹⁴⁹ See HM Government, *Technical Note: Benefits of a new data protection agreement* (2018), 1; See also Ashford, *supra* note 147.

¹⁵⁰ See OLIVER PATEL & NATHAN LEA, *EU-UK DATA FLOWS, BREXIT AND NO-DEAL: ADEQUACY OR DISARRAY?* 9 (2019). see also G.D.P.R., *supra* note 13, Recital 107, Art. 45(5).

¹⁵¹ The UK’s independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. See ICO. <https://ico.org.uk/>.

¹⁵² See generally *Guide to the General Data Protection Regulation (GDPR)*, ICO, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr>

¹⁵³ See *Secretary of the State for the Home Department v. Watson: Case Analysis*, GLOBALFREEDOMOFEXPRESSION.COLUMBIA.EDU, <https://globalfreedomofexpression.columbia.edu/cases/secretary-state-home-department-v-watson>.

¹⁵⁴ See C-698/15, *Secretary of State for the Home Department v. Watson*, 2016 ECLI: EU:C:2016:970, ¶ 103 (Dec.21, 2016).

¹⁵⁵ William R.M. Long & Francesca Blythe, *Data Protection and Post-Brexit Issues*, INT’L J. DATA PROT. OFFICER, PRIV. OFFICER & PRIV. COUNS., no. 2, 2018, at 8.

Similarly, the “Five Eyes Alliance”, an intelligence alliance consisting of the U.S., Canada, Australia, New Zealand and the U.K., dealing with cooperation on signal intelligence sharing, proposed that the law enforcement agencies should have access to encrypted data to make them stronger.¹⁵⁶ The concerns of the European Commission herein also remain the same, i.e. this exercise might lead to an unchecked transboundary transfer of personal data of the E.U. citizens under the garb of national security.¹⁵⁷ Therefore, such issues will act as a major hindrance in the achievement of an adequacy status, even though the laws are entirely consistent with G.D.P.R. .

CONCLUSION

While there are several provisions in G.A.T.S which are helpful in the regulation of data through various mediums, it is well documented that none of those provisions is conducive for protection of the same data, even when the transfer of such data is happening through electronic services.¹⁵⁸ The rationale behind the non-existence of such standards can be attributed to the fact that the protection of data deals with issues directly linked to privacy, and the right to privacy is more of a fundamental and constitutional right raising questions revolving around the sovereignty of a state. Therefore, it is necessary to look for solutions that can act as a bridge between the need for regulation of data under the W.T.O.-law and reasonable application of privacy laws for the protection of this data.¹⁵⁹

Weber suggested that one of the most viable justifications for a W.T.O. member’s need for applying stringent data protection laws can be read in reference to the general exception under Article XIV (lit. c) of the G.A.T.S.¹⁶⁰ Nonetheless, the level of the protection of data can always be increased in bilateral or regional trade agreements by having specific chapters looking into the concerns of members for the regulation and protection of their data.¹⁶¹ However, as far as protection of data under G.D.P.R. is concerned, it has been argued by several scholars that if the G.D.P.R. is challenged before a W.T.O. panel, the E.U. would have to heavily rely on the exceptions under G.A.T.S,

¹⁵⁶ See “Five Eyes” security alliance calls for access to encrypted material, REUTERS (Jul. 30, 2019), <https://www.reuters.com/article/us-security-fiveeyes-britain-idUSKCN1UP199>.

¹⁵⁷ See David Meyer, *Post-Brexit U.K.’s Surveillance Practices Could Spell Big Problems for Business*, FORTUNE (Feb. 7, 2020), <https://fortune.com/2020/02/07/post-brexit-uk-data-protection-adequacy/>.

¹⁵⁸ See Weber, *supra* note 5, at 25.

¹⁵⁹ *Id.*

¹⁶⁰ *Id.*

¹⁶¹ *Id.*

creating a difficult situation for them considering the fact that only in one case the W.T.O. D.S.B. has allowed the innovation of such exception.¹⁶²

Now, after the transition period, the Commission has not given its adequacy decision as of now, and there are possibilities that the data protection regimes of the U.K. and E.U. would remain consistent;¹⁶³ nonetheless, the authors are of the opinion that all the legal entities must start preparing themselves with an alternative method, having included such B.C.R.s or S.C.C.s, which may help them deal with the international transfer of data; otherwise, the entire economic activity surrounding the banking, finance, and e-commerce sectors will be halted. Furthermore, post-transition period, the authority of the Information Commission Office as the D.P.A. will cease under the G.D.P.R. . Hence, business organizations need to approach the E.U. Data Protection Authority for any kind of approval, which will put more burden on them.

Lastly, the authors also are of the opinion that the option of the U.K.-E.U. C.F.T.A. with proper incorporation of data privacy arrangements under it would be the best option for the U.K. moving forward, since this approach allows the U.K. to retain its autonomy and sovereignty, whilst also managing to get an adequate level of protection in the eyes of G.D.P.R. for areas/sectors where the lack of an adequacy decision, immediately after the end of transition period, might have significant implications. Therefore, it seems fit to say that whatever path the U.K. may choose for its relationship with the E.U. pertaining to the concerns surrounding the international transfer of data, it must start finalising the guidelines around the same, as otherwise the economic activity of the business organisations will be endangered due to the hindrances in the transfer of data.

¹⁶² See Appellate Body Report, *European Communities - Measures Affecting Asbestos and Asbestos-Containing Products*, ¶3243, WTO Doc. WT/DS135/AB/R (adopted 5 April 2001).

¹⁶³ See generally Wimmer & Jones, *supra* note 12, at 1561.