BRILL
NIJHOFF

GLOBAL JOURNAL OF COMPARATIVE LAW
13 (2024) 201–226

GJCL
brill.com/gjcl

# The Extraterritoriality of the GDPR and Its Effect on GCC Businesses

*Mohammed Khair Alshaleel* | ORCID: 0000-0002-1974-0979
Senior Lecturer, University of Essex, Essex Law School, Essex, United Kingdom
*mkalsh@essex.ac.uk*

Received 7 February 2024 | Accepted 22 May 2024 | Published online 7 August 2024

## Abstract

This article considers the extraterritoriality of the General Data Protection Regulation (GDPR) and its effect on Gulf Cooperation Council (GCC) businesses. Given the robust economic ties to the European Union (EU), many GCC businesses fall under the scope of the GDPR. This article argues that the territorial gateways through which the GDPR applies are much wider than might be thought and so may capture many GCC businesses, and that while the personal data protection laws in the GCC countries have been influenced to varying degrees by the GDPR, there are significant disparities, especially regarding their approach to data protection. This suggests that the level of data protection in the GCC countries is not equivalent to that offered by the GDPR. The article is divided into six sections, covering the EU's data protection laws, framework evolution, GDPR's impact on GCC businesses, and GCC's data protection framework.

## Keywords

GDPR – extraterritoriality – GCC businesses – fundamental right – protection

## 1 Introduction

Data has become the lifeblood of our society and an increasingly valuable asset. Given the developments in the data-driven economy, data privacy and the

Published with license by Koninklijke Brill BV | DOI:10.1163/2211906X-13020004
 | ISSN: 2211-906X (online)

regulation of data protection have become a primary concern.[1] In response to this concern, over the last two decades, legislators around the world have been working to establish and implement laws and regulations specifically designed to protect personal data from being misused or abused. In the European Union (EU), the General Data Protection Regulation (GDPR), which replaced the 1995 Data Protection Directive (DPD), was adopted on the 14th of April 2016 and became officially enforceable on 25 May 2018. In addition to facilitating the free movement of personal data between the EU's various Member States (MS s), the GDPR creates a framework of fundamental rights protection, based on the right to data protection in Article 8 of the Charter of Fundamental Rights.[2] The GDPR has changed the global data protection landscape by providing a stricter paradigm for protecting personal data than had previously existed. It also increased global awareness of the significance of data protection, with many regulators seeking to introduce or improve data protection regulations. In 2020, the EU Commission published an evaluation of the GDPR, emphasising that the GDPR has quickly become a significant benchmark on the global stage and has spurred numerous countries worldwide to contemplate implementing contemporary privacy regulations.[3]

To protect all data subjects on the EU territory, the GDPR claims a broad extraterritorial jurisdiction, regardless of their nationalities.[4] The extraterritorial scope of the GDPR indicates that it is applicable even outside of the borders of the EU. In contrast to the DPD, the GDPR has considerably extended grounds for the applicability to any business or organisation worldwide that collects, processes, controls or uses the information of data subject on the EU territory, regardless of geographical location.[5] The GDPR's exterritorial scope is determined by Article 3. There are two main criteria of the GDPR applicability to the data processing activities carried out by a non-EU controller or processor: the establishment principle (Article 3(1)) and the targeting principle (Article 3(2)). They are, as will be discussed later,

1 Christopher Kuner, *European Data Protection Law Corporate Compliance and Regulation* (2nd edn, Oxford: Oxford University Press, 2007) 20.

2 Charter of Fundamental Rights of the European Union 2000, art 8.

3 See, European Commission.2020. '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. European Commission' 24 June. Retrieved 17 September 2022 https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vl9thg3be9uy.

4 Dimosthenis Lentzis, 'Revisiting the Basics of EU Data Protection Law: On the Material and Territorial Scope of the GDPR' in Maria Tzanou (ed), *Personal Data Protection and Legal Developments in the European Union* (Information Science Reference 2020) 27.

5 Herke Kranenborg, 'Article 8 – Protection of Personal Data' in Steve Peers and others (ed), The EU Charter of Fundamental Rights: A Commentary (Nomos Verlag 2022) 257.

based on the direct links with the EU either through having an establishment or targeting individuals in its territory. This paper will show that the GDPR extraterritorial jurisdictional claims are reasonable to provide effective protection for data subjects.

Given the robust economic ties to the EU, many data controllers and processors in the Gulf Cooperation Council's countries (GCC) fall under the scope of the GDPR when they process EU residents' personal data. The GCC is a regional group, including Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates (UAE). Diplomatic and economic relations between Europe and GCC predate the formation of the EU and can be traced to the inaugural European Council-GCC joint ministerial meeting in 1985.[6] After the creation of the EU, relations between the EU and the GCC were formalised through the 1988 Cooperation Agreement, which established regular dialogues on cooperation between both parties on different issues, including trade and investment, macroeconomic matters, the environment, energy, and research.[7] Since that period, these relations have grown institutionally and become multi-faceted. The EU and the GCC total trade in goods in 2020 amounted to 97.1 billion EUR.[8] The EU is the 2nd biggest trade partner of the GCC, representing 12.3 percent of the GCC's total trade in goods with the world in 2020, and was the 4th biggest export partner of the GCC as 6.9 percent of the GCC's exports went to the EU.[9]

Although the GDPR came into application in 2018, many businesses in the GCC still do not comply with it. This is mainly due to the ambiguity around the extraterritorial scope of the GDPR. As a result, they may largely risk potential law breaches in case they do not follow the GDPR's data protection requirements for different reasons. Whether GCC businesses are subject to the GDPR depends on various factors which will be examined in this article. In undertaking this research task, the focus is placed on the extraterritoriality of the GDPR and its impact on GCC businesses. This article argues that the territorial gateways through which the GDPR applies are much wider than might be thought and so may capture many GCC businesses which might not have thought they are

6 European Commission. 1990. 'EC/Gulf Cooperation Council Joint Council'16 September. Retrieved 17 September 2022 https://ec.europa.eu/commission/presscorner/detail/en/MEMO_90_12.

7 The agreement can be found here: retrieved 17 September 2022 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:1989:054:FULL&from=EN.

8 European Commission. 2021. 'EU trade relations with Gulf region. Facts, figures and latest developments'. 31 March. Retrieved 17 September 2022 https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/gulf-region_en.

9 Ibid.

under its scope. It sheds light on significant case law to support this argument by eliminating Article 3 ambiguity. It also argues that while the personal data protection laws in the GCC countries have been influenced to varying degrees by the GDPR, there are significant disparities, especially regarding their approach to data protection. The extensive global reach of the GDPR is mainly related to its foundation: the notion of fundamental rights and promoting human rights, particularly the right to privacy. This article will show that categorising the right to data protection as a fundamental right could appear to constitute a decisive reinforcement of the level of protection effectively provided to individuals throughout the EU. Contrary to the GDPR, the main priority of data protection regulations in the GCC countries is protecting individuals from malicious actors and activities. This suggests that the level of data protection in the GCC countries is not equivalent to that offered by the GDPR. Thus, even when GGC businesses comply with their national data protection laws and regulations, they might still need to adhere to the GDPR requirements and obligations if they are under its scope. It is significant to mention that the article will concisely discuss the question of how the EU can unilaterally extend its authority over GCC businesses and organisations and whether the EU actually have the necessary means to ensure that the GDPR obligations are satisfied by them.

The remainder of article is divided into five sections. Section 2 briefly discusses data protection as a fundamental right under EU law, highlighting the difference between the right to privacy and the right to data protection. Section 3 examines the defining features of the GDPR and its principles, focusing on the rationale for its adoption. Section 4 analyses the extraterritorial applicability of the GDPR to GCC businesses, with a focus on the "*establishment*" and "*targeting*" criteria under Article 3 of the GDPR. In doing so, it sheds light on the practical interpretation of Article 3 by Courts. Section 5 considers the GCC data protection framework. It highlights the recent wave of data protection regulations in the GCC countries, the reasons for this wave, and the difference between the GPDR's approach to data protection and those regulations. Section 6 is a conclusion.

## 2 Data Protection as a Fundamental Right

In order to understand the extraterritoriality of the GDPR and its effect on GCC businesses, it is necessary to understand the rationale and significance of data protection. The need for a right to protection of personal data considerably grew with the emergence of communication technology in the second half

of the twentieth century.[10] To illustrate, the increasing use of computing applications was recognised as posing a threat to individuals' rights and freedoms, especially their right to privacy.[11] Computers also made it easier and cheaper to aggregate and store personal data. Therefore, it was expected that, over time, more and more personal data would be stored and kept for long periods of time.[12] This personal data could in turn be made available to a growing number of parties, who could use it for different purposes. Thus, protecting personal data was the main concern.

It is important to point out that data protection has always been connected to the concept of privacy in such a way that it is difficult to evaluate its nature and purpose without falling back to the principles and rules of privacy.[13] The notion of the right to privacy is considered broader than the right to data protection because it covers all issues related to one's private life, including the protection of the personal data of an individual if this personal data falls within the sphere of one's private life.[14] This means that data protection is one of the aspects of the right to privacy. In the EU, the right to data protection is a fundamental right recognised by Article 8 of the Charter of Fundamental Rights of the EU and the constitutional laws of many MSs, as well as the case law of the European Court of Justice (ECJ). Article 8 of the Charter of Fundamental Rights states that '*Everyone has the right to the protection of personal data concerning him or her*' and '*Such data must be processed fairly for specific purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law*'.[15] It separates the right to data protection from the right to privacy and coins it a fundamental right as well. Article 7 of the Charter of Fundamental Rights guarantees the right to privacy: '*Everyone has the right to respect for his or her private and family life, home and communications*'.[16] Article 16 (1) of the Treaty on the Functioning

10 Stefano Rodot`a, 'Data Protection as a Fundamental Right' in Cécile de Terwangne and others (eds), *Reinventing Data Protection?* (Springer, 2009) 78.

11 Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Berlin: Springer International Publishing, 2014) 156.

12 Andrew Puddephatt, 'ITCs, Privacy and the (Criminal) misuse of data' in M. R. McGuire and Thomas J. Holt (ed), *The Routledge Handbook of Technology, Crime and Justice* (Oxon: Taylor & Francis, 2017) 179.

13 See, Peter Blume, 'Data Protection and Privacy – Basic Concepts in a Changing World', Scandinavian Studies 56 (2010) 151 at 154.

14 See, Maria Tzanou, 'Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right', International Data Privacy Law 3 (2013) 88 at 93.

15 Charter of Fundamental Rights of the European Union 2000, art 8.

16 Ibid, art 7.

of the European Union (TFEU) also provides that everyone has the right to the protection of personal data concerning him or her.[17] Further, the GDPR expressly makes the distinction between the right to data protection and the right to privacy in recital 4 where it is stated that the GDPR *'respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data'*.[18] This suggests that categorising the right to data protection as a fundamental right could appear to constitute a decisive reinforcement of the level of protection effectively provided to individuals throughout the EU.

The foregoing discussion raises a significant question about the meaning and interpretation of the term "*fundamental right*" under EU law. There are different positions in this debate. While some scholars view fundamental rights primarily as constitutional rights, others argue that the term fundamental rights should be seen as equivalent to human rights.[19] In her extensive research on this point, Gloria Fuster pointed out that within the EU framework, the term "*fundamental rights*" typically pertains to the rights safeguarded by EU legislation, while "*human rights*" typically refers to rights acknowledged in international law. EU law places strong emphasis on the phrase "*fundamental freedoms*" which traditionally encompasses the essential liberties associated with the EU single market, including the free movement of goods, individuals, services, and capital. EU law has never supplied a comprehensive definition of fundamental rights. Their present recognition owes a great deal to their identification and establishment by the European Court of Justice throughout its history.[20]

This suggests that an interpretation might be derived from the different EU and international legal documents and scholarly literature. Given that the right to data protection is a fundamental right in the EU, it is inalienable. This means that the right to data protection cannot be taken away, transferred or forfeited although personal data itself can be owned and considered as a commodity.[21]

---

17 Treaty on the Functioning of the European Union 1957, art 16(1).

18 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/EC (General Data Protection Regulation) [2016] OJL 119/1 (GDPR).

19 Tzanou (n 14) at 92.

20 Fuster (n 11) 166.

21 Bart Custersa and Gianclaudio Malgieri, 'Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data', International Data Privacy Law 45 (2022) 1 at 8.

## 3 General Data Protection Regulation: Evolution Not Revolution

As a leading and far-reaching legislation, the GDPR is an evolution, not a revolution because it builds on the notions and principles of data protection provided by the European Data Protection Directive (DPD) of 1995.[22] The GDPR, which entered into force in the EU on 26 May 2016 and into application on 25 May 2018, was adopted to replace the outdated EU DPD. Taking the form of European regulation, the GDPR is binding in its entirety and directly applicable in all MS s. This suggests that the previous issues regarding the harmonisation of EU data protection law will not exist anymore.[23] It is the most forward-thinking and extensive legal provision for personal data protection. The GDPR seeks to create a harmonised data protection law across the EU and is designed to give individuals more control over how their data is collected, stored, processed and used by organisations.[24] As will be discussed later, the GDPR imposes obligations onto organisations anywhere, so long as they target or collect data related to people in the EU and fines of up to 4 percent of worldwide turnover or 20 million EUR (whichever is greater) will be levied on businesses breaching them.[25]

The adoption of the GDPR to replace the outdated DPD was necessary to bring data protection into the 21st century by providing data subjects within the EU with the ultimate protection for their data in a world where the internet is borderless. Adopted in the mid-90s, the DPD was designed to regulate the continuously developing relations in the digital world and to achieve a minimum level of data protection within the EU.[26] However, it failed to face upcoming challenges of the developing technological world which at the time of creating the Directive did not even exist such as blockchain, machine-learning software and Artificial Intelligence (AI). Recent decades have witnessed some personal data breaches and scandals that gave alarming signals on existing data security frameworks and urged the EU legislature to undertake data protection reform such as Edward Snowden's leaks about the spying practices of the National Security Agency (NSA) and the Facebook-Cambridge Analytica scandal,

22 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] OJL 281/31.

23 IBM Security. 2018. 'Blockchain and GDPR: How blockchain could address five areas associated with GDPR compliance' White paper. 10 March. Retrieved 21 August 2022 https://iapp.org/resources/article/blockchain-and-gdpr/.

24 Fuster (n 11) 117.

25 GDPR, art 83.

26 Kuner (n 1) 20.

in which the data of up to 87 million Facebook users were inappropriately collected.[27]

The GDPR rules can generally be divided into protection-oriented rules that bind entities which use data for their commercial purposes, and control-granting provisions that aim at granting specific rights to data subjects who are the ultimate source of personal data. As mentioned earlier, one of the main objectives of the GDPR is to give back control to European citizens over their data. Therefore, the regulation is driven by fundamental principles from which individual requirements are drawn that have to be implemented in entities that process personal data from EU citizens. These principles were formed before the GDPR was written and courts can use them to interpret the law.[28] These principles are also important to keep the GDPR contemporary in a time of fast-evolving information technology. They are 6 in total and can be found in article 5 of the GDPR:

### 3.1 *Lawfulness, Fairness, and Transparency*

The GDPR states that personal data should be '*processed lawfully, fairly and in a transparent manner*'.[29] As can be noted, this principle consists of three elements. While these elements overlap, they must be satisfied. For the processing of personal data to be lawful, specific grounds for the processing should be identified.[30] This is called a "lawful basis" for processing. Fairness means personal data must only be used in ways that data subjects would reasonably expect and not used in ways that have unjustified adverse effects on them.[31] Transparency is fundamentally linked to fairness. Data controllers have to be clear, open and honest with data subjects from the start about how and why they use their personal data.[32]

### 3.2 *Purpose Limitation*

Personal data must be collected for specified, express and legitimate purposes and not further processed in a way that is incompatible with those purposes.[33]

27 Agustín Rossi, 'How the Snowden Revelations Saved the EU General Data Protection Regulation', The International Spectator 53 (2018) 95 at101.

28 Paul De Hert and others, 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services', Computer Law & Security Review 34 (2018) 193 at 198.

29 GDPR, art 5.1 (a).

30 Ibid, art 6.

31 Salvatore Sapienza, *Big Data, Algorithms and Food Safety: A Legal and Ethical Approach to Data Ownership and Data Governance* (Cham: Springer International Publishing, 2022) 138.

32 GDPR, Recital 39.

33 Ibid, art 5(1)(b).

Specifying the purposes from the outset helps achieve the accountability of data controllers. This principle is directly linked to the lawfulness, fairness and transparency principle because being clear about why personal data are processed will help to ensure that processing is fair, lawful, and transparent.[34]

### 3.3 *Data Minimisation*

Personal data must be limited and relevant to what is necessary relating to the purposes for which they are processed.[35] This implies that the use of excess data is prohibited. Data processors should not process personal data if it is insufficient for its intended purpose.

### 3.4 *Accuracy*

This principle aims at protecting data subjects from wrong decisions made based on profiling and has the potential to reduce the risk of identity theft which usually occurs with outdated data.[36] Therefore, data controllers and processors must take reasonable steps to ensure the accuracy of any personal data.[37] For instance, if an individual moves house from Liverpool to Birmingham a record saying that they currently live in Liverpool will obviously be inaccurate.

### 3.5 *Storage Limitation*

Once the purpose of the data collection is satisfied or not valid any longer, the data must be removed from the servers.[38] This principle is linked to the data minimisation and accuracy principles. To illustrate, erasing personal data when no longer needed will reduce the risk that it becomes excessive, irrelevant, out of date or inaccurate.[39]

### 3.6 *Integrity and Confidentiality* (*Security*)

Data controllers and processors must have proper security in place to prevent the personal data they hold from being deliberately or accidentally compromised.[40] Although the GDPR, in general, is more about privacy and not about cybersecurity, this principle links privacy to cybersecurity by stating

34 Gianclaudio Malgieri, *Vulnerability and Data Protection Law* (Oxford: Oxford University Press, 2023) 126.
35 GDPR, art 5(1)(c).
36 Ibid, art 5(1)(d).
37 Malgieri (n 34) 128.
38 GDPR, art 5(1)(e).
39 Malgieri (n 34) 147.
40 GDPR, art 5(1)(f).

that it is imperative to address the security of personal data '*in a manner that ensures appropriate security*'.[41]

The above principles embody the spirit of the GDPR and as such there are very limited exceptions. Compliance with them is therefore a crucial building block for good data protection practice. These principles are also used to derive a specific set of rights for data subjects and obligations for data controllers, including, for instance, the right to be informed, right of rectification, right to erasure, right to restrict processing, right of access, right to data portability, right to object and right related to automated processing.[42]

## 4 Extraterritorial Applicability of the GDPR to GCC Businesses

While the GDPR is mainly directed to the protection of EU residents data, it has an extraterritorial reach and covers any business or organisation worldwide that collects, controls, processes or uses the data of any EU citizen, regardless of geographical location.[43] This implies that the GDPR, as will be discussed later, affects any business in any sector in the GCC countries that sell goods or provide services to any of the EU MSs, or handles data belonging to EU citizens and residents. It is significant to note that it is difficult to clearly define extraterritoriality. According to the definition presented by the United Nations International Law Commission, extraterritorial jurisdiction means '*an attempt to regulate by means of national legislation, adjudication or enforcement the conduct of persons, property or acts beyond its borders which affect the interests of the state in the absence of such regulation under international law*'.[44] This definition suggests that the differentiation between territorial and extraterritorial claims of jurisdiction can often be blurred.

The territorial scope of the GDPR is dealt with in Article 3 and represents a major evolution of the EU data protection law compared to the rules defined by the DPD. Generally, although the GDPR confirms choices made, by the ECJ in the context of the DPD, it has introduced new elements. To illustrate, unlike Article 4 of the DPD which defined which MS national law is applicable, Article 3 of the GDPR determines the territorial scope of a directly applicable text.[45]

41 Ibid, art 5(1)(f).

42 Ibid, arts 12–22.

43 Soriano v Forensic News LLC and Others [2021] EWHC 56 (QB).

44 United Nations. 2006. 'Report of the International Law Commission' (2006) Fifty-eighth session, Supplement No. 10 (A/61/10). 1 May. Retrieved 29 November 2022 https://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf.

45 Andrew T. Kenyon, *Comparative Defamation and Privacy Law* (Cambridge: Cambridge University Press, 2016) 205.

Further, Article 4 of the DPD made a clear reference to the "*use of equipment*" in the Union's territory as a reason for bringing controllers who were "*not established on Community territory*" within the scope of EU data protection law. However, Article 3 of the GDPR does not make such a reference.[46]

Article 3 of the GDPR reflects the EU legislator's intention to ensure comprehensive protection of the rights of data subjects in the EU against threats emanating from outside the Union. As asserted by the Commission when proposing the GDPR, '*individuals' rights must continue to be ensured when personal data is transferred from the EU/EEA to third countries, and whenever individuals in Member States are targeted and their data is used or analysed by third country service providers*'.[47] However, the extraterritoriality of the GDPR raises significant questions about how the EU can unilaterally extend its authority over non-EU businesses and organisations and whether the EU actually have the necessary means to ensure that the GDPR obligations are satisfied by them. It is significant first to note that extraterritorial claim is not an extraordinary phenomenon and has been carried out by most countries, particularly regarding criminal matters.[48]

Being one of the world's largest economic and political power, the EU have the power to pressure countries, organisations and businesses to adopt the principles of the GDPR. Interestingly, in 2012, Anu Bradford introduced the notion of the "*Brussels Effect*", which explains '*Europe's unilateral power to regulate global markets*'.[49] According to this theory, any political actor able to leverage and combine the five factors of regulatory capacity, inelastic targets, market size, stringent standards, and non-divisibility will be able to set the global regulatory standard for a specific regulatory area.[50] As a result, the EU was able to increasingly establish such standards since the 1990s and therefore has become the '*global regulatory hegemon*'.[51] Most global businesses adopt the EU regulatory requirements for designing their services and products as

46 Ibid, 205.

47 European Commission. 2012. 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century', COM (2012) 9/3. 25 January. Retrieved 12 August 2022 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0009&from=en.

48 See, George T Felkenes, 'Extraterritorial Criminal Jurisdiction: Its Impact on Criminal Justice' Journal of Criminal Justice 21 (1993) 583 at 588.

49 Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (New York: Oxford University Press, 2020) 25.

50 Ibid, 25–27.

51 Ibid, 7.

this allows them to adhere to a single regulatory regime albeit it requires more costly adjustments. Compliance with EU standards allows those services and products to be marketed globally. Bradford's analysis includes the advancement of the GDPR with the extraterritorial effect. Her theory also stresses the crucial role of economic scale and political influence.

Further, while the GDPR came into application in 2018, many businesses in the GCC still do not comply with it. This is mainly due to the ambiguity around the extraterritorial scope of the GDPR. Whether GCC businesses are subject to the GDPR depends on various factors which will be discussed in the following sections.

### 4.1 *Article 3 of the GDPR: Territorial Scope Rules*

As noted above, Article 3 of the GDPR defines the territorial scope of the GDPR. The provision states the following:

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
   a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
   b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
3. *This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.*[52]

Article 3 of the GDPR describes the territorial scope on the basis of two main criteria: the "*establishment*" criterion (Article 3(1)), and the "*targeting*" criterion (Article 3(2)). If one of these two criteria is satisfied, the relevant provisions of the GDPR will apply to the relevant processing of personal data by the controller or processor concerned. Further, Article 3(3) asserts the application of the GDPR to the processing where an MS law applies by virtue of public international law.[53] Importantly, the rules of Article 3 are mandatory and

52 GDPR, art 3.

53 This case will not be discussed in this article.

cannot be limited or suspended under any circumstance.[54] Therefore, any attempt to change them will be regarded as void.

#### 4.1.1 Data Controllers and Processors

Since the roles of the data controller and data processor are central to the GDPR, it is crucial to understand these roles before discussing the establishment and targeting criteria. The GDPR divides the actors, who are processing data, into data controllers and data processors.[55] The data controller, on the one hand, is the party responsible for ensuring that personal data is processed in compliance with the GDPR rules. Article 4 (7) of the GDPR defines a controller as '*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*'.[56] The controller is responsible for determining the purposes of processing activities, who to collect data from, which data will be collected, and so on. The controller is required to implement '*appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with* [*the GDPR*]'.[57] Data processors, on the other hand, are those entities contracted by the controller to carry out specific functions on personal data. According to Article 4(8) of the GDPR, a processor is '*a natural person or legal person, public authority, agency or other body which processes personal data on behalf of the controller*'.[58] Contracts between controllers and processors have a number of specific requirements listed in Article 28 of the GDPR. Given that the definition of processing is broad, which includes the collection and disposal of personal data, the data controller and the data processor, in many cases, will be the same entity.[59]

#### 4.1.2 Evaluation of the Establishment Criterion (Article 3(1) GDPR) and the Relevant Case Law

Article 3(1) of the GDPR provides that the *'Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in*

54 Dan Jerker B Svantesson, 'Article 3 Territorial scope' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford: Oxford University Press, 2020) 82.

55 Kuner (n 1) 69.

56 GDPR, art 4 (7).

57 Ibid, art 24.

58 Ibid, art 4 (8).

59 Antoni Gobeo, Connor Fowler and William J. Buchanan, *GDPR and Cyber Security for Business Information Systems* (Gistrup: River Publishers, 2022) 89.

*the Union or not*'.[60] At first glance, the nature of this Article appears to be purely territorial: the GDPR is applicable when a controller or a processor established in the EU engages in data processing activities. However, it does not require the processing activities to be taken place within the EU. This means that the actual place of processing activities does not affect the applicability of the GDPR, rather the location of the establishment matters.[61] The importance of the notion of establishment comes from the fact that the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union triggers the application of the GDPR rules and the related obligations for the data controller or processor concerned.

In order to apply the establishment criterion, it is necessary, first, to determine whether a non-EU controller or processor is established through an establishment in the EU, and second, to assess whether the personal data is processed in the context of the activities of the said EU establishment.

#### 4.1.2.1 *An Establishment in the Union*

Although the term "*main establishment*" is defined in Article 4(16), the GDPR does not provide a definition of "*establishment*" for the purpose of Article 3. However, Recital 22 states that an '[*e*]*stablishment implies the effective and real exercise of activities through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect*'.[62] It is important to know that Recital 22 wording is identical to that found in Recital 19 of the DPD, to which the ECJ has referred in several rulings broadening the interpretation of the term "*establishment*". Therefore, to determine whether a non-EU entity has an establishment in the Union, both the degree of stability of the arrangements and the effective exercise of activities must be taken into account.[63] For instance, if an industrial machinery and equipment manufacturing company in Qatar has a fully owned branch office located in Paris overseeing its operations in Europe, including marketing its products, the French branch can be considered to be a stable arrangement, which exercises real and effective activities in light of the nature of the economic activity performed by the industrial machinery and equipment manufacturing company. As such, the French branch could

60 GDPR, art 3 (1).

61 See, Dan Jerker B. Svantesson, 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses' (2014) 50 Stan. J. Int'l L 53–102.

62 GDPR, Recital 22.

63 See, Dan Jerker B. Svantesson, 'The CJEU's Weltimmo Data Privacy Ruling – Lost in the Data Privacy Turmoil, Yet So Very Important' (2016) 23 Maastricht J. Eur. Comp. Law 232–241.

therefore be considered as an establishment in the Union, within the meaning of the GDPR.

#### 4.1.2.2 *Processing of Personal Data Carried Out "in the Context of the Activities of" an Establishment*

When it is concluded that a controller or processor is established in the Union, an assessment should then follow to determine whether the processing in question is performed in the context of the activities of this establishment. Article 3(1) confirms that the controller or processor will be subject to the GDPR obligations whenever the processing is carried out "*in the context of the activities*" of its relevant establishment in the Union.[64] This means that it is not necessary that the processing of the data in question is carried out "by" the relevant EU establishment itself. The European Data Protection Board (EDPB) advises that determining whether the processing is being carried out in the context of an establishment of the controller or processor in the Union for the purposes of Article 3(1) should be carried out on a case-by-case basis.[65] It also considers the meaning of '*processing in the context of the activities of an establishment of a controller or a processor*' is to be understood in view of the relevant case law.[66] For instance, the data processing activities of a data controller or processor established outside the EU may be inseparably linked to the activities of an EU establishment, and this may trigger the applicability of EU law, even if that EU establishment is not actually taking any role in the data processing itself.[67] For example, an e-commerce website is run by a company based in Saudi Arabia. The personal data processing activities of the company are exclusively carried out in Saudi Arabia. The Saudi company has established an office in Brussels for the purpose of marketing campaigns toward EU markets. In this case, it can be considered that the activities of the European office in Brussels are inseparably linked to the processing of personal data performed by the Saudi e-commerce website, insofar as marketing campaign toward EU markets particularly serve to make the service offered by the e-commerce website profitable. The processing of personal data by the Saudi company regarding EU sales can therefore be considered as performed in the context of the activities of the European office, as an establishment in

64 GDPR, art 3 (1).

65 European Data Protection Board. 2019. 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)'. 12 November. Retrieved 6 September 2022 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en.

66 Ibid.

67 Ibid.

the Union. This processing activity by the Saudi company will therefore be subject to the obligations of the GDPR as per its Article 3(1).

As noted previously, the ECJ's judgments have helpfully interpreted the notion of "*establishment*" within the meaning of EU data protection law. For instance, in Weltimmo case, it was concluded that the concept of establishment is flexible and must be interpreted apart from a formalistic approach, which indicates that entities are considered to be established only in the place of registration.[68] The lack of a registered office in an MS does not prevent a non-EU entity from having an establishment there within the meaning of EU data protection law.[69] This suggests that the place of registration does not necessarily mean the same as the place of establishment. However, it may serve as an indicator for an establishment. The relevant question for this research concerned the interpretation of the notion of "*establishment*" in Article 4(1)(a) of the DPD. The Court found that Article 4(1)(a) allows the application of the law on the protection of personal data of an MS other than the MS in which the controller is registered considering that the controller exercises, through stable arrangements within the territory of that MS, a real and effective activity in the context of which the processing of the personal data is performed.[70]

Another important example is Google Spain and Google case, where one of the questions before the ECJ was the interpretation of an "*establishment*" in Article 4(1)(a) DPD.[71] It was found that Article 4(1)(a) should not be interpreted restrictively. Interestingly, the ECJ's reasoning was principally focused on determining the meaning of "*in the context of the activities*" of an establishment, rather than the notion of "*establishment*". The ECJ noted that "*carried out in the context of the activities*" in Article 4(a) of the DPD cannot be given a restrictive interpretation because the provision needs to be read in accordance with the objective of the DPD.[72] It was also stated that one of the main objectives of the DPD is to ensure the effective protection of the data subjects with respect to

68 Case C- 230/ 14 Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, judgment of 1 October 2015 (ECLI:EU:C: 2015:639).

69 Graça Canto Moniz, 'Finally: A Coherent Framework for the Extraterritorial Scope of EU Data Protection Law – The End of the Linguistic Conundrum of Article 3(2) of the GDPR'. UNIO-EU Law Journal 4 (2018) 105 at 111.

70 Case C- 230/ 14 Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság,.

71 Case C-131/12 Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, May 2014, ECLI:EU:C:2014:317.

72 Christopher Kuner. 2021. 'Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection' University of Cambridge Faculty of Law Research Paper No. 20/2021. 16 April. Retrieved 6 September 2022 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827850.

the processing of their personal data. Regarding the notion of "*establishment*", it was found that,

> It is not disputed that Google Spain engages in the effective and real exercise of activity through stable arrangements in Spain. As it moreover has a separate legal personality, it constitutes a subsidiary of Google Inc. on Spanish territory and, therefore, an 'establishment' within the meaning of Article 4(1)(a) of Directive 95/46.[73]

The findings of Weltimmo and Google Spain were later adopted and reaffirmed in Verein für Konsumenteninformation[74] and Wirtschaftsakademie,[75] confirming the broad interpretation of Article 4(1)(a). It is therefore evident that the interpretation of "*establishment*" in Article 3(1) of the GDPR (and its counterpart in Article 4(1)(a) DPD) is much broader than it may seem at first.

#### 4.1.3 Applicability of the Targeting Principle (Article 3(2) GDPR)

The targeting principle is stipulated in Article 3(2) of the GDPR which reads as follows:

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
   (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.[76]

The absence of an establishment in the Union does not automatically mean that processing activities by a data controller or processor established in a non-EU country will not be subject to the GDPR rules, since Article 3(2) defines the circumstances in which the GDPR applies to a controller or processor not established in the Union, depending on their processing activities. Contrary to the establishment criterion that is applicable to both the EU entities and the

73 Case C-131/12 Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, May 2014, ECLI:EU:C:2014:317

74 Case C-191/15, Verein für Konsumenteninformation v Amazon EU Sàrl, 28 July 2016.

75 Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein V Wirtschaftsakademie Schleswig-Holstein GmbH, interveners: Facebook Ireland Ltd, Vertreter des Bundesinteresses beim Bundesverwaltungsgericht, 5 June 2018.

76 GDPR, art 3 (2).

non-EU ones, the targeting principle is oriented mainly towards the controllers and processors that are not established in the Union.[77]

Since the wording of Article 3(2) refers to '*personal data of data subjects who are in the Union*', the application of the targeting principle is not restricted by citizenship, residence or any legal status of the data subject whose personal data are being processed. This is confirmed by Recital 14, which states that '*[t]he protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data*'.[78] If the data subject is located in the Union must be assessed at the time of offering of goods or services or when the behaviour is being monitored, irrespective of the duration of the offer made or monitoring undertaken.[79]

The GDPR applies to the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union if one of the two conditions in Article 3(2) is met: (a) processing of personal data in relation to the offering of goods or services to data subjects in the EU or (b) processing of personal data in relation to the monitoring of personal behaviour of a data subject if this behaviour occurs within the EU.[80]

#### 4.1.3.1 *Offering of Goods or Services to Data Subjects in the Union*

The first scenario triggering the application of Article 3(2) is the "*offering of goods or services*".[81] The GDPR does not define the terms "*goods*" and "*services*". However, A definition of "goods" can be found in Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on Consumer Rights (the 2011 Directive). Article 2(3) of the 2011 Directive describes goods as *'any tangible movable items, with the exception of items sold by way of execution or otherwise by authority of law; water, gas and electricity shall be considered as goods within the meaning of this Directive where they are put up for sale in a limited volume or a set quantity*'.[82] Because the GDPR does not exclude any types

77 Dan Jerker B Svantesson, 'Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation', International Data Privacy Law 5 (2015) 226 at 230.

78 GDPR, Recital 14.

79 European Data Protection Board (n 65).

80 GDPR, art 3 (2).

81 Ibid, art 3 (2)(a).

82 Directive 2011/83/Eu of The European Parliament and of The Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011] OLJ 304/64, art 2 (3).

of goods or services, all categories of goods and services should be covered by its scope irrespective of whether a payment by the data subject is required.

Another fundamental element that should be considered in determining the application of Article 3(2)(a) is whether the conduct of the controller, which determines the manner and purposes of processing, demonstrates its intention to offer goods or services to a data subject located in the Union. Recital 23 of the GDPR indeed clarifies that *'in order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union'*.[83] For instance, a Qatari company offers daily and weekly mobile sports news and video content services, based on subscribers' preferences and interests. The sports news service is offered exclusively to subscribers located in Qatar, who must provide a Qatari phone number and email address when subscribing. Assuming, a Qatari subscriber travels to the Netherlands on holiday and continues using the service. Even though the Qatari subscriber will be using the service while in the Union, the service is not "*targeting*" individuals in the Union, but targets only individuals in Qatar. Therefore, the processing of personal data by the Qatari company does not fall within the scope of the GDPR.

It is significant to note that the processing of personal data of EU citizens or residents that occurs in a non-EU country does not trigger the application of the GDPR, as long as the processing is not related to a specific offer directed at individuals in the EU or to monitoring of their behaviour in the Union. If the Saudi immigration authority, for example, processes the personal data of EU citizens when entering Saudi Arabia territory for the purpose of examining their Hajj, the greater Muslim pilgrimage to Mecca, visa application, this processing is not subject to the GDPR.

The elements included in Recital 23 mirror the ECJ case law based on Council Regulation 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, particularly Article 15(1)(c).[84] In Pammer v Reederei Karl Schlüter GmbH & Co and Hotel Alpenhof v Heller (Joined cases C-585/08 and C-144/09), the ECJ was asked to clarify the meaning

83 GDPR, Recital 23.

84 Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2001] OLJ 12/1 art 15(1)(c).

of "*direct activity*" in Article 15(1)(c) of Regulation 44/2001 (Brussels I).[85] It was held that, in order to determine whether a trader can be considered to be "*directing*" its activity to the MS of the consumer's domicile, within the meaning of Article 15(1)(c) of Brussels I, the trader must have demonstrated its intention to establish commercial relations with such consumers. The ECJ considered whether the accessibility of a website from an MS justifies the conclusion that an activity is directed towards the said MS. The Court confirmed that a mere accessibility of a website from an MS does not constitute that the activities are orientated to the said MS. Although the concept of "*directing an activity*" differs from the "*offering of goods or services*", the Pammer case might assist in considering whether goods or services are offered to a data subject in the Union.[86]

#### 4.1.3.2 *Monitoring Data Subjects' Behaviour in the Union*

The second type of activity triggering the application of Article 3(2) is monitoring of data subjects' behaviour as far as their behaviour takes place within the EU, as expressed in Article 3(2)(b) of the GDPR.[87] The concept of monitoring is innovative in the applicability of EU data protection law because it broadens the scope of the GDPR to catch those non-EU controllers and processors who target the EU. Recital 24 clarifies that,

> The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union.[88]

In order to trigger the application of the GDPR, the behaviour monitored must relate to a data subject in the Union and must take place in the Union territory.[89] For example, a retail consultancy company established in the UAE provides advice on retail layout to a shopping centre in Germany based on an analysis of customers' movements throughout the centre collected through

85 Joined Cases C- 585/ 08 and C- 144/ 09, Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG and Hotel Alpenhof GesmbH v Oliver Heller, judgment of 7 December 2010 (Grand Chamber) (ECLI:EU:C:2010:740).

86 Ibid.

87 GPDR, art 3(2)(b).

88 Ibid, Recital 24.

89 Brendan Van Alsenoy, 'Reconciling the [Extra]territorial Reach of the GDPR with Public International Law' in Eva Lievens, Gert Vermeulen (ed), *Data Protection and Privacy Under Pressure Transatlantic tensions, EU surveillance, and big data* (Antwerp: Maklu, 2017) 87.

Wi-Fi tracking. The analysis of a customers' movements will amount to the monitoring of individuals' behaviour because the shopping centre is located in Germany and the data subjects' behaviour occurs in the Union. As a result, the consultancy company is subject to the GDPR regarding the processing of this data according to Article 3(2)(b). Recital 24 further specifies that *'in order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet …'*.[90] Although Recital 24 refers only to the monitoring of a behaviour through the tracking of a person on the internet, the EDPB suggests that tracking through other types of networks or technology involving personal data processing should also be considered in determining whether a processing activity amounts to a behavioural monitoring.[91]

As noted earlier, the concept of targeting requires an intention to target. This raises a significant question about whether an intention to monitor is required. In contrast to the provision of Article 3(2)(a), neither Article 3(2)(b) nor Recital 24 requires the data controller or processor "*intention to target*" to determine whether the monitoring activity would trigger the application of the GDPR to the processing activities.[92] Nevertheless, the use of the word "*monitoring*" suggests that the controller has a particular purpose in mind for the collection and subsequent reuse of the relevant data about an individual's behaviour in the Union. For example, profiling, as a form of monitoring, is defined in Article 4(4) of the GDPR as:

> Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.[93]

It is, therefore, necessary to consider the controller's aim for processing the data and, particularly, any subsequent behavioural analysis or profiling techniques involving relevant data.[94]

90 GDPR, Recital 24.

91 European Data Protection Board (n 61).

92 See, Paul de Hert and Michal Czerniawski, '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 (2016) 230 at 238.

93 GDPR, art 4(4).

94 V. Kumar and Werner Reinartz, *Customer Relationship Management Concept, Strategy, and Tools* (3rd edn Berlin: Springer Berlin Heidelberg, 2018) 298.

It is significant to know that data controllers or processors subject to the GDPR according to Article 3(2) are under an obligation to designate a representative in the Union.[95] Thus, a controller or processor not established in the Union but subject to the GDPR failing to appoint a representative in the Union would be in breach of the GDPR.

Based on the foregoing discussion, the territorial gateways through which GDPR applies are much wider than might be thought and so capture businesses and organisations outside Union, including GCC businesses, which might not have thought they are under its scope. A recent English court ruling has increased the risk that non-EU data controllers or processors will be covered by the GDPR scope, irrespective of their location. In the case of Soriano v Forensic News LLC and Others, the UK's Court of Appeal ruled on the application of extraterritorial jurisdiction under EU GDPR.[96] In this case, a UK-based claimant complained about a number of articles, social media posts and a podcast published by a US journalism website linking the claimant to third parties in a way which, according to the judge, amounted to '*a sustained assault on the Claimant and his reputation*'. The claimant brought various claims, including the territorial scope of the GDPR. At the first instance, the English court refused permission to serve the claim outside the jurisdiction, ruling that the data protection case disclosed no real prospect of meeting either of the two tests in Article 3 which are necessary for the GDPR to apply.[97] However, the Court of Appeal disagreed, ruling that there was a reasonable prospect that all of the jurisdictional grounds set out in Article 3 were present in this case. The impact of Soriano has been to accept that the bar for a data controller or processor to be covered by either Article 3(1) or 3(2) is arguably much lower, and this increases the risk that GDPR will apply to their activities. While the UK is no longer an EU member, UK GDPR is identical to the EU version. Thus, the grounds on which the English Court of Appeal has reached its conclusion that UK GDPR has extraterritorial reach might be equally persuasive to EU courts.[98]

## 5 GCC Data Protection Framework

The introduction of the GDPR in 2016 has sparked a global legislative movement that aims at protecting individuals' privacy and curbing data

95 GPDR, art 27.
96 Soriano v Forensic News LLC and Others [2021] EWCA Civ 1952.
97 Soriano v Forensic News LLC and Others [2021] EWHC 56 (QB).
98 Ibid.

vulnerability. Countries with robust economic ties to the EU have taken a proactive approach to compliance with the GDPR rules.[99] Thus, many of the new laws were directly influenced by the GDPR. Theoretically, this will ensure that local companies comply with the GDPR and can continue doing business in the EU without breaching its strict requirements. The GCC countries have followed this global trend by adopting specific data protection regulations.[100] Qatar was the first GCC country to enact a law specific to data protection at the end of 2016, followed by Bahrain in 2018, Saudi Arabia,[101] UAE[102] and Kuwait[103] in 2021, and finally Oman[104] in 2022. However, it is significant to know that, unlike the GDPR, in the GCC, there is no overreaching federal law that governs data protection, rather, each country has independently developed its own approach to data protection legislation, influenced, to varying degrees, by international standards, such as GDPR, and best practice.[105]

This article argues that the unprecedented spike in data protection legislative activity across the GCC over the past five years can be mainly attributed to competition. To illustrate, as part of their efforts to facilitate the transformation from hydrocarbon-driven to data-driven economies, Bahrain and Qatar have introduced the GCC first data protection laws, which aim at attracting foreign investments by offering a specific and comprehensive framework for data protection. In preparing to become the region's hub for data centres, with Amazon Web Services (AWS)[106] and Huawei Technologies planning to extend their data centres, Bahrain, for example, introduced its comprehensive Personal Data Protection Law (PDPL) in 2018.[107] The PDPL was designed specifically to ensure that these data centres and foreign parties are able to safely store data in Bahrain and to clarify jurisdictional and procedural rules.[108] This has encouraged the engagement of global companies in Bahrain,

99 Hiroyuki Tanaka, 'Impact of the GDPR on Japanese Companies', Business Law International 20 (2019) 137 at 140.

100 Robert L. Ford. 2018. 'The Impacts of the GDPR on Corporate Governance Practices in the GCC'. 6 October. Retrieved 20 September 2022 https://www.lexis.ae/2018/06/10/the-impacts-of-the-gdpr-on-corporate-governance-practices-in-the-gcc-by-robert-l-ford/.

101 Personal Data Protection Law Royal Decree M/19 of 9/2/1443H (2021).

102 Federal Decree Law No. 45 of. 2021 on Personal Data Protection.

103 Kuwait Data Privacy Protection Regulation – Resolution No. 42 (2021).

104 Royal Decree 6/2022 Promulgating the Personal Data Protection Law.

105 Sarah Johansson and Ahmed El-Masry. 2021 'Dust in the Cloud: The Future of Data Governance in the GCC' Middle East Institute. 6 December. Retrieved 11September 2023 https://www.mei.edu/publications/dust-cloud-future-data-governance-gcc.

106 One of the world's largest cloud computing providers.

107 Law No. (30) of 2018 with Respect to Personal Data Protection Law.

108 Ibid, art 3.

which in turn ensured a fundamental avenue for economic growth.[109] Similarly, Qatar introduced the first data protection law in the region in 2016 which was substantially updated in 2021.[110] In order to enhance the performance of local and international companies operating in its jurisdiction and ensure that they will be compliant with international standards, such as the GDPR, the comprehensive data protection framework in Qatar describes the rules for storing, processing, and transferring data.[111] In theory, all businesses operating in Qatar and Bahrain that offer services to clients based in the EU are required to be compliant with the GDPR. Therefore, establishing modern legislative frameworks in line with GDPR and other international standards is necessary to enable them to compete and operate across borders.

In contrast to Qatar and Bahrain, the lack of specific and comprehensive data protection laws in UAE, Saudi Arabia, Oman and Kuwait was a critical challenge that undermined the businesses' ability to compete and operate in international markets including the EU market and made these countries less attractive for foreign investors willing to invest in sectors that require cross-border data flows.[112] Therefore, in order to ensure that their laws and regulations are in line with international data protection standards, these countries have recently witnessed a wave of specific personal data protection laws. While these laws have been influenced to varying degrees by the GDPR, there are significant disparities, especially regarding their approach to data protection.[113] As noted above, the reason for the extensive global reach of the GDPR is mainly related to its foundation: the notion of fundamental rights and promoting human rights, particularly the right to privacy. This can be clearly seen in the restraints and compliance rules for data acquisition, storage, and usage. The GDPR, for instance, distinguishes between personal and sensitive personal data.[114] If a website stores information like customers' date of birth when they register, and also saves sensitive data such as their religion, under the GDPR that information must be stored and treated differently. Contrary to

109 Johansson and El-Masry (n 105).
110 Law No. (13) of 2016 on Protecting Personal Data Privacy.
111 Ibid, art 8.
112 STA Law Firm 'A Guide to Information Security and Data Protection Laws in the GCC Countries'. Ct Uncourt 6 (2019) 17 at 25.
113 Johansson and El-Masry (n 105).
114 GPDR, Recital 51; Jon Truby, Rafael Dean Brown & Imad Antoine Ibrahim, "Regulatory options for vehicle telematics devices: balancing driver safety, data privacy and data security" (2024) 38(1) International Review of Law, Computers & Technology. 86–110 (2024).

the GDPR, the main priority of data protection regulations in the GCC countries is protecting individuals from malicious actors and activities.[115] This suggests that the level of data protection in the GCC countries is not equivalent to that offered by the GDPR. Importantly, the European Commission has the power to determine, on the basis of article 45 of GDPR whether a country outside the EU offers an adequate level of data protection. However, the Commission has not yet included any GCC countries on its lists.

### 5.1 *Is It the Time to Establish GCC-Wide Data Protection Law?*

The disparities between the GCC countries regarding their approaches to data protection raise a significant question about whether this is the time to establish a GCC-wide legislative framework for data protection. As noted earlier, in contrast with the EU, the GCC countries lack an overarching regional framework for data protection. While the political and economic environment of the EU is mainly organised in such a way as to integrate economic benefits and legislative efforts between MSs in a shared economic cooperation area, an equivalent body of governance does not exist in the GCC. Although the GCC promotes shared principles and similarities in national regulations on issues such as trade and security, the existing data protection regulations do not identify a specific regional standard.[116] It is significant to emphasise that the lack of a governing body in the GCC prevents the establishment and enforcement of a GCC-wide data protection law similar to the GDPR. Therefore, aligning the GCC's different approaches and transforming them into a unified legal framework in the absence of a regional authority or authorities can be a daunting task.

## 6 Conclusion

This article has examined the extraterritoriality of the GDPR and its effect on GCC businesses. Understanding the extraterritorial application of the GDPR is significant to assess whether GCC businesses might fall under its scope, which in turn means that those businesses might be subject to very strict rules and obligations which ensure that data subjects are well protected.[117] GCC businesses could be fined up to 4 percent of worldwide turnover or 20 million

115 STA Law Firm (n 112) at 23.

116 Ibid at 24.

117 Rafael Brown, Jon Truby & Imad Antoine Ibrahim, "Mending Lacunas in the EU's GDPR and Proposed Artificial Intelligence Regulation" (2022) 9 European Studies. 61–90.

euros (whichever is greater) for breaching those obligations. As explained in this article, categorising the right to data protection as a fundamental right could appear to constitute a decisive reinforcement of the level of protection effectively provided to individuals throughout the EU, and since the GDPR builds on the notions and principles of data protection provided by the DPD of 1995, it is an evolution, not a revolution. Due to the ambiguity around the extraterritorial scope of the GDPR, many GCC businesses still do not comply with it. Therefore, this article has attempted to remove this ambiguity by examining the extraterritoriality criteria under Article 3, focusing on the establishment and the targeting principles. To achieve this, the research has relied on case law and the EDPB guidance, showing that the territorial gateways through which the GDPR applies are much wider than might be thought and so may capture many GCC businesses which might not have thought they are under its scope.

The research then discussed the GCC data protection framework, highlighting that the unprecedented spike in data protection legislative activity across the GCC over the past five years can be mainly attributed to competition. While the recent laws have been influenced to varying degrees by the GDPR, there are significant disparities, especially regarding their approach to data protection. The article also has raised the issue of establishing GCC-wide data protection law similar to the EU, arguing that aligning the GCC's different approaches and transforming them into a unified legal framework in the absence of a regional authority or authorities can be a challenging task.