

# White Paper on the Data Protection Regimes in the GCC

A Comprehensive Overview and Comparative Analysis



**IIC MENA CHAPTER DATA PRIVACY (DP)  
COMMITTEE**

**Disclaimer:** This is a working paper, and hence it represents research in progress. This paper represents the opinions of the IIC MENA Chapter - Data Privacy Committee and is the product of professional research. It is not meant to represent the position or opinions of the International Institute of Communications (IIC).

# Data Protection Regimes in the GCC

## A Comprehensive Overview and Comparative Analysis

### Table of Contents

<b>1. Introduction</b> .....	<b>3</b>
<b>1.1. Background</b> .....	<b>3</b>
<b>1.2. Scope and Objectives</b> .....	<b>3</b>
<b>1.3. Methodology</b> .....	<b>3</b>
<b>2. Data Protection Landscape in the GCC</b> .....	<b>5</b>
<b>2.1. Overview of Data Protection Concepts</b> .....	<b>5</b>
2.1.1 Key areas of Data Protection Laws.....	6
<b>2.2. Importance of Data Protection in the GCC</b> .....	<b>20</b>
2.2.1 Privacy and Data Protection in the Context of Emerging Technologies.....	20
<b>3. Comparative Analysis of Data Protection Laws in Select GCC Countries</b> .....	<b>24</b>
<b>3.1. Data Protection Officer (“DPO”)</b> .....	<b>24</b>
<b>3.2. Cross Border Transfers (general prohibition)</b> .....	<b>25</b>
<b>3.3. Prior Consultation</b> .....	<b>27</b>
<b>3.4. Design and Default</b> .....	<b>27</b>
<b>3.5. Data Protection Impact Assessment (“DPIA”)</b> .....	<b>28</b>
<b>4. Cross-Country Comparison and Common Trends</b> .....	<b>29</b>
<b>4.1. Overview of Similarities</b> .....	<b>29</b>
4.1.1. Overseeing and enforcing data protection laws and regulations .....	30
4.1.2. Promoting awareness and compliance .....	31
4.1.3. Handling complaints and investigations .....	32

4.1.4. Establishing guidelines and standards .....	34
4.1.5. Collaboration .....	36
4.1.6. Support and guidance .....	37
4.1.7. Audit and assessments .....	38
4.1.8. Penalties and sanctions .....	39
4.2.1. Governance structure .....	41
4.2.2. Scope of applicability.....	44
4.2.3 Legal framework.....	47
4.2.4. Powers and enforcement capabilities .....	48
4.2.5. Collaboration and information exchange .....	52
4.2.6. Cultural and societal factors.....	52
<b>4.3. Data Protection Challenges in the GCC .....</b>	<b>53</b>
<b>4.4. Emerging Trends and Best Practices .....</b>	<b>55</b>
<b>5. Future Directions and Potential Changes .....</b>	<b>56</b>
5.1 Strengthening GCC Data Protection Laws and Regulations.....	56
5.2 What can data controllers do to comply across the GCC region? .....	57
5.3 What can national GCC authorities do to ease compliance across the GCC region? .....	57
<b>ANNEX 1 .....</b>	<b>59</b>
<b>ANNEX 2 - DATA PROTECTION LAWS IN GCC COUNTRIES.....</b>	<b>60</b>

# 1. INTRODUCTION

## 1.1. Background

With the increasing reliance on digital technologies and the proliferation of personal data, safeguarding individual privacy and ensuring robust data protection mechanisms have become crucial in the GCC, with repercussions that go well beyond the sectoral concerns of the regional communications industry. This evolution comes at a time when the need to share personal data to grow and develop regional businesses and economies has never been greater.

This paper examines the existing data protection laws, regulations, and initiatives adopted by GCC countries (together, the "**Data Protection Laws**") with the focus on assessing the opportunity to develop a regional data protection framework, similar to the EU-wide General Data Protection Regulation ("**GDPR**"), that would allow for consistency in Data Protection Laws and their interpretation, the role of data protection and other regulatory authorities, and a harmonized implementation and enforcement across the GCC.

## 1.2. Scope and Objectives

In undertaking this comparative analysis, the authors wish to highlight the fundamental principles underpinning the data protection regimes within the region, placing particular focus on the commonalities between the various jurisdictions that they have examined. This paper also discusses the divergences between the applicable regulatory frameworks and proposes ways to harmonise these differences. Legal certainty is fundamental for prospective investors. The adoption of harmonised rules would undoubtedly serve to facilitate transactions and minimise the cost of doing business in the GCC. With this in mind, this paper calls upon the various policy makers and regulatory bodies to bridge the gaps between the various data protection frameworks to ensure that data controllers and data processors can operate seamlessly throughout the region.

## 1.3. Methodology

This paper has undertaken a detailed comparative analysis of the Data Protection Laws with a focus on identifying key aspects of the Data Protection Laws, highlighting their similarities and differences, opportunities for common approaches while discussing the remaining challenges to a truly regionalized approach to privacy. Please note that this paper does not constitute legal advice.

We have examined, in particular, the following Data Protection Laws:

- **United Arab Emirates (“UAE”):** Federal Decree No. 45/2021 for the Protection of Personal Data (“**UAE Law**”). Kindly note although the UAE Law is currently in force, companies are required to "regularise their status" in accordance with the UAE Law within 6 months from the date of issuance of the executive regulations<sup>1</sup> (“**UAE Executive Regulations**”). The UAE Executive Regulations have not yet been issued;
- **Saudi Arabia (“KSA” or “the Kingdom”):** Personal Data Protection Law issued pursuant to Royal Decree No. (M/19) dated 09/02/1443 AH corresponding to 16/09/2021(G) (as amended), (“**PDPL**”), The Implementing Regulation of the Personal Data Protection Law (“**KSA Implementing Regulation**”) and Regulation on Personal Data Transfer Outside the Kingdom (“**Transfer Regulations**”), (together, “**KSA Law**”);
- **Oman:** Sultani Decree No. 6/2022 (“**Oman Law**”) and Ministerial Decision No. (34) of 2024 Issuing the Implementing Regulation of the Personal Data Protection Law (“**Oman Executive Regulations**”). The timeline for companies to align their data processing operations with the Oman Law has been extended another year, to 05 February 2026<sup>2</sup>;
- **Bahrain:** Law No. 30/2018 (“**Bahrain PDPL**”), Bahrain Ministerial Decision No. 48/2022 On the Rights of Owners of Personal Data, Bahrain Ministerial Decision No. 42/2022 On the Transfer of Personal Data Outside the Kingdom of Bahrain, and Bahrain Ministerial Decision No. 43/2022, Bahrain Ministerial Decision No. 46/2022 On Data Protection Controllers and Bahrain Ministerial Decision No. 43/2022, Defining the Requirements to be met in Technical and Organizational Measures to Protect Personal Data (“**Bahrain Implementing Regulations**”) (together, “**Bahrain Law**”);
- **Qatar:** Law No. 13/2016 (“**Qatar Law**”) and guidelines for regulated entities issued by the National Cyber Governance and Assurance Affairs (“**NCGAA**”) of the National Cyber Security Agency (“**NCSA**”) (“**NCGAA Guidelines**”); and
- **Kuwait:** Administrative Decision No. 26/2024 Concerning the Issuance of the Data Privacy Protection Regulation – (“**Kuwait Law**”). Kindly note that this law is published by the Communications and Information Technology Regulatory Authority and is applicable to service providers licensed by the authority.

We have not considered the following regional Middle East data protection laws:

---

<sup>1</sup> UAE Law, Article 29.

<sup>2</sup> Oman Ministerial Decision No. 06/25, amending Oman Ministerial Decision No. 34/24.

- Dubai International Financial Centre (“**DIFC**”) DIFC Law No. 5/2020 Data Protection Law or DIFC Data Protection Regulations 2020 (as amended);
- Abu Dhabi Global Market (“**ADGM**”) Data Protection Regulations 2021;
- Qatar Financial Centre (“**QFC**”) Data Protection Law 2021; or
- Data Protection guidelines issued by the Telecommunications Regulatory Authority of the Kingdom of Bahrain or the Saudi Data and AI Authority (“**SDAIA**”).<sup>3</sup>

The reason for this exclusion from this paper’s scope is that we have generally not considered industry specific regulations that cover data protection, e.g., in relation to the financial services, healthcare and telecommunications industries or the government sector; neither have we considered consumer protection regulations or cybercrime laws that also include data protection requirements.

## **2. DATA PROTECTION LANDSCAPE IN THE GCC**

### **2.1. Overview of Data Protection Concepts**

The Data Protection Laws largely reflect concepts set out in foreign data protection regulatory regimes that serve as a regional or global reference, notably the GDPR. Such a common reference can greatly assist with the harmonization of the Data Protection Laws. It can also support their implementation and compliance as international businesses coming into the Middle East are already familiar with GDPR-style data protection laws.

That said, alignment with the GDPR has only driven harmonization so far and there are still significant differences between the Data Protection Laws in key areas that require additional focus and effort to ensure that the Data Protection Laws can be effectively aligned.

---

<sup>3</sup> SDAIA's structure, powers and tasks are defined in Council of Ministers Resolution No. (292) dated 27/4/1441 AH, as amended by Council of Ministers Resolution No. (195) dated 15/3/1444 AH.

## 2.1.1 Key areas of Data Protection Laws

### 2.1.1.1 Consent

The Data Protection Laws are largely consistent in emphasizing the role of consent as a lawful basis for processing personal data. In most Data Protection Laws, it is prohibited (except under certain circumstances established by law) to process personal data without the consent of the data subject and (for example), in Oman and Kuwait, guardian consent for children/minor personal data.

The Data Protection Laws set out conditions for obtaining consent. Although such conditions vary under each law, there are some similarities. For example, the laws of the UAE, KSA, Bahrain, Oman and Kuwait require consent to be proven or documented. Some jurisdictions also require consent to be requested or received in a clear and specific manner. For instance, KSA Law, Bahrain PDPL and Oman Law require that consent is given by a person with full legal capacity, by a competent person, or by a fully qualified person (respectively).

Since the overarching mechanism with regards to consent varies amongst the various GCC countries, it is paramount that the Data Protection Laws are considered separately and, in some detail, when determining whether consent has been adequately obtained. For example, Article 11(2) of the KSA Implementing Regulation requires consent to be explicit in certain cases only (i.e., when processing sensitive or credit data, or if decisions are made based entirely on automated data processing), whilst Oman Law requires, under Article 10, controllers to prove the written (express) consent of data subjects.<sup>4</sup> Although no corresponding conditions are set out under Qatar Law, the NCGAA Guidelines<sup>5</sup> provide a checklist (for privacy programmes) with consent conditions including (without limitation) a positive opt-in requirement, having consent statements which are clear, specific, concise and separate from other terms and conditions, and the requirement to name any third-party controllers who will rely on such consent.

General compliance with the consent conditions under the Data Protection Laws requires effective consent management including a requirement to obtain consent together with granting the data subject the right to withdraw such consent. The table below illustrates the extant positions under the various Data Protections Laws.

	UAE	KSA	Oman	Bahrain	Qatar	Kuwait
--	-----	-----	------	---------	-------	--------

<sup>4</sup> We would note, however, that Article 4 of the Oman Executive Regulation requires controllers to obtain explicit consent. The approval shall be given in writing, electronically or other means determined by the controller. It is uncertain, therefore, whether written consent is required or not.

<sup>5</sup> More specifically, the Personal Data Management System (PDMS) Checklist for Regulated Entities issued by NCGAA.

Conditions to consent (Y/N)	Yes <sup>6</sup>	Yes <sup>7</sup>	Yes <sup>8</sup>	Yes <sup>9</sup>	Yes. Although not in the law but in the Personal Data Management System Guidelines. <sup>10</sup>	Yes

With the notable exception of Oman Law, the various Data Protection Laws offer exceptions to the general prohibition (of not processing personal data without consent) and list out lawful bases (other than consent) to processing personal data (although we would note in that the Oman Law has broad exceptions to its application that we would normally see as legal basis in other laws including performance of a legal obligation imposed on the controller under law, judgment or decision of a court or executing a contract to which the data subject is a party).

Lawful bases vary, particularly as regards to the right to process personal data for the legitimate interests of the data controller, which can be found including under the KSA Law, Qatar Law and the Bahrain PDPL. Article 16 of the KSA Implementing Regulation sets out further conditions when relying on legitimate interest as a lawful basis with some exceptions, particularly to public entities or as regards the processing of Sensitive Data<sup>11</sup> (please see Appendix 3 for more information on lawful bases for such processing).

Under the Qatar Law (apart from consent) processing personal data can be done to achieve a Legitimate Purpose.<sup>12</sup> There are exceptions under Article 19 including fulfilling a legal obligation or order, or protecting the vital interests of the individual. The NCGAA Guidelines suggest that a Lawful Purpose may also include legal or contractual obligation or legitimate interest.

---

<sup>6</sup> UAE Law, Article 6(1).

<sup>7</sup> PDPL, Article 5 and KSA Implementing Regulation, Article 11.

<sup>8</sup> Oman Law, Article 10.

<sup>9</sup> Bahrain PDPL, Article 24(1).

<sup>10</sup> <https://assurance.ncsa.gov.qa/sites/default/files/library/2022-12/Personal%20Data%20Management%20System%20%28PDMS%29%20-%20Guideline%20for%20Regulated%20Entities.pdf?csrt=8264902638380098942>

<sup>11</sup> As defined in PDPL.

<sup>12</sup> Legitimate Purpose: The purpose for which the personal data of an individual are being processed, in accordance with Law.

For completeness, we would note that the Oman Law also prohibits the processing of certain types of data (namely considered as sensitive personal data in other data protection laws as it includes Genetic data<sup>13</sup>, Biological Data<sup>14</sup>, Health Data<sup>15</sup>, ethnic origins, sexual life, political or religious opinions or beliefs, criminal convictions, or security measures)<sup>16</sup> without a permit from MTCIT (which the Oman Executive Regulations set out the application process for). It also prohibits the processing of personal data of a child without guardian consent (unless the processing is in the child’s best interest). The Oman Executive Regulations set out further details and conditions for processing children personal data.

	UAE	KSA	Oman	Bahrain	Qatar	Kuwait
Other lawful bases available (Y/N)	Yes <sup>17</sup>	Yes <sup>18</sup>	No, but the Oman Law does not apply in various cases, some of which are similar to lawful bases in other data protection laws e.g, including performance of a legal obligation imposed on the controller under law, judgment or decision of a court or executing a contract to which the data subject is a party <sup>19</sup> and requires a permit from MTCIT to process certain types of data including Genetic data, Biological Data, Health Data, ethnic origins, sexual life, political or	Yes <sup>20</sup>	Yes, may include Legitimate Purpose (which we understand from NCGAA Guidelines to be (legitimate interest, legal obligations and contractual obligations) as well as exceptions under Article 19.	Yes <sup>21</sup>

<sup>13</sup> Genetic Data: Personal Data relating to inherited or acquired genetic characteristics, obtained from the analysis of the biological sample.

<sup>14</sup> Biological Data: Personal Data that results from specific technical Processing related to physical, psychological or behavioral characteristics, such as a face image or DNA data.

<sup>15</sup> Health Data: Personal Data relating to physical, mental and physiological health.

<sup>16</sup> Oman Law, Article 5, and the Oman Executive Regulations, Article Chapter 2.

<sup>17</sup> UAE Law, Article 4.

<sup>18</sup> KSA Law, Article 6.

<sup>19</sup> Oman Law, Article 3.

<sup>20</sup> Bahrain Law, Article 4.

<sup>21</sup> Kuwait Law, Article 3.

			religious opinions or beliefs, criminal convictions.			
--	--	--	--	--	--	--

### 2.1.1.2 Purpose Limitation

Under the purpose limitation principle, personal data can only be processed for a clear and specific purpose.

The concept of purpose limitation is found in all of the Data Protection Laws to varying degrees. Some examples include (without limitation):<sup>22</sup>

- Bahrain PDPL requires personal data to be collected for a legitimate, specific and clear purpose, not to be altered nor any subsequent processing to be inconsistent with the purpose for which it was collected;<sup>23</sup>
- Kuwait Law requires a Service Provider<sup>24</sup> to explain the purpose of collecting personal data necessary to provide the service...<sup>25</sup> and “during the provision of the Service or after its completion” for the Service Provider to determine the purpose of data collection, legal basis and retention period;<sup>26</sup>
- Qatar Law requires for the controller to verify that the personal data collected is adequate and relevant to the Legitimate Purpose and accurate, complete and kept up to date to meet the Legitimate purpose and shall not be kept for longer than necessary to achieve the purpose.<sup>27</sup> The NCGAA Guidelines (including the Principles of Data Privacy and Data Privacy by Design and by Default) also set out purpose limitation as a principle under the law;<sup>28</sup>

<sup>22</sup> Kindly note the below examples do not detail any exceptions under the laws.

<sup>23</sup> Bahrain PDPL, Article 3(2).

<sup>24</sup> Service Provider/Licensee: The person licensed to provide one or more telecommunication services to the public or licensed to manage, establish or operate a telecommunication network or internet service to provide telecommunication services to the public. This includes providers of information or content through the telecommunication network.

<sup>25</sup> Kuwait Law, Article 2(3).

<sup>26</sup> Kuwait Law, Article 4(2).

<sup>27</sup> Qatar Law, Article 10.

<sup>28</sup> Qatar Law, Article 10.

- UAE Law requires personal data to be collected for a specific and clear purpose<sup>29</sup> and should not be kept after fulfilling the purpose of processing;<sup>30</sup>
- PDPL requires controllers to only collect personal data directly from the data subject and to process personal data for the purposes for which they have been collected.<sup>31</sup>

There are some exceptions (in some Data Protection Laws) to these general rules, such as the UAE Law which extends the scope by allowing processing for similar purposes, an exception that is inherently open to much interpretation. Also, the PDPL (under Article 10) and KSA Implementing Regulations (under Articles 15 and 18) set out the instances and conditions where personal data can be collected from another source or processed for a purpose other than the one which it was initially collected (e.g. where consent has been obtained or where personal data collection is necessary to achieve the legitimate interests of the controller (without prejudice to the rights and interests to the data subject and provided no Sensitive Data<sup>32</sup> is processed)).

Some jurisdictions oblige data processors and data controllers to store personal data only until such time as the purpose has been fulfilled. Subsequent to that being achieved, personal data has to be anonymized (UAE and in certain cases Bahrain)<sup>33, 34</sup>, removed (Kuwait – where personal data is no longer necessary to provide the services requested by the user<sup>35</sup>) or destroyed (KSA<sup>36</sup> – although KSA Implementing Regulation also sets out conditions for anonymising personal data).

It remains a challenge within the GCC to ensure the effective application of this principle and to ensure that there are effective controls on the processing of personal data for the specific purposes set out in the privacy notices, thereby limiting a wider processing of personal data that goes beyond the established purpose.

---

<sup>29</sup> UAE Law, Article 5(2).

<sup>30</sup> UAE Law, Article 5(7).

<sup>31</sup> PDPL, Article 10.

<sup>32</sup> Sensitive Data: *“Personal Data revealing racial or ethnic origin, or religious, intellectual or political belief, data relating to security criminal convictions and offenses, biometric or Genetic Data for the purpose of identifying the person, Health Data, and data that indicates that one or both of the individual’s parents are unknown.”*

<sup>33</sup> UAE Law, Article 5(7).

<sup>34</sup> Bahrain Law, Article 3(5).

<sup>35</sup> Kuwait Law, Article 13.2.

<sup>36</sup> KSA Law, Article 11(4).

### *2.1.1.3 Data minimization*

Traditionally, there have been limited effective controls on minimizing the amount of personal data processed and the importance of undertaking an assessment of whether their processing is actually required. The concept of data minimization is found in a number, but not all, of the Data Protection Laws, limiting the processing of personal data only to that which is necessary to achieve the purpose for which it is being processed. The language in the different Data Protection Laws varies, referring to the personal data that may be processed as being “limited”; “adequate” and “not excessive”. Certain Data Protection Laws, such as the Kuwait Law, are much broader and less specific in their focus on data minimization in comparison to (for example) the KSA Implementing Regulations which dedicates an entire article in the KSA Implementing Regulations on data minimisation (Article 19) or the requirement in the Oman Executive Regulations in relation to obtaining consent from children to “request from the child a minimum of data from their guardian for the purpose of verifying identity and obtaining the consent of the latter.”<sup>37</sup>

### *2.1.1.4 Security measures*

The Data Protection Laws have highlighted the importance of data security, thus reflecting global data protection best practice for adequate technical and organizational measures to protect personal data that is being processed. Thus, it is imperative that effective data security controls are put in place. Only a handful of countries - notably the UAE Law (under Article 20), Bahrain PDPL (under Article 8) and Kuwait Law (under Article 5) – set out in some detail data security requirements. whilst (for example) the KSA Implementing Regulation requires compliance with the standards imposed by the National Cybersecurity Authority (“NCA”) or the best recognized cybersecurity practices and standards if the controller has not legally bound by the NCA standards.<sup>38</sup>

It will be key for regulatory authorities in the GCC to clearly communicate their view of what constitutes effective data security controls to enable organizations to right size their data security measures. In a number of Data Protection Laws, data security is covered elsewhere in related regulations. For example, although limited information on security can be found in the Qatar Law, certain NCGAA Guidelines such as the Personal Data Management System Guidelines set out a checklist of core activities controllers should undertake. Additionally, the Data Privacy by Design and By Default Guidelines explain key precautions for controller to implement, including technical precautions. Together, these Guidelines provide further detail to implementing security measures. As another example, the Bahrain Implementing Regulations further define, in Article 2, technical and organizational measures to be applied.<sup>39</sup>

---

<sup>37</sup> Oman Executive Regulations, Article 11.

<sup>38</sup> KSA Implementing Regulation, Article 23.

<sup>39</sup> Bahrain Ministerial Decision No. 43/2022 Defining the Requirements to be Met in Technical and Organisational Measures to Protect Personal Data

### 2.1.1.5 Data subject rights

By definition, the Data Protection Laws cover data subjects' rights, but vary in terms of the specific rights they include. Most Data Protection Laws include the data subjects' fundamental right to access information on their personal data held, the way it is used and their ability to withdraw consent to its processing. They also include rights to have their personal data corrected or deleted. However, the Data Protection Laws differ in relation to data subjects' right to have their personal data ported to another data controller or how they can respond to automated processing or the processing of their personal data by different technologies. For instance, UAE and Oman set out a data subject's right to request transfer of personal data to another Controller, while both the Bahrain PDPL and UAE Law and NCGAA Guidelines<sup>40</sup> respectively allow data subjects to object to automated data processing.

A brief overview of the various rights across the different laws is provided in the below table. Kindly note that this only provides a high-level overview of the rights available under the Data Protection Laws and does not set out exceptions to its application. It is not a substantive list, as some rights may be present across different provisions of the laws (instead of explicitly being referred to as a right). For example, the Oman Law lists out the right for data subjects to be notified of any hacking or infringement of personal data and of the actions that have been taken in this regard. Although not an explicit right in any of the other laws, similar requirements may be found in data breach notification provisions instead.

A key challenge for data subjects will be to ensure the effective exercise of these rights, as the outcome will largely depend on how regulatory authorities across the GCC will enable them to do so, and the balance these authorities may need to strike between supporting individual data subjects in their exercise of their rights and limiting the administrative burden on GCC businesses in managing data subject requests.

<b>Non-exhaustive category of rights</b>	<b>UAE</b>	<b>KSA</b>	<b>Oman</b>	<b>Bahrain</b>	<b>Qatar<sup>41</sup></b>	<b>Kuwait</b>
--	------------	------------	-------------	----------------	---------------------------	---------------

<sup>40</sup> the Individuals' Rights Guidelines for Regulated Entities issued by NCGAA, Article 4.3.

<sup>41</sup> Kindly note, the Individual's Rights Guideline for Regulated entities usefully sets out in more detail when the rights apply, what each right means and how to comply (among other things).

Right to access personal data	Yes. <sup>42</sup>	Yes. <sup>43</sup>	Yes – right to obtain a copy of their processed personal data <sup>44</sup> , in a readable and clear format. <sup>45</sup>	Yes. <sup>46</sup>	Yes. <sup>47</sup>	Yes. <sup>48</sup>
Right to obtain information/ be informed <sup>49</sup>	Yes. <sup>50</sup>	Yes. <sup>51</sup>	Yes, although this is not set out under the rights of data subjects, the requirement is there for controllers to meet through	Yes. <sup>53</sup>	Yes. <sup>54</sup>	Yes, although this is set out throughout the Kuwait Law including under Article 4 and within the privacy policy provision.

<sup>42</sup> UAE Law, Article 14(1).

<sup>43</sup> Article 4(2), PDPL and KSA Implementing Regulation, Article 5.

<sup>44</sup> Oman Law, Article 11(c).

<sup>45</sup> Oman Executive Regulations, Article 19.

<sup>46</sup> Bahrain Law, Article 18.

<sup>47</sup> Qatar Law, Article 6.

<sup>48</sup> Kuwait Law, Articles 4(6) and 5(9).

<sup>49</sup> Please refer to “notice” in Appendix 3 for more information.

<sup>50</sup> UAE Law, Article 14(2).

<sup>51</sup> PDPL, Article 4(1) and KSA Implementing Regulation, Article 4.

<sup>53</sup> Bahrain Law, Article 17.

<sup>54</sup> Qatar Law, Article 6.

			their privacy policies. <sup>52</sup>			
Right to request transfer of Personal Data to another Controller	Yes. <sup>55</sup>	No, although KSA Law does provide the right to data portability by granting data subjects the right to access their personal data (in a readable and clear format). <sup>56</sup>	Yes. <sup>57</sup>	No.	No.	Maybe. Article 4(8) (although with very limited information) sets out that Service Providers shall determine “the mechanism for obtaining, correcting or deleting Personal Data, restricting access to such data or processing it, objecting to its processing or <b>requesting transfer</b> of Personal Data.” <sup>58</sup> [ <b>Bold</b> is our emphasis].

<sup>52</sup> Oman Law, Article 14 and Oman Executive Regulations, Article 21.

<sup>55</sup> UAE Law, Article.

<sup>56</sup> PDPL, Article 4(3) and KSA Implementing Regulation, Article 6.

<sup>57</sup> Oman Law, Article 11(d) and Oman Executive Regulations, Article 20.

<sup>58</sup> Kuwait Law, Article 4(8).

						Whether this includes the right to request to transfer personal data to another controller is uncertain.
Right to correction of Personal Data	Yes. <sup>59</sup>	Yes, <sup>60</sup> although the KSA Implementing Regulations explain the right as a restriction of processing for a period of time to enable the controller to verify the accuracy of personal data. The restriction does not apply where it contravenes the	Yes. <sup>62</sup> Controller and processors must also provide the means by which a child's guardian can access the child's personal data to update and modify it. <sup>63</sup>	Yes. <sup>64</sup>	Yes. <sup>65</sup>	Yes. <sup>66</sup>

<sup>59</sup> UAE Law, Article 15.

<sup>60</sup> PDPL, Article 4(4).

<sup>62</sup> Oman Law, Article 11.

<sup>63</sup> Oman Executive Regulations, Article 13.

<sup>64</sup> Bahrain Law, Article 23.

<sup>65</sup> Qatar Law, Article 5(4).

<sup>66</sup> Kuwait Law, Articles 4(6), 4(12) and 5(9).

		PDPL or the Implementing Regulation. <sup>61</sup>				
Right to erasure/destruction of Personal Data	Yes. <sup>67</sup>	Yes. <sup>68</sup>	Yes. <sup>69</sup>	Yes. <sup>70</sup>	Yes. <sup>71</sup>	Yes. <sup>72</sup> .
Right to restrict processing	Yes. <sup>73</sup>	No.	No, although the Oman Law does give data subjects the right to amend, update or block their personal data. <sup>74</sup> It is	No, although the Bahrain PDPL does give data subjects the right to correct, block or wipe their personal data. <sup>75</sup> It is uncertain	No.	Yes, if Article 4(8) <sup>76</sup> is interpreted as a data subject right and Article 4(12) applies. <sup>77</sup>

<sup>61</sup> KSA Implementing Regulation, Article 7.

<sup>67</sup> UAE Law, Article 15.

<sup>68</sup> PDPL, Article 4(5), and KSA Implementing Regulation, Article 8.

<sup>69</sup> Oman Law, Article 11(e) and Oman Executive Regulations Article 18.

<sup>70</sup> Bahrain Law, Article 23.

<sup>71</sup> Qatar Law, Article 5(3).

<sup>72</sup> Kuwait Law, Article 5(9).

<sup>73</sup> UAE Law, Article 16.

<sup>74</sup> Oman Law, Article 11(b).

<sup>75</sup> Oman Law, Article 11(b), Oman Law.

<sup>76</sup> Kuwait Law, Article 4(8): *“During the provision of the Service or after its completion, the Service Provider shall collect and process Data in accordance with the following conditions: ... Determining the mechanism for obtaining, correcting, or removing Personal Data, or restricting access to or Processing it, or objecting to its Processing, or requesting the transfer of Personal Data.”*

<sup>77</sup> Kuwait Law, Article 4(12) *“During the provision of the Service or after its completion, the Service Provider shall collect and process Data in accordance with the following conditions: ... The Service Provider shall provide an easy-to-use, practical and easily accessible means that enables the User to*

			uncertain what the latter (i.e what block entails).	what “block” entails.		
Right to object/stop processing	Yes, (in certain cases including if the processing is for direct marketing purposes including profiling related to direct marketing). <sup>78</sup> We would also note that data subjects also have the right to withdraw their consent. <sup>79</sup>	Yes, (withdrawing consent). <sup>80</sup>	Yes, in the form of cancelling their consent to the processing. This withdrawal of consent may be seen as different since this is the only legal basis under the law.	Yes <sup>81</sup> , including withdrawing consent in Bahrain Implementing Regulations. <sup>82</sup>	Yes, in the form of withdrawing consent <sup>83</sup> and objecting to the processing in certain cases. <sup>84</sup>	Yes, including withdrawing consent. <sup>85</sup>

*modify his Data, withdraw his consent, disable a service, or method of collecting, using, Processing or disclosing his Personal Data.”*

<sup>78</sup> UAE Law, Article 17.

<sup>79</sup> UAE Law, Article 6(2).

<sup>80</sup> PDPL, Article 5(2), and KSA Implementing Regulation, Article 12.

<sup>81</sup> Bahrain Law, Articles 20 and 21.

<sup>82</sup> Bahrain Ministerial Decision No. 48/2022 On the Rights of Owners of Personal Data, Article 6.

<sup>83</sup> Qatar Law, Article 5(1).

<sup>84</sup> Qatar Law, Article 5(2).

<sup>85</sup> Kuwait Law, Article 4(12). Article 4(8) may also apply if it is interpreted as a data subject right.

Right to object to decisions by Automated Processing.	Yes (with certain exceptions including where automated processing is included in a contract between the data subject and controller or where the data subject gave their prior consent). <sup>86</sup>	No, however the controller has certain obligations in relation to automated processing.	No.	Yes. <sup>87</sup>	Yes, as made clear in the Guidelines which set out when this right applies. <sup>88</sup>	Maybe, since Article 4(12) broadly enables users to “disable a service, or method of collecting, using, Processing or disclosing his Personal Data”, although this does not explicitly refer to automated processing. However, this is uncertain.
Right to Lodge a complaint with the applicable data protection authority	Yes. <sup>89</sup>	Yes. <sup>90</sup>	Yes. <sup>91</sup>	Yes. <sup>92</sup>	Yes. <sup>93</sup>	No.

UAE Law,<sup>86</sup> Article 17.

<sup>87</sup> Bahrain Law, Article 22.

<sup>88</sup> The Individuals’ Rights Guidelines for Regulated Entities issued by NCGAA, Article 4.3.

<sup>89</sup> UAE Law, Article 24(1).

<sup>90</sup> PDPL, Article 24 of PDPL and KSA Implementing Regulations, Article 37.

<sup>91</sup> Oman Law, Article 12 and Oman Executive Regulations, Article 41.

<sup>92</sup> Bahrain PDPL, Article 25.

<sup>93</sup> Qatar Law, Article 26.

### *2.1.1.6 Data transfers*

There are wide variations in how the Data Protection Laws approach cross-border data transfers. This varies from comprehensive data transfer provisions under the UAE Law, KSA Law, Oman Executive Regulations and Bahrain PDPL to much more limited data transfer options under other Data Protection Laws such as the Qatar Law. For example, the Bahrain Implementing Regulations on data transfers even details the process of applying for an authorization to transfer data, while the Qatar Law takes a different, less regulated approach by merely placing obligations on the data controller to ensure that cross-border data flow should not be restricted, so long as they remain compliant with the Qatar Law.<sup>94</sup> Similarly, the Kuwait Law's approach is less specific, in that it merely obliges data controllers/processors to: a) determine the mechanisms of data transfer; b) notify data subjects of transfers outside Kuwait; and c) maintain a record of data transfers that, if necessary, include the names of countries outside Kuwait that the data is being transferred to.

In Saudi Arabia, the PDPL allows the transfer or disclosure of personal data outside the Kingdom only for a number of strictly defined purposes such as to perform an obligation to which the data subject is a party. The Transfer Regulations add other purposes including to perform necessary operations for central processing to enable the controller to conduct its activities; to provide a service or benefit to the subject of the personal data; or to conduct scientific research and studies.<sup>95</sup> Additionally, the transfer or disclosure must meet certain conditions. These conditions (set out under Article 29(2) of the PDPL) require the transfer or disclosure not to cause any prejudice to national security or the vital interests of the Kingdom; there to be an adequate level of protection for personal data outside the Kingdom; and for the transfer or disclosure to be limited to the minimum amount of personal data needed. There are certain exceptions under Article 29(3) of the PDPL and under Article 4 of the Transfer Regulations. The Transfer Regulations provide more detail on the substantive conditions for any such transfers, and associated procedural and governance matters.

The Data Protection Laws follow, generally, the approach of identifying "adequate" jurisdictions for cross-border data transfers, although the number of adequate jurisdictions can vary widely based on the applicable Data Protection Law. There are similar means for enabling cross-border data transfers to countries that are deemed to be adequate and some commonality in the way "non-

---

<sup>94</sup> We would note, however that the NCGAA Guidelines on Data Protection Impact Assessments explain that transferring personal data outside Qatar may cause serious damage. This could mean that a DPIA should be done for such processing.

<sup>95</sup> Transfer Regulations, Article 2.

adequate” jurisdictions are covered, allowing data transfers in certain limited circumstances although there is no consistency across the Data Protection Laws in terms of these limited circumstances, varying from the use of consent, transfers under certain contractual conditions, use of standard contract clauses, binding corporate rules or other mechanisms for enabling data transfer.

As a result, there are enough variations to place challenges on organizations undertaking extensive regional cross-border data transfers seeking to adopt a regional policy for managing data transfers. It is therefore essential to establish some regional principles to facilitate and encourage the cross-border flow of personal data. There is a clear argument to build a regional “adequacy” arrangement that will enable personal data to flow easily across the region under specific circumstances. This will require significant collaboration from the regional regulatory authorities overseeing the respective Data Protection Laws and a common interest in driving great regional data sharing for the benefit of the wider regional economy as well as their own jurisdictions.

Please note that we have not looked at data localization restrictions under other, industry-specific, laws that cover, whether wholly or partially, data protection. These can prove particularly challenging for the regional movement of personal data, particularly depending on the type of personal data being transferred and the type of technology being used.

#### *2.1.1.7 Accountability and transparency*

These principles are clearly represented in most of the Data Protection Laws, particularly transparency. In addition to these principles, the Data Protection Laws set out, in their notice requirements, what organizations need to be communicating to data subjects regarding their data processing operations to provide such accountability and transparency.

## **2.2. Importance of Data Protection in the GCC**

### ***2.2.1 Privacy and Data Protection in the Context of Emerging Technologies***

#### *2.2.1.1 Artificial Intelligence (“AI”) and Machine Learning (“ML”)*

There are no specific regulations dedicated to the processing of personal data by AI and ML. The DIFC Data Protection Law has been one of the first to address data protection issues around the use of AI in its updated regulations<sup>96</sup>. Instead, these are generally covered in relation to the processing of personal data by emerging technologies, but AI and ML are not mentioned explicitly. Most particularly,

---

<sup>96</sup> [DIFC sets out AI requirements in updated data protection regulations; DIFC sets out AI requirements in updated data protection regulations \(pinsentmasons.com\)](https://www.pinsentmasons.com/difc-data-protection-regulations-consolidated-version-no-2); DIFC Data Protection Regulations (Consolidated Version No.2).

they are covered under the data protection impact assessment and/or the data protection officer requirements under the Data Protection Laws, which are triggered, depending on the Data Protection Law, by the use of emerging or new technologies.

As implementing regulations to the UAE Law is in the process of being adopted, we may see this issue being addressed in the near future, whether in terms of AI and ML specifically or, more generally, as emerging technologies.

Some high-level considerations for companies to note include:

- Typically, AI systems need to rely on large sets of data (also including personal data) to train and adjust their algorithm. This requires appropriate safeguards, in line with data protection laws, especially when it comes to special or sensitive types of data. One of the associated challenges is to define the circumstances under which regulatory sandboxes can provide a solution to this type of issue.
- Algorithmic bias, a problem in and by itself, may also be contrary to personal data protection provisions, as these require fairness and non-discrimination in the processing of personal data. On the other hand, remedying algorithmic bias may also raise, by itself, separate issues of compliance with the protection of personal data. This is why the EU's AI Act allows, exceptionally and under strict safeguards, the processing of sensitive personal data to the extent strictly necessary to ensure bias detection and correction in "high-risk" AI systems.
- Another associated question is whether different rules should apply to different AI systems depending on the different levels of risk to personal data/privacy that these normally entail. For example, as is the case already under the AI Act in the EU, should there be levels of risk for AI systems? How should these be defined?
- AI systems may need to anticipate individuals' future reliance on their rights to data portability.
- Other laws and/or publications or guidance issued by relevant authorities in the GCC jurisdictions should also be considered as these may shed further light on developing, using, implementing, adopting (etc.) AI and ML. Although we have not set this out in detail, by way of example, in the UAE, the Minister of State for Artificial Intelligence, Digital Economy and Remote Work Applications has published several non-binding guidelines on AI for the consideration of both the public and private sectors. There are also sector-specific, as well as emirate specific guidance, initiatives and policies from various authorities to consider as well as existing laws such as UAE criminal laws.

### 2.2.1.2 Internet of Things (IoT)

There are a number of IoT-related regulations across the GCC, issued by the national ICT regulators. There has been particular regulatory focus on IoT in the UAE<sup>97</sup>, KSA<sup>98</sup> and Oman<sup>99</sup>. IoT technologies also involve the processing of personal data, and although IoT and other emerging technologies are not yet specifically addressed in the Data Protection Laws, the proliferation of IoT devices may well raise IoT-specific questions in the context of data protection. Eventually, these may need to be addressed through some form of regulatory guidance to ensure that the Data Protection Laws are fit for purpose to address privacy issues relating to IoT technologies, particularly for the regional communications industry.

We list below a few examples of IoT-specific issues in the context of data protection:

- IoT devices may also collect and process personal data, which can be particularly vulnerable to privacy breaches or unauthorized use by service providers, insurance, employers etc. This is particularly the case with consumer IoT devices, such as smart wearables.
- Privacy policies and protective measures will normally be required at all levels of the IoT value chain: manufacturers, connectivity providers, application and platform providers, business users. They may all qualify as data controllers or at least data processors, depending on the circumstances, and hence be exposed to liability under data protection laws – possibly of more than one jurisdiction.
- IoT devices should adhere, in particular, to principles of data minimization, data retention, cross-border transfer restrictions, etc. Before being asked to provide their consent, consumers should be given adequate explanation as to how and why their personal data is being processed and information relating to how, once given, consent may be withdrawn.

---

<sup>97</sup> Internet of Things Regulatory Policy (from the TDRA).

<sup>98</sup> Internet of Things (IoT) Regulatory Framework (from the CST).

<sup>99</sup> Issuing Regulation for the Provision of Internet of Things services (from the TRA), Decision No. 93/2022.

### *2.2.1.3 Cloud Computing*

There are specific cloud computing regulations in various GCC jurisdictions which also cover, at least in part, data protection matters. These need to be considered along with the requirements in the Data Protection Laws relating to the use of emerging technologies (see 2.2.1.1 above) and cross-border data transfers as data loads are moved between cloud infrastructure across multiple countries.

Here are some typical data protection questions arising in the context of cloud computing services:

- Under which conditions (if any) will cloud computing service providers qualify as data controllers or data processors?
- When does the routine processing of data stored on the cloud qualify as processing under data protection laws?
- Beyond any contractual obligations under their agreements with users, what are the legislative obligations cloud service providers may have regarding security, encryption, access control, data breach notification and portability of personal data stored or processed on their systems?

Does the end-user's access to its data stored in the cloud qualify as a cross-border data transfer? If so, when is it allowed?

### *2.2.1.4 Biometrics*

Biometrics (or biological data) are addressed in most of the Data Protection Laws. In some of them, biometrics are dealt with as Sensitive Personal Data. In others, they are covered under the general “Personal Data” definition, as an undefined term or as a subset of biometrics (e.g. facial images; fingerprints, etc.) and/or listed along with “Genetic Data” or “DNA”.

In general, biometric data are typically subject to particularly strict protection under data protection laws, such as a requirement for the data subject's explicit and informed consent prior to processing. There are also some interesting additional provisions in certain Data Protection Laws. For example, under the Bahrain Law, the automated processing of biometric data provided for personal identification is subject to the prior written permission of the relevant authority<sup>100</sup>. As biometric recognition technologies continue to proliferate, it will be increasingly important to effectively manage the processing of biometric personal data. This will require

---

<sup>100</sup> Bahrain Law, Article 15(1)(B).

regulatory authorities to scrutinize how their Data Protection Laws address biometrics and take any steps necessary to ensure that the Data Protection Laws keep pace with the growth of biometric recognition technologies.

Additionally, Oman Sultani Decree No. 21/2024 On the Issuance of the Biometrics Law sets out requirements in relation to the collection and processing of biometric and genetic data including fingerprints, palmprints, facial and eye scans, and DNA.

### **3. COMPARATIVE ANALYSIS OF DATA PROTECTION LAWS IN SELECT GCC COUNTRIES**

#### **3.1. Data Protection Officer (“DPO”)**

**KSA Implementing Regulation, Article 32** - obligation to appoint a DPO if certain conditions are met, and definition of the DPO’s tasks.

**Bahrain PDPL, Article 10(4)** - voluntarily appointment of an “observer for data protection”, however the Board of Directors<sup>101</sup> may issue a decision requiring certain controllers to appoint one.<sup>102</sup>

**Kuwait Law** - no clearly defined DPO requirement.

**Qatar Law** - no clearly defined DPO requirement, however, the Data Privacy Impact Assessment (DPIA) Guidelines for Regulated Entities issued by the data protection authority, the Compliance and Data Protection Department (the CDP) in November 2020, states that a DPIA should be completed by a person or group of people that bring together, among others, sufficient understanding of Qatar Law No. 13/2016 requirements and data protection concepts and practices, which is often provided by a “data protection officer or champion”.

**UAE Law, Articles 10, 11 and 12** - appointment, responsibilities of the DPO and obligations of the controller and processor towards the DPO.

**Oman Law (Article 20) and Oman Executive Regulations (Chapter 7)** - appointment, tasks of the DPO and publishing DPO details.

---

<sup>101</sup> Board of Directors: The board of directors of the Authority formed in accordance with the provisions of Bahrain PDPL, Article 39.

<sup>102</sup> Bahrain PDPL, Article 10(4).

### 3.2. Cross Border Transfers (general prohibition)

**PDPL, Article 29 and Transfer Regulations** – Transfer of personal data outside the Kingdom must achieve certain purposes. These are: to perform an obligation under an agreement to which the Kingdom is a party; to serve the interests of the Kingdom; to perform of an obligation to which the Data Subject is a party; to perform necessary operation for central processing to enable the controller to conduct its activities; to provide a service or benefit to the data subject; or if it is to conduct scientific research and studies.<sup>103</sup>This is, however, subject to certain cumulative conditions including: not prejudicing national security or the Kingdom’s vital interests; adequate level of protection in the country of data export; and minimum amount of personal data transferred to what is necessary.<sup>104</sup> There are exceptions to meeting these conditions in cases of a necessity to preserve the life or vital interests of the Data Subject or to prevent, examine or treat a disease. The Transfer Regulations also set out in Article 4 specific cases in which controllers are exempt from meeting the conditions of adequate level of protection and the minimum transfer of personal data where required safeguards are implemented in specific cases e.g. adopting standard contractual clauses where the transfer or disclosure of personal data is necessary to perform central operations and the controller is part of a group of multinational entities. Further details and requirements are set out in the Transfer Regulations including the procedures and standards for evaluating the level of personal data protection outside the Kingdom, and cases which require a transfer risk assessment (and what such assessments should include).

**Bahrain Law, Article 12** – Controllers may not transfer personal data outside of Bahrain except where:

- the transfer is to a country or territory deemed adequate by the data protection authority\*; or
- the data protection authority has issued a permit for such transfer after deeming the location can provide a sufficient level of protection. Bahrain Ministerial Decision No. 42/2022 On the Transfer of Personal Data Outside the Kingdom of Bahrain sets out transfer requirements in more detail, including the submission of an application for the data protection authority’s approval to transfer.

**Kuwait Law, Article 4(7) and (9)** - Service providers are required to provide information about where personal data is stored (if inside or outside Kuwait) and to notify data owners about their intention of transferring the personal data of the data owners outside Kuwait.

---

<sup>103</sup> PDPL, Article 29(1) and the Transfer Regulations, Article 2.

<sup>104</sup> PDPL, Article 29(2).

**Qatar Law, Article 15**– A controller may not take any action or measure that may limit the processing of personal data outside the boundaries of Qatar, unless the processing would:

- violate the data protection law; or
- cause serious damage to the personal data or the individual. The NCGAA Guidelines on Data Protection Impact Assessment (“DPIA Guidelines”) considers transferring personal data outside the State of Qatar as a processing activity that may cause serious damage to individuals and requires a DPIA (section 5.1 of the DPIA Guidelines). The Personal Data Management System (PDMS) Checklist for Regulated Entities sets out the need to put appropriate safeguards in place to protect the personal data involved in transfers, unless an exception can be provided for.

**UAE Law, Articles 22 and 23** – Cross-Border transfers may only take place if:

- the country or territory to which personal data is transferred has personal data protection legislation in place that entail the key provisions, measures, controls, requirements, and rules in relation to the protection of confidentiality and privacy of the data subject’s personal data and his ability to exercise his rights, and provisions relating to the imposition of appropriate measures against the Controller or the Processor through a supervisory or judicial body; or where the UAE has entered into bilateral or multilateral agreements relating to personal data protection with jurisdictions to which personal data is transferred. This is similar to “adequacy” approaches in other data protection laws (e.g. KSA). We would note that the jurisdictions deemed adequate by the UAE data protection authority have not been confirmed or issued yet; or
- additional safeguards are adopted in relation to transfers of personal data to jurisdictions where no data protection laws exist (and which are not approved by the data protection authority). These safeguards include (without limitation) entering into standard contractual clauses, obtaining express consent from the data subject, or if the transfer is necessary to enter into or execute a contract between the controller and data subject, or between the controller and a third party to achieve the data subject's interest.

**Oman Law, (Article 23) and Oman Executive Regulations (Chapter 8)** - Without prejudice to the competences prescribed to the Cyber Defence Centre, the controller may transfer personal data outside Oman, on the basis that express consent of the data subject is obtained (other than in specific cases set out in Article 37 of the Oman Executive Regulations) and the transfer is to a third party processor with an adequate degree of protection of personal data (not less than required by Oman Law and Oman Executive Regulations) which will be conducted through an assessment (as set out in Article 39 of the Oman Regulations). Controllers are

prohibited from transferring personal data if it has been processed in violation of the provisions of Oman Law, or if it would cause harm to the data subject.

### **3.3. Prior Consultation**

**PDPL, Article 29** – There is no such specific obligation, other than a general obligation on the data controller to cooperate with the data protection authority.

**Bahrain PDPL, Article 15** – The controller should obtain the Authority’s prior written authorisation to the types of processing set out in Article 15.

**Kuwait Law** – There are no such obligation.

**Qatar Law** - There is no directly comparable provision.

**UAE Law** – There is currently no explicit provision to this effect, but the UAE Executive Regulations will likely provide further information.

**Oman Law, (Article 5) and Oman Executive Regulations (Chapter 2)** - It is prohibited to process personal data relating to genetic data, biometric data, health data, racial origin, sex life, political or religious opinions, philosophical beliefs, criminal convictions, or those relating to security measures, except after obtaining a permit for this from the ministry, in accordance with the controls and procedures set out in the Oman Executive Regulations.

### **3.4. Design and Default**

In addition to our comments in 2.1.1.4 “*Security measures*”:

**PDPL, Article 19** –Controllers must implement all the necessary organizational, administrative and technical measures to protect personal data, including during transfers, in accordance with the KSA Implementing Regulation. The KSA Implementing Regulations require (technical) measures in various provisions including ensuring prompt response to data subject requests,<sup>105</sup> avoiding the risks

---

<sup>105</sup> KSA Implementing Regulations, Article 3(1)(b).

to anonymisation,<sup>106</sup> and avoiding the impact of processing inaccurate, incomplete or outdated personal data<sup>107</sup>. Controllers may also collect only the minimum amount of personal data necessary for the purposes of the processing, by relying on appropriate means, including data maps indicating the specific needs for each type of collected data and links to the objectives of the processing.<sup>108</sup>

**UAE Law, Articles 7 and 8** – controller and processor obligations including taking appropriate technical and organizational measures.

**Oman Law, Articles 13 and 15** - Article 13 of the Oman Law sets out examples of controls and procedures to be complied with when processing personal data. The Oman Executive Regulations expands on this including under Article 26 requiring controllers to “establish, using and activating electronic systems to prevent illegal access to, leakage, tampering with or misuse of Personal Data; set systems to recover Personal Data when a physical or technical accident occurs; and the existence of processes for testing the effectiveness of its existing technical procedures.”

### **3.5. Data Protection Impact Assessment (“DPIA”)**

**PDPL (Article 22) and KSA Implementing Regulation(Article 25)** –Controllers must conduct impact assessments and document these where: (i) the processing is of sensitive data; (ii) collecting, comparing or linking personal data from different sources; (iii) the large scale or frequent processing of personal data of persons with limited or ineligible capacity, or data processing requiring the continuous monitoring of personal data subjects, or the processing of personal data using emerging technologies, or making decisions based on automated processing; and (iv) the provision of a product or service that involves the processing personal data and is likely to pose serious harm to the privacy of personal data subjects.

**Kuwait Law** – no similar DPIA requirement.

**Bahrain Implementing Regulations** - Article 3 of Bahrain Ministerial Decision No. 43/2022 Defining the Requirements to be Met in Technical and Organisational Measures to Protect Personal Data sets out instances where a DPIA is required, including in instances of automated processing, extensive processing of data, high-risk data or data related to criminal cases, systematic observation of an area widely available to the public, and data processing by visual recording or automated processing of biometric data. Article 3 also sets out what the assessment should contain.

---

<sup>106</sup> KSA Implementing Regulations, Article 9(1)(c).

<sup>107</sup> KSA Implementing Regulations, Article 22(5).

<sup>108</sup> KSA Implementing Regulations, Article 19.

**Qatar Law** - The DPIA Guidelines set out when controllers should perform DPIAs and the steps to completing one. Examples of DPIA triggers include i. technology implementations or upgrades such as collecting, storing or securing personal data in a new way ii. changes to existing processes such as processing personal data for a new use case or disclosing it to a new third party or iii. changes to product services such as developing a new product or service offering.<sup>109</sup> It also states that conducting an effective DPIA demonstrates compliance with Qatar Law , providing a record that Controllers have conducted the required review under Article 11.1 and have identified appropriate precautions to be put in place under Article 8(3) and 13 of Qatar Law and that not conducting a DPIA when one is required could lead to a fine of QAR1,000,000.<sup>110</sup>

**UAE Law, Article 21** – Before processing, controllers are required to conduct a DPIA when using any modern technologies that would pose a high risk to the privacy and confidentiality of personal data to the data subject. A DPIA is required where the processing: i. involves a systematic and comprehensive the personal aspects of a data subject based on automated processing which would have legal consequences of seriously affect the data subject; or ii: is made on a large amount of Sensitive Personal Data (as defined in the law).

**Oman Law, Article 13** – Controllers must put in place the controls and procedures required when processing personal data, including in particular the following: identifying the risks that the data subject will be exposed to as a result of the processing. As noted above, a controller is also required to conduct a transfer impact assessment (as set out in Article 39 of the Oman Executive Regulations).

## 4. CROSS-COUNTRY COMPARISON AND COMMON TRENDS

### 4.1. Overview of Similarities

- 1. Protection of personal information:** All GCC countries emphasize the protection of personal information and establish guidelines on how organizations should handle and process such data.
- 2. Consent requirements:** Consent is generally required for the collection, use, and disclosure of personal information. GCC countries often have provisions that specify the conditions under which consent must be obtained and the rights of individuals to withdraw their consent.

---

<sup>109</sup> Appendix A – Example DPIA Triggers, DPIA Guidelines.

<sup>110</sup> DPIA Guidelines, Sections 3 and 5.

**3. Security measures:** All GCC countries have introduced requirements on organizations to ensure the security of personal data by implementing appropriate technical and organizational measures to protect against unauthorized access, loss, or disclosure.

**4. Rights of data subjects:** Data protection laws in the GCC typically recognize the rights of individuals, such as the right to access their personal information, request correction or erasure of data, and lodge complaints if their rights are violated.

**5. Cross-border data transfers:** GCC countries have regulations governing the transfer of personal data outside their jurisdictions, generally requiring organizations to ensure adequate safeguards are in place when transferring data to countries that do not provide an equivalent level or protection.

#### ***4.1.1. Overseeing and enforcing data protection laws and regulations***

**KSA:** The principal authority in charge of overseeing and enforcing these rules is the SDAIA.

**Bahrain:** The Data Protection Authority (“**DPA**”) is responsible for overseeing and enforcing data protection laws and regulations in Bahrain. The DPA plays a vital role in monitoring compliance with the Bahrain PDPL and ensuring that organizations adhere to their obligations.

The DPA provides guidance and support to organizations to help them understand their data protection obligations and implement effective practices. They offer educational resources, conduct workshops, and provide assistance in developing data protection policies and procedures. In addition, the DPA has the power to conduct investigations into organizations' data processing activities. It can request information, carry out audits, and interview individuals involved in the processing of personal data. If the DPA identifies any violations of the law, it has the authority to impose penalties on non-compliant organizations. The penalties for non-compliance can include fines, warnings, or orders to rectify the violation. The DPA strives to ensure that organizations take data protection seriously and comply with the law to protect individuals' personal data. Overall, the DPA's role is crucial in overseeing and enforcing data protection laws and regulations in Bahrain. It works to raise awareness, provide guidance, and take enforcement actions to promote compliance and protect individuals' privacy rights.

**Kuwait:** The Communications and Information Technology Regulatory Authority (“**CITRA**”) was established under Law 37 of 2014. CITRA introduced the Kuwait Law which imposes regulatory requirements on Service Providers licensed by the CITRA.

**Qatar:** The NCSA was established by Qatar Emiri Decision No. 1/2021 Establishing the National Agency for Cybersecurity (“**Decision No. 1/2021**”) and the NCGAA of the NCSA is the responsible data protection authority in Qatar.

**Oman:** The Ministry of Transport, Communications, and Information Technology (“**MTCIT**”) is the responsible data protection authority in Oman, which oversees compliance with the Oman Law and Oman Executive Regulations.

**UAE:** The UAE Law makes reference throughout to the “Office” which is defined as the UAE Data Office established by Federal Decree-Law No. 44/2021 On the Establishment of the Emirates Data Office (“**Law No. 44/2021**”). In the interim, and for the purposes of operating the UAE Data Office in the first two years of its work, the Telecommunications and Digital Government Regulatory Authority (“**TDRA**”) has been appointed to provide the UAE Data Office with administrative and logistic support.<sup>111</sup> Our understanding is, however, that the UAE Data Office is not fully set up and the UAE Law, although in force, is not actively being enforced by either authority. As set out in 1.3 of this paper, companies are required to "regularise their status" in accordance with the UAE Law within 6 months from the date of issuance of UAE Executive Regulations.<sup>112</sup> The UAE Executive Regulations have, however, not been issued yet.

#### ***4.1.2. Promoting awareness and compliance***

**KSA:** Among other relevant tasks, the SDAIA has been in charge of promoting awareness and compliance in this, still quite new, regulatory area in the KSA. For example, on the day of the PDPL's entry into force, SDAIA launched a national awareness campaign, in cooperation with other government entities, to familiarize the Saudi public with the rights and obligations flowing from the new personal data regime in the KSA.

**Bahrain:** The DPA promotes awareness and compliance through various means. It engages in educational initiatives to raise awareness about data protection laws and regulations. This may include organizing seminars, workshops, and training programmes for organizations and individuals to understand their rights and obligations. Additionally, the DPA may publish guidelines, codes of practice, or other informative material to provide practical guidance on complying with data protection laws. These resources can help organizations understand best practices for data handling, storage, and security. The DPA also collaborates with other government agencies, industry associations, and international organizations to share information and exchange experiences on data protection. This collaboration helps to establish a network of support and expertise in promoting compliance and addressing emerging challenges in the field. Furthermore, the DPA encourages organizations to adopt privacy-enhancing technologies and practices to protect personal data. They may provide incentives or recognition for organizations that demonstrate exceptional data protection measures. Overall,

---

<sup>111</sup> Law No. 44/2021, Article 9.

<sup>112</sup> UAE Law, Article 29.

the DPA takes a proactive approach to promote awareness and compliance by combining education, guidance, collaboration, and technological advancements.

**Kuwait:** The CITRA may issue instructions or guidance regarding the privacy of the data whenever necessary to ensure compliance with the Kuwait Law.

**UAE:** Please see the UAE analysis above, in 4.1.1 *“Overseeing and enforcing data protection laws and regulations”*.

**Oman:** The Oman Law sets out the responsibilities the MTCIT has for implementing the Oman Law - which do not prejudice the competencies of the Cyber Defense Centre. Such responsibilities include verifying compliance of the controller and processor against the necessary controls and procedures for processing personal data (issued by MTCIT).<sup>113</sup> Please also see Oman analysis in *“4.2.6. Cultural and societal factors”*.

**Qatar:** Unlike other laws, the Qatar Law does not set out the powers, responsibility, or role of the NCGAA, although it does list the penalties for non-compliance of the Qatar Law. Nonetheless, Decision No. 1/2021 gives the NCSA the power to implement laws, regulations and decisions related to protecting the privacy of personal data.<sup>114</sup>

#### ***4.1.3. Handling complaints and investigations***

**KSA:** Any person affected as a "data subject" may submit to SDAIA a complaint relating to the PDPL's implementation. The deadline to do this is, as a rule, 90 days of the data protection incident concerned or the data subject's becoming aware of it,<sup>115</sup> and the Executive Regulations prescribe the minimum contents of such complaints. SDAIA has the power to take the necessary measures regarding any complaint it receives and notify the complainant of its outcome.

**Bahrain:** This is governed by Order No. (49) of 2022, with respect to the rules and procedures governing submission of complaints regarding violations of the Bahrain PDPL. The DPA handles complaints and investigations in a systematic manner. When a complaint is received, the DPA will assess its validity and determine if it falls within its jurisdiction. If the complaint is deemed valid, the DPA will initiate an investigation. During the investigation process, the DPA has the power to request information from the organization involved, conduct audits, and interview individuals who are relevant to the case. It may also gather any evidence necessary to support

---

<sup>113</sup> Oman Law, Article 7.

<sup>114</sup> Decision No. 1/2021, Article 3(21).

<sup>115</sup> PDPL, Article 34; Executive Regulations, Article 37.

its investigation. Once the investigation is complete, the DPA will analyze the findings and determine if any violations of data protection laws have occurred. If violations are identified, the DPA has the authority to impose penalties on the non-compliant organization. These penalties can include fines, warnings, or orders to rectify the violation.

Throughout the process, the DPA maintains confidentiality and protects the rights of both the complainant and the organization being investigated. They strive to handle complaints and investigations impartially and in a timely manner. It is worth noting that the specific procedures and guidelines followed by the DPA may be subject to change.

**Kuwait:** In the event of a proven violation of the provisions of these regulations or the laws of the State of Kuwait, the CITRA may apply the penalties and fines stipulated under Law No. 73 of 2014 establishing the Communications and Information Technology Regulatory Authority as amended by Law No. (98) of 2015.

**UAE:** Law No. 44/2021 sets out (among other things) the powers of the UAE Data Office including conducting investigations to ensure compliance with UAE Law and receiving complaints.<sup>116</sup> Under the UAE Law, data subjects have the right to file a complaint with the UAE Data Office for any violation of the law. The UAE Data Office will then verify such complaints with the controller and processor and impose any penalties. Grievance against any decision may be submitted to the Office General Manager within 30 days from the date of being notified of the decision. It is expected that the UAE Executive Regulations will provide further detail on the procedures for filing a grievance.

**Oman:** Chapter 9 of the Oman Executive Regulations set out the complaints and penalties procedure. A data subject or any other interested person can file a complaint to MTCIT about a violation of the Oman Law or Oman Executive Regulations within a maximum of 30 days from the date of knowledge of the violation, provided that MTCIT gives a copy of the complaint to the controller within 7 days of its submission. The Controller has the right to respond to the complaint within 14 days from notification. MTCIT will come to a decision within 60 days of the controller's response and can issue penalties. Grievance following the issuance of penalties by MCTIT is permitted.

**Qatar:** Some of the NCGAA's strategic objectives in relation to data privacy include receiving and responding to complaints about misuse of personal data and investigating and issuing penalties to companies.<sup>117</sup> Individuals may lodge complaints with NCGAA for violation of the Qatar Law. The NCGAA, after investigating and establishing its seriousness, may issue a decision requiring the controller or processor to remedy the violation within a specified time frame. A grievance against this decision may be submitted within 60 days

---

<sup>116</sup> Law No.44/2021, Article 3.

<sup>117</sup> [Personal Data Privacy | National Cyber Governance and Assurance Affairs \(ncsa.gov.qa\)](#)

of the notification which the NCSA will examine within 60 days from the filing date. The NCGAA's decision on the grievance will then be final.<sup>118</sup> Controllers are also required to establish internal systems to receive complaints.<sup>119</sup> The NCGAA Guidelines, specifically Individuals' Complaints, further explain what individuals can submit a claim about and how the NCGAA manages complaints (among other things).

#### ***4.1.4. Establishing guidelines and standards***

**KSA:** The organizational structure of SDAIA includes a National Data Management Office (NDMO), which is entrusted with the tasks of establishing data policies and standards, developing data governance mechanisms, monitoring compliance with data policies and standards, and developing data management and protection capabilities. The NDMO's remit therefore extends to data management and is not limited to personal data protection. As part of its tasks prior to the adoption of the PDPL, NDMO issued Data Management and Personal Data Protection Standards<sup>120</sup>, for adoption by all KSA public entities and any business partners handling government data. SDAIA has also issued various procedure manuals, guidelines and rules including Rules for Appointing Personal Data Protection Officer and Risk Assessment Guideline for Transferring Personal Data Outside the Kingdom. These are available on the Knowledge Center of the National Data Governance Platform along with e-Services such as for Personal Data Breach Notification, Reports and Complaints and tools such as DPO Appointment Guiding Tool.

**Bahrain:** The DPA established guidelines and standards through a collaborative process involving various stakeholders. Some key steps are:

- **Research and Analysis:** The DPA conducts research and analysis to understand the current data protection landscape, including local and international best practices. This helps identify areas where guidelines and standards are needed.
- **Stakeholder Engagement:** The DPA engages with relevant stakeholders, such as industry associations, professional bodies, government agencies, and the public, to gather input and insights. This collaborative approach ensures that diverse perspectives are considered in the development of guidelines and standards.

---

<sup>118</sup> Qatar Law, Article 27.

<sup>119</sup> Qatar Law, Article 11(4).

<sup>120</sup> Version 1.5, January 2021.

- **Consultation and Feedback:** The DPA may hold consultations or seek public feedback on draft guidelines and standards. This allows interested parties to provide their input and helps ensure that the final guidelines and standards are comprehensive and practical.
- **Review and Revision:** The DPA reviews the feedback received from consultations and refines the guidelines and standards accordingly. It takes into account any new developments or changes in data protection laws and regulations.
- **Publication and Dissemination:** Once finalized, the guidelines and standards are published and made available to the public.

**Kuwait:** The CITRA sets forth guidelines and standards through a cooperative effort involving diverse stakeholders. Several pivotal stages include:

- Data Classification
- Personal Data Collection and Processing Conditions
- Security and Protection of Personal Data for Service Providers
- Notification Procedure in the Event of Breaches to Personal Data
- Violating Content Rules

**UAE:** Please see the UAE analysis above, in 4.1.1. Accordingly, no guidance has been issued yet, although the UAE Data Office has responsibilities under Law No. 44/2021 to issue handbooks and instructions necessary for the implementation of the UAE Law as well as to raise awareness of data protection requirements by organizing conferences, forums, workshops, etc.<sup>121</sup>

**Oman:** The MTCIT has issued policies, frameworks, guidelines, and standards around IT Governance. More recently, MTCIT issued a personal data protection policy for governmental entities through Circular 6/2024 Regarding the Personal Data Protection Policy of the Units of the Administrative Apparatus of the State (given the Oman Law does not apply to the processing of personal data by government entities).

---

<sup>121</sup> Law No.44/2021, Article 3.

**Qatar:** The NCGAA has published guidelines for regulated entities as well as for individuals including the DPIA Guidelines, Personal Data Management System (PDMS) Checklist and Individual’s Rights Guidelines, as previously referred in this paper. Its strategic objectives in relation to data privacy also include increasing awareness of privacy rights among individuals and companies and updating guidance on privacy around emerging technologies; and issuing data protection policies for controllers.<sup>122</sup>

#### **4.1.5. Collaboration**

**KSA:** See “Powers and enforcement capabilities” section.

**Bahrain:** The DPA collaborates with other government agencies and organizations within Bahrain to address specific data protection challenges or concerns. This can involve sharing resources, expertise, and knowledge to ensure the effective implementation and enforcement of data protection laws. The DPA may engage in collaborations with industry stakeholders, such as businesses and technology companies, to promote awareness and compliance with data protection regulations. It also includes providing guidance, conducting trainings, and facilitating discussions to enhance understanding and cooperation in protecting personal data. Collaboration plays a vital role in the overall functioning of the DPA as it helps in fostering a coordinated and comprehensive approach to data protection, ensuring the rights and privacy of individuals are upheld.

**Kuwait:** Currently, the CITRA is an active telecommunications regulator.<sup>123</sup> The CITRA has the option to initiate partnerships with industry stakeholders, including businesses and technology firms, to encompass activities such as offering guidance, delivering training sessions, and facilitating dialogues to improve comprehension and collaboration in safeguarding personal data. With time, we will see its collaboration efforts in terms of data protection.

**UAE:** Please see the UAE analysis above, in 4.1.1. The UAE Data Office, once set up, will also be involved in “proposing joining international treaties and agreements or signing them, and proposing partnership agreements with Gulf, regional, and international

---

<sup>122</sup> [Personal Data Privacy | National Cyber Governance and Assurance Affairs \(ncsa.gov.qa\)](#)

<sup>123</sup> For example, actively engages with both regional and international telecommunications organizations (Arab Regulators Network of Telecommunication & Information Technologies (ARNET), the Asia Pacific Top-Level Domain Association (APTLD), the Governmental Advisory Committee (GAC) in The Internet Corporation for Assigned Names and Numbers (ICANN), and the Regional Internet Registry for Europe Network Coordination Centre (RIPE NCC)), while also cultivating strong relationships with fellow regulators. International Affairs plays a pivotal role in CITRA's goals and strategies by harnessing the expertise of global organizations like the ITU and the Arab Regulators Network to offer valuable international benchmarks and best practices applicable to Kuwait. The CITRA holds sector membership in the International Telecommunications Union (ITU) across all three sectors: radio communication, telecommunication standardization, and telecommunication development.

countries, organizations, and bodies relevant to the Bureau’s activities and terms of reference, or signing them, in coordination with the Ministry of Foreign Affairs and International Cooperation and other concerned bodies” .<sup>124</sup>

**Oman:** The MTCIT is also responsible for cooperating with personal data protection authorities in other countries as well as “providing advice, support and coordination with the units of the administrative apparatus of the State and other public legal persons in any matter related to the Personal Data protection.” <sup>125</sup>

**Qatar:** The NCGAA’s strategic objectives include “engaging with industry sector groups effectively to increase standard of data protection practices and participating actively in international privacy communities.”<sup>126</sup>

#### ***4.1.6. Support and guidance***

**Bahrain:** The DPA provides support and guidance in various ways. Firstly, the DPA offers resources on its website, including guidelines and templates, to help individuals, organizations, and government agencies understand and comply with data protection laws. Secondly, the DPA may provide direct support through its helpline or personalized consultations. Individuals or organizations on specific data protection matters, seek guidance on best practices, or report any concerns or breaches. Furthermore, the DPA conducts awareness campaigns and educational programmes to promote understanding and compliance with data protection regulations. This may involve organizing workshops, seminars, or webinars to educate individuals and organizations on their rights and obligations regarding personal data. Overall, the DPA aims to provide comprehensive support and guidance to individuals and organizations, ensuring they have the necessary tools and knowledge to protect personal data and comply with data protection laws.

**Kuwait:** The CITRA prepares and offers different resources and general guideline on its website to support individuals, organizations and government agencies understand and comply with data protection laws. Moreover, the CITRA provides an avenue for individuals and entities interested in voicing their opinions prior to the adoption of any regulatory framework affecting the telecommunications and information technology sector. These comments and suggestions are thoroughly reviewed before the official release of the document, allowing all interested parties the opportunity to submit their input within the specified deadline. As one of the most important activities, the CITRA has instituted the Information Security and Emergency Response Department, aligning with the

---

<sup>124</sup> Law No. 44/2021, Article 3(10).

<sup>125</sup> Oman Law, Article 7.

<sup>126</sup> [Personal Data Privacy | National Cyber Governance and Assurance Affairs \(ncsa.gov.qa\)](#).

principles outlined in the National Cybersecurity Strategy. This department holds authority over cybersecurity matters and responsibilities on a national scale, possessing the requisite powers to fulfil its mandate effectively.

**KSA:** SDAIA’s duties include building specialized national expertise and capabilities in the data and AI sectors, adopting professional standards, and building standards, professional tests, and educational and training programs in those fields, implementing them, and coordinating with the Ministry in those matters. It is also responsible for raising awareness of relevant policies, provisions of laws, regulations and decisions. Further, as reported by SDAIA, it has introduced several specific initiatives to serve society, including the “Ehsan” platform, which aims to promote charitable and developmental work in the Kingdom, in addition to its role in raising the quality of community life through the use of innovative digital technologies and platforms. From a data protection perspective, please note the SDAIA guidance mentioned above in “4.1.4. Establishing guidelines and standards”.

**UAE:** Please see our comments above in “4.1.4. Establishing guidelines and standards”.

**Oman:** Please see our comments above in “4.1.4. Establishing guidelines and standards”.

**Qatar:** Please see our comments above in “4.1.4. Establishing guidelines and standards”.

#### ***4.1.7. Audit and assessments***

**KSA:** The SDAIA may grant licenses to entities that plan to issue accreditation certificates to data controllers and data processors or those conducting audits or checks of personal data processing and data controller’s activities in particular.<sup>127</sup>

**Bahrain:** The Authority is required to prepare an annual report that outlines its activities and operations from the previous financial year. This report should highlight the achievements of the Authority, any challenges it faced and how they were overcome, as well as any suggestions or recommendations for maintaining data protection and other important matters. The full report, along with the audited closing accounts for the financial year, will be published within four months of the end of the financial year. Both an English and Arabic version of the abstract of the report and closing account will be approved by the Board and made available to the public.

**Kuwait:** The Service Provider is required to conduct comprehensive audits and reviews to the extent of protecting personal data.

---

<sup>127</sup> PDPL, Article 33 and Executive Regulations, Article 36.

Also, all service providers or such parties licensed to own public communication networks shall reconcile their status with the provisions of these regulations and other related regulations issued by the CITRA within a period not exceeding one year from the date of publication.

**UAE:** There is limited information on auditing and assessment under the UAE Law, and the UAE Executive Regulations, once issued, may provide further information on this. For completeness, we would note that under Article 11, the DPO is responsible for (among other things) verifying the quality and validity of the procedures adopted by the controller and processor.

**Oman:** Under the Oman Law and Oman Executive Regulations, controllers and processors are required to appoint (upon request of MTCIT) a licensed and independent external auditor or Verifier (as reference to in the Oman Executive Regulations) to ensure processing is in accordance with the Oman law and Oman Executive Regulations. A report from the external auditor should be provided to MTCIT within 60 days from the date of appointing the external Verifier.

**Qatar:** There is limited information on auditing and assessment under the Qatar Law, however controllers are required to conduct a comprehensive audit and review of its operations and compliance with the protection of personal data.<sup>128</sup> The NCGAA Guidelines also set out the importance of audit provisions in contracts with third party processors.

#### ***4.1.8. Penalties and sanctions***

**KSA:** The PDPL prescribes a penalty of imprisonment of up to two years and/or a fine of up to three million Riyals against violations of its provisions if these concern the disclosure or publication of Sensitive Data with the intention of harming the data subject or obtaining a personal benefit.<sup>129</sup> Penalties may be doubled in cases of repeated violations. "Sensitive Data" include personal data revealing racial or ethnic origin; religious, intellectual or political belief; security criminal convictions and offenses; biometric or genetic data for the purpose of identifying the person; health data; and data that indicates that one or both of the individual's parents are unknown.<sup>130</sup> Less serious violations of the PDPL than those mentioned above are punishable by a warning or a fine of up to five million Riyals, which may be doubled in the event of a repeat violation.

---

<sup>128</sup> Qatar Law, Article 11(7).

<sup>129</sup> PDPL, Article 35.

<sup>130</sup> PDPL, Article 1(11).

**Bahrain:** The Bahrain PDPL provides for both civil and criminal penalties. In terms of civil liability, the Law provides that anyone who suffers damage resulting from the processing of his data may seek compensation from the data controller or the Data Protection Guardian<sup>131</sup> if such processing breaches the provisions of the Law.

The Bahrain PDPL (Article 58) stipulates that in the event of the commission of certain offences, a natural person<sup>132</sup> could be liable to imprisonment for a term not exceeding one year and/or a fine of not less than BD 1,000 and not exceeding BD 20,000. These offences include:

- Processes sensitive personal data without obtaining the consent of the data subject;
- Transferring data outside the Kingdom of Bahrain in breach of Articles 12 and 13 of the Bahrain PDPL;
- Provides the Authority or data subjects with incorrect or misleading data;
- Withholds from the Authority any information, records, documents, or data;
- Disrupting the work of the Authority's inspections or investigations; or
- Discloses any information available to her/him by virtue of their work for their personal benefit.

**Kuwait:** The Authority may, in the event of a violation of the provisions of this Regulation or the laws of the State of Kuwait, impose the penalties and fines stipulated in Kuwait Law No. 37/2014 on the Establishment of the Communication and Information Technology Regulatory Authority (CITRA), as amended by Kuwait Law No. 98/2015.

The CITRA will have the authority to apply the penalties under the Telecom Law for any violation of the Telecom Law and/or the Data Privacy Protection Regulations in addition to the penalties set out in the Combating Cyber Crimes Law.

---

<sup>131</sup> Under Bahrain PDPL (Article 10), the concept of Data Protection Guardian has been introduced. The DPG is tasked with duties that are not too dissimilar to those of the Data Protection Officer under the GDPR.

<sup>132</sup> Bahrain PDPL, Article 59 allows for the possibility of Corporate Criminal Responsibility, in which case the amounts of the penalties are double those applicable to natural persons.

**UAE:** Article 26 of the UAE Law explains that a Cabinet decision will set out the acts that constitute a violation of the UAE Law and UAE Executive Regulations and the administrative penalties imposed. Our understanding is that this decision has not yet been issued. We know, for example under the UAE Law, that the UAE Data Office can impose penalties for personal data breaches.<sup>133</sup>

**Oman:** The Oman Executive Regulations set out the administrative penalties the Ministry of Transport, Communications, and Information Technology may impose for violations of the Oman Law and Oman Executive Regulation including issuing warnings; suspending permits until the violation is corrected or revocation of the permit; and fining up to OMR 2,000 per violation (approx. USD \$5,200).<sup>134</sup>

**Qatar:** Chapter 7 of the Qatar Law sets out the penalties for violation of the law which are without prejudice to any greater penalty in any other law. The penalties in the Qatar Law range from 1,000,000 Qatari Riyals (approx. USD\$ 274,100) for violations of processing personal data without consent or Legitimate Purpose, violations of various controller obligations such as not informing individuals of the information (set out in Article 11 of the law) before processing their personal data (e.g not having a privacy policy in place), and for not adhering to cross-border data flows (i.e international transfer) requirements, to 5,000,000 Qatari Riyals (approx. USD\$ 1,370,500) for violations including the requirements for electronic websites catered to children (Article 17). Juristic persons who commit the crime in its name and for its account can also be liable up to 1 million Qatari Riyals.

## **4.2. Overview of Differences**

### **4.2.1. Governance structure**

**KSA:** Any policy, legislation, SDAIA's budget and other important matters must be approved by SDAIA's Board of Directors.<sup>135</sup> The Board's Chairman<sup>136</sup> is appointed by the Council of Ministers, and the other members are appointed by the Prime Minister. The Board's Chairman appoints SDAIA's president who is generally responsible for managing the SDAIA's affairs.

**Bahrain:** The DPA is governed by a Board, which is responsible for overseeing the organization's operations and decision-making processes. The Board consists of a Chairman and several members who are appointed by a royal decree. The Chairman is usually a high-ranking government official with expertise in data protection or related fields. The Board sets the strategic direction and policies

---

<sup>133</sup> UAE Law, Article 9(4).

<sup>134</sup> Article 44, Oman Executive Regulations.

<sup>135</sup> Id., Article 6.

<sup>136</sup> The current Chairman of the SDAIA Board is His Royal Highness Prince Mohammed bin Salman bin Abdulaziz Al Saud, Crown Prince and Prime Minister.

of the Authority, ensuring that it operates effectively in fulfilling its mandate. It also reviews and approves the guidelines and standards developed by the Authority, as well as any amendments or updates to these documents. The Authority's day-to-day operations are managed by an executive team, led by the Chief Executive Officer (“CEO”). The CEO is responsible for implementing the Board's decisions and overseeing the Authority's activities. The CEO is supported by various departments, such as legal, compliance, technical, and communication, which work together to carry out the Authority's functions. Overall, the governance structure of the Bahrain Data Protection Authority ensures transparency, accountability, and effective decision-making in protecting individuals' data and promoting a culture of privacy in Bahrain.

**Kuwait:** CITRA was established in 2014 and is responsible for overseeing the telecommunications sector, monitor and protect the interests of users and service providers and regulate the services of telecommunication networks in the country, while ensuring transparency, equality of opportunity and fair competition. The list of Laws of CITRA concerning the establishment in addition to its executive regulations issued by the authority:

- The Executive Regulations of Law No. 37 of 2014 regulating the establishment of the Communication and Information Technology Regulatory Authority
- Law No. 98 of the Year 2015 Amending some Provisions of the Law 37 of 2014 on the Establishment of Communication and Information Technology Regulatory Authority (CITRA)
- Law No. 37 of 2014 on the Establishment of Communication and Information Technology Regulatory Authority

CITRA Board of Directors comprises the ICT professionals:

- Chairman and CEO
- Vice-Chairman of the Communication and Information Technology Regulatory Authority and 3(three) Board Members

CITRA's Executive Management team consists of the ICT experienced individuals:

- Chief of Administrative and Financial Affairs Sector
- Chief of Market and Regulation Competition Affairs (MRC)

- Chief of Telecommunications Sector
- Chief of Information Technology Sector

Some of CITRA's primary functions include:

- Protecting consumer affairs
- Regulating services, tariffs, and rates within the ICT sector
- Encouraging competition and investment in the ICT sector and preventing unfair competition
- Regulating and licensing telecommunications services

CITRA oversees four ICT subsectors, and they are:

- Telecommunications Sector
- Operators and Fair Competition Sector
- Information Technology (IT) Sector
- Administrative and Financial Affairs Sector

**UAE:** Please see the UAE response in 4.1.1 *“Overseeing and enforcing data protection laws and regulations”*.

**Oman:** Please see the Oman response in 4.1.1 *“Overseeing and enforcing data protection laws and regulations”*. The MTCIT was established by Oman Sultani Decree No. 90/2020 Establishing the Ministry of Transport, Communications, and Information Technology, Determining Its Competences, and Adopting Its Organisational Structure. MTICT offers information technology services

and has developed various projects such as for national IT infrastructure (e.g National Program for AI & Advances Technologies<sup>137</sup>) and information security (such as the launch of Oman CERT to analyse and raise awareness on cybersecurity threats (and protections)<sup>138</sup>).

**Qatar:** Please see the Qatar response in 4.1.1 “*Overseeing and enforcing data protection laws and regulations*”. The NCGAA has various responsibilities separate from ensuring compliance with the Qatar Law. These responsibilities focus on cybersecurity and include developing cybersecurity policies, legislations, standards and controls, executing National Cyber Security Drills, setting standards for accrediting and issuing certificates to cybersecurity service providers, and issuing cyber security assurance certificates for devices, systems, and applications in accordance with national and international frameworks and standards.<sup>139</sup>

#### **4.2.2. Scope of applicability**

**KSA:** The PDPL applies to the processing of any personal data (i) that takes place in the Kingdom or (ii) is carried out outside the Kingdom but relates to individuals that reside in the Kingdom. The scope of the data protected also includes data of deceased persons if their processing leads to their or a member of their family being individually identified.<sup>140</sup> Its provisions do not apply to the processing of personal data by individuals merely for personal or family use purposes.

**Bahrain:** The Bahrain PDPL shall apply to processing of data by total or partial automatic means and the processing by non-automatic means of data which form part of a filing system or are intended to form part of a filing system. Additionally, the DPL applies to every natural person who is habitually resident in Bahrain or maintains a place of business in Bahrain, every legal person with a place of business in Bahrain, and every natural or legal person not habitually resident nor maintains a place of business in Bahrain, but processes data by using means situated in Bahrain, unless such means are used only for purposes of transit of data over Bahrain’s territory. Every legal person must appoint a representative who is authorized on his behalf to undertake obligations in Bahrain as set out under the Bahrain PDPL and shall immediately notify the Authority about such appointment and all amendments thereof. This appointment shall not preclude any legal recourse that could otherwise be initiated by the Authority or others against the data controller upon the data controller’s violation of any of his specified duties. The provisions of the Bahrain PDPL shall not apply to the processing of data undertaken by any individual for the sole purposes of this individual’s personal or family affairs and the processing operations concerning public security handled by the Ministry of Defence, Ministry of Interior, National Guard, National Security

---

<sup>137</sup> [Ministry of Transport, Communications and Information Technology \(mtcit.gov.om\)](http://mtcit.gov.om)

<sup>138</sup> [Ministry of Transport, Communications and Information Technology \(mtcit.gov.om\)](http://mtcit.gov.om)

<sup>139</sup> [National Cyber Governance and Assurance Affairs \(ncsa.gov.qa\)](http://ncsa.gov.qa)

<sup>140</sup> PDPL, Article 2.

Service, or other security body in Bahrain. Please note that the provisions of the Bahrain PDPL do not prejudice any duties of confidentiality in relation to the Bahrain Defence Force matters.

**Kuwait:** The Kuwait Law applies to all service providers<sup>141</sup>, licensed by the CITRA, who collect, process and store personal data and user data in whole or in part, either permanently or temporarily using automated means or any other means that are part of a data storage system, whether processing occurs inside or outside the State of Kuwait.

The Kuwait Law does not apply to practices related to security investigations, monitoring of violations, or practices violating the laws, decisions, judicial rulings, or financial claims arising from the subscription contract.

**UAE:** The UAE Law has extra-territorial application by capturing the processing of personal data by any:

- “Data Subject who resides or has a place of business in the State.
- Controller or Processor located in the State who carries out the activities of Processing Personal Data of Data Subjects inside or outside the State.
- Controller or Processor located outside the State who carries out the activities of Processing Personal Data of Data Subjects inside the State.”<sup>142</sup>

The application of the UAE has various exceptions including (without limitation) to government data, government authorities that control or process personal data, health personal data and banking or credit personal data subject to legislation around the protection and processing of personal data, as well as companies located in freezones subject to legislation on personal data protection (i.e DIFC and ADGM).<sup>143</sup> The UAE Data Office may also exempt Establishments<sup>144</sup> which do not process large amounts of personal data from all or some of the UAE Law.

---

<sup>141</sup> Service Provider is defined in the Kuwait Law as “*The person licensed to provide one or more telecommunication services to the public or licensed to manage, establish or operate a telecommunication network or internet service to provide telecommunication services to the public. This includes providers of information or content through the telecommunication network.*”

<sup>142</sup> UAE DP Law, Article 2(1).

<sup>143</sup> UAE Law, Article 2(2).

<sup>144</sup> Establishment: Any company or sole proprietorship established inside or outside the State, including companies which the federal or local government partially or wholly owns or has a shareholding therein.

**Oman:** The Oman Law applies to personal data that is processed<sup>145</sup> however sets out numerous exceptions including where processing personal data is for: <sup>146</sup>

- “a. Protection of the national security or the public interest;*
- b. Performance by the units of the administrative apparatus of the State and other public legal persons of the competencies prescribed for them by law;*
- c. Performance of a legal obligation imposed on the Controller under any law, judgment or decision of a court;*
- d. Protection of the economic and financial interests of the State;*
- e. Protection of a vital interest of the Personal Data Owner;*
- f. Detection or prevention of any criminal offense based on an official written request from the investigation authorities;*
- g. Executing a contract to which the Personal Data Owner is a party;*
- h. If the Processing is in a personal or family context;*
- i. The purposes of historical, statistical, scientific, literary or economic research, by the authorities authorized to carry out such works, provided that no indication or reference related to the Personal Data Owner is used in the research or statistics they publish, to ensure that Personal Data is not attributed to an identified or identifiable natural person; or*
- j. If the data is available to the public in a manner that does not violate the provisions of this Law.”*

**Qatar:** The Qatar Law applies to the electronic processing of personal data, or personal data obtained, collected, or extracted in any other manner as a preliminary step to be processed electronically, or personal data processed in combination between electronic processing and traditional processing. The Qatar Law, however, does not apply to personal data processed i. by individuals in connection with personal or family matters; or ii. with the aim to obtain official statistical data according to Qatar Law No. 2/2011 on

---

<sup>145</sup> Oman Law, Article 2.

<sup>146</sup> Oman Law, Article 3.

The Official Statistics (as amended by Qatar Law No. 4/2015).<sup>147</sup> Unlike the UAE Law, it is unclear whether the Qatar Law has extra-territorial application or whether it just applies to controllers located in Qatar. We have seen commentary online with both interpretations.

### **4.2.3 Legal framework**

**KSA:** With the adoption of the PDPL, which entered into force on 14 September 2023, KSA now has a first full set of legislative rules in this domain. The PDPL is complemented by the KSA Implementing Regulations and Transfer Regulations. All parties concerned have one year to ensure compliance of their operations with the new personal data protection regime.

**Bahrain:** The Bahraini legislature issued Law No. (30) of 2018 on 19 July 2019, with respect to personal data protection. Bahrain PDPL aims to protect the rights and freedoms of individuals and their personal data, by establishing a legal framework that defines the methods and means of processing data in a way that gives individuals confidence in all matters concerning their data handled by companies and organizations, and to be managed in an accurate, up-to-date, and secure manner. The Bahrain PDPL came into effect on 1 August 2019. The Ministry of Justice, Islamic Affairs and Waqf was designated, by Royal Decree No. (78) of 2019, to assume the duties of the Data Protection Authority. The Bahrain PDPL sets out the rights and obligations of data controllers and data subjects. It defines personal data and sensitive personal data and outlines the conditions for lawful processing of such data. The Bahrain PDPL also establishes principles for data protection, including transparency, purpose limitation, data minimization, accuracy, storage limitation, and security. The Bahrain PDPL includes measures for data breach notification, consent requirements, and the rights of data subjects, such as access to information, rectification, erasure, and objection to processing. It also includes provisions on international data transfers and the appointment of a data protection officer by certain organizations. Violations of the Bahrain PDPL can result in administrative fines, penalties, and other enforcement measures. The DPA has the authority to investigate complaints, carry out inspections or audits, and impose sanctions for non-compliance. Overall, the legal framework of the DPA is designed to ensure the protection of personal data and safeguard individuals' privacy rights in Bahrain.

**Kuwait:** In April 2021, CITRA introduced Regulation No. 42 of 2021, titled the Data Privacy Protection Regulation, which was abrogated by the Kuwait Law. This development represented a significant turning point in Kuwait's legal framework. Notably, prior to the enactment of this Regulation No. 42 of 2021, Kuwait lacked a dedicated data protection law or regulation. Consequently, the legal framework relied on a sparse set of pertinent provisions scattered across various legislations, including the 1962 Constitution of Kuwait and Law No. 20 of 2014 concerning Electronic Transactions.

---

<sup>147</sup> Qatar Law, Article 2.

The following legislative acts are used to specify various aspects of the Regulation:

- Kuwait Decision No. 42/2021 On the Data Privacy Protection Regulation as amended by virtue of Article 1 of Kuwait Decision No. 244/2023, Article 7(3);
- Kuwait Law No. 37/2014 On the Establishment of the Telecommunications and Information Technology Regulatory Authority, Chapters 10 to 11;
- Kuwait Law No. 63/2015 On Combating Cyber Crimes, Chapter 2, Articles 2-21; and
- Kuwait Law No. 1 of 1970 Organizing Postal Works Articles 34-35 Welcome to Ministry of Communications ([moc.gov.kw](http://moc.gov.kw)).

**UAE:** Before the UAE Law, there was no standalone data protection law in the UAE. As set out in section 1.3 of this paper, companies are required to "regularise their status" in accordance with the UAE Law within 6 months from the date of issuance of UAE Executive Regulations. The UAE Executive Regulations have, however, not been issued yet. Companies should not only consider their obligations under the UAE Law, but also any criminal laws such as Federal Decree-Law No. 31/2021 on the Issuance of the Crimes and Penalties Law and Federal Decree-Law No. 34/2021 - Concerning the Fight Against Rumors and Cybercrime, or other sector-specific or emirate specific-laws with data protection requirements.

**Oman:** The Oman Executive Regulations added further detail to the data protection regime in Oman and we expect, following its issuance, for MTCIT to enforce its provisions.

**Qatar:** The Qatar Law is supplemented by the NCGAA guidelines which provide entities with practical guidance into various requirements under the law. Companies should also consider any restrictions from other laws with data protection principles and requirements including Article 145 of Law No. 13 of 2012 Qatar Central Bank and the Regulation of Financial Services which requires all customer accounts, deposits, savings and safes to be confidential and not to disclose any related information or data without the consent of the customer, or Article 8 of Law No. 14 of 2014 On the Issuance of the Law on Combating Cyber Crimes which penalises the publishing of news, photos, video or audio recording affecting private or family life of individuals where it insults or defames.

#### ***4.2.4. Powers and enforcement capabilities***

**KSA:** In parallel with the NDMO's more specific tasks, SDAIA has general regulatory powers over the data and artificial intelligence sectors, and may thus define relevant policies, standards and controls. It is also empowered to represent the Kingdom in international

forums on data and artificial intelligence matters, and collaborates with the Ministry of Communications and Technology in a number of policy areas.

**Bahrain:** The DPA has powers and enforcement capabilities to ensure compliance with data protection laws, this includes:

- **Investigation Powers:** The DPA has the authority to conduct investigations into potential violations of data protection laws. This includes the power to request information from organizations, carry out audits, and review documentation and records.
- **Enforcement Actions:** If the DPA determines that a violation has occurred, it has the power to take various enforcement actions. This can include issuing warnings or orders to comply with data protection requirements. In more serious cases, the DPA may impose fines, penalties, or administrative sanctions.
- **Remedial Measures:** The DPA can require organizations to take remedial measures to address any non-compliance with data protection laws. This may involve implementing specific security measures, changing data processing practices, or providing compensation to affected individuals.
- **Cross-Border Cooperation:** The DPA can cooperate and collaborate with other data protection authorities in different jurisdictions. This allows for effective handling of cross-border data protection issues, ensuring consistent enforcement and protection of individuals' rights.
- **Awareness and Education:** The DPA plays a role in raising awareness and educating organizations and individuals about their data protection rights and obligations. This includes providing guidance, conducting training programs, and promoting best practices in data protection.

**Kuwait:** In the event of a proven violation to the provisions of these regulations or the laws of the State of Kuwait, CITRA may apply the penalties and fines stipulated under Law No. 73 of 2014 establishing the Communications and Information Technology Regulatory Authority as amended by Law No. (98) of 2015.

**UAE:** Article 3 of Law No. 44/2021 sets out the powers of the UAE Data Office which are:

- *“Proposing and preparing the policies, strategies, and legislations related to the affairs of data protection, in coordination with the competent bodies; and supervising their implementation after the approval of the Cabinet.*”

- *Proposing and endorsing the bases and criteria concerning control of the application of the Federal legislations that regulate data protection, in coordination with the competent bodies.*
- *Preparing and endorsing the regulations of complaints and grievances related to data protection, in coordination with the competent bodies.*
- *Issuing the handbooks and instructions necessary for the implementation of data protection legislations.*
- *Implementing control of the application of the Federal legislations that regulate data protection; and conducting the investigations necessary for ensuring compliance with these legislations.*
- *Receiving complaints and grievances concerning data protection; and verifying them with all competent bodies.*
- *Raising awareness of the provisions and requirements of data protection by organizing conferences, forums, workshops, etc.*
- *Conducting specialized studies and research in the fields relevant to the Bureau's terms of reference, including surveying and analyzing the regional and international phenomena, risks, and orientations.*
- *Proposing joining international treaties and agreements or signing them, and proposing partnership agreements with Gulf, regional, and international countries, organizations, and bodies relevant to the Bureau's activities and terms of reference, or signing them, in coordination with the Ministry of Foreign Affairs and International Cooperation and other concerned bodies.*
- *Representing the State in regional and international organizations, fairs and conferences in the fields related to the Bureau, in coordination with the Ministry of Foreign Affairs and International Cooperation and other concerned bodies.*
- *Any other terms of reference that it may be entrusted with pursuant to the laws or the regulations and decisions issued by the Cabinet."*

**Oman:** Article 7 of the Oman Law sets out the responsibilities of MTIC (which are without prejudice to the competencies of the Cyber Defense Centre). These are to:

- *“Prepare and approve controls and procedures related to the Personal Data protection, including determining the necessary safeguards, necessary measures and codes of conduct relating to the Personal Data protection;*
- *Issue the necessary controls and procedures for Processing Personal Data and verify compliance of the Controller and the Processor therewith;*
- *Receive and decide on communications and complaints filed by the Personal Data Owners within the period specified in the Regulations;*
- *Cooperate with the authorities concerned with the Personal Data protection in other countries;*
- *Provide advice, support and coordination with the units of the administrative apparatus of the State and other public legal persons in any matter related to the Personal Data protection;*
- *Issue and cancel the licenses of service providers entrusted with studying and evaluating the compliance of the Controller and the Processor with the provisions of this Law, in accordance with the controls and procedures specified in the Regulations;*
- *Prepare indicative forms for the purposes of implementing the provisions of this Law, whenever necessary;*
- *Prepare periodic reports on its activities in the field of Personal Data protection, and published on its website; and*
- *Prepare a register in which the Controllers and the meeting the prescribed conditions are registered, as specified in the Regulations.”*

**Qatar:** Please see the response for Qatar in “4.1.2. Promoting awareness and compliance”. The powers listed under Article 3 of Decision No. 1/2021 largely focus on cybersecurity, however, nonetheless include implementing laws, regulations and decisions related to persona data protection. The NCGAA also has strategic objectives in relation to data privacy which are to:<sup>148</sup>

- *“Increase awareness of privacy rights among individuals and organisations*

---

<sup>148</sup> [Personal Data Privacy | National Cyber Governance and Assurance Affairs \(nca.gov.qa\)](https://nca.gov.qa)

- *Receive and respond effectively to complaints about misuse of personal data*
- *Investigate and support issuing of fines or penalties to organisations in line with the PDPL*
- *Engage with industry sector groups effectively to increase standard of data protection practices*
- *Participate actively in international privacy communities*
- *Stay relevant and update guidance on privacy around emerging technologies*
- *Enhance capability and build world-class privacy leadership in Qatar*
- *Develop and issue data protection policies for controllers.”*

#### **4.2.5. Collaboration and information exchange**

**KSA:** SDAIA represents the Kingdom in international fora related to data and artificial intelligence.

#### **4.2.6. Cultural and societal factors**

**KSA:** At this stage, there is hardly any experience with the PDPL's interpretation and enforcement in practice. It is reasonable to assume that, under these circumstances, a culture for personal data protection based on modern regulatory principles may take some time to be established.

**Bahrain:** Bahrain was one of the foremost jurisdictions within the GCC to enact a data protection law. This notwithstanding, the concept of data protection is still relatively in its infancy. Awareness campaigns have taken place and the telecommunications regulator has also published sector-specific guidelines.

**Kuwait:** The Kuwait Law is currently the comprehensive data protection law for the communication and information technology services sector. It abrogated Kuwait Decision No. 42 of 2021 and companies must regularise their status in accordance with the Kuwait Law (and other regulations related to it issued by the CITRA) within one year from the date of its publication.

**UAE:** Please see the UAE response to “4.1.1. Overseeing and enforcing data protection laws and regulations.”

**Oman:** With the Oman Executive Regulations being issued on 28 January 2024 and coming into force on 5 February 2024, supplementing the Oman Law and data protection regime in the jurisdiction, Oman has a complete standalone data protection framework. Companies have until 5 February 2025 to align their activities in adherence to the Oman Law and Oman Executive Regulations. We also expect for the MTCIT to increase awareness by publishing guidelines, policies and standards, before harshly enforcing the law.

**Qatar:** Although a more older data protection law compared to others in the GCC jurisdictions, we are not aware of any enforcement action taken by the NCGAA although these may not be public as done in other countries.

### 4.3. Data Protection Challenges in the GCC

**Bahrain:** In Bahrain, some of the common data protection challenges include:

- **Cross-border data transfers:** Ensuring the protection of personal data when transferring it to countries or territories that do not have adequate data protection measures in place can be a challenge. Data controllers must adhere to certain conditions and safeguards to ensure the privacy and fundamental rights of individuals.
- **Privacy concerns with emerging technologies:** As technology advances, privacy concerns arise with the use of emerging technologies such as AI, blockchain, and IoT. This requires a careful balance between innovation and protecting individuals' personal data.
- **Lack of public awareness and education:** There is a need for increased public awareness and education regarding data protection rights and responsibilities. Many individuals may arguably not be fully aware of their rights or how to exercise them.

**Kuwait:** The Kuwait Law represents a significant step in addressing data protection concerns in Kuwait. However, like many data protection regulations, it also presents several challenges and considerations. Some potential data protection challenges include:

- **Lack of Historical Data Protection Culture:** Before Regulation No. 42 of 2021, titled the Data Privacy Protection Regulation, which was abrogated by the Kuwait Law, Kuwait did not previously have a dedicated data protection law, which means that organizations and individuals may not be well-versed in data protection practices. Building a culture of data protection and awareness could be a challenge.

- **Enforcement and Compliance:** Ensuring that organizations comply with the Kuwait Law’s provisions is a significant challenge. Establishing enforcement mechanisms and penalties for non-compliance, as well as monitoring and auditing, is essential but can be resource intensive.
- **Data Protection Impact Assessments (DPIAs):** Missing DPIAs can lead to a lack of clarity on data processing activities and the potential harm caused to data subjects.
- **Data Protection Officers (DPOs):** Without requirements for a DPO, individuals, companies, and government agencies could face issues related to effective data protection oversight, compliance, and accountability.
- **Cross-Functional Cooperation:** Ensuring collaboration between IT, legal, and other relevant departments within organizations to implement data protection measures effectively can be a challenge.

**UAE:** Please see the UAE response to “4.1.1. Overseeing and enforcing data protection laws and regulations”. Given that the UAE Executive Regulations are not yet issued, which would only provide more information on the data protection requirements under the UAE onshore data protection regime, but would also start the clock for companies to ensure compliance. Given also that the UAE Data Office is not fully set up, it is uncertain when the UAE Law will be enforced albeit it is already in force. Another challenge in the UAE, is the application (whether direct or indirect) of other UAE laws with data protection and privacy requirements, for example, companies who cater to financial services clients which are subject to UAE Central Bank regulations and may be required to localise data and such requirements are flown down contractually. Companies, currently, need to map their data and understand the requirements applicable for various sets. It is uncertain whether a harmonisation between UAE laws and regulations or further collaboration between regulators in the UAE is in the pipeline to aid such a challenge.

**Oman:** Although the Oman data protection regime generally reflects international best practice on data protection, there are some important differences which may be seen as challenges from some companies (particularly international companies) which have aligned their activities to (for example) the GDPR. Some differences include (without limitation) the requirement to apply for a permit from MTCIT to process certain types of data (namely considered as sensitive personal data in other data protection laws as it includes Genetic data<sup>149</sup>, Biological Data<sup>150</sup>, Health Data<sup>151</sup>, ethnic origins, sexual life, political or religious opinions or beliefs, criminal

---

<sup>149</sup> Genetic Data: Personal Data relating to inherited or acquired genetic characteristics, obtained from the analysis of the biological sample.

<sup>150</sup> Biological Data: Personal Data that results from specific technical Processing related to physical, psychological or behavioral characteristics, such as a face image or DNA data.

<sup>151</sup> Health Data: Personal Data relating to physical, mental and physiological health.

convictions, or security measures)<sup>152</sup>, the requirement to appoint a DPO (which is generally a requirement in other data protection laws in certain instances, for example, where businesses process sensitive data on a large scale or whose core activities include large scale, regular and systemic monitoring of individuals , and the requirement to appoint an external auditor to oversee compliance with the Oman Law.

**Qatar:** International data protection challenges (including those listed above such as privacy concerns with emerging technologies, lack of public awareness and education, lack of historical data Protection culture, enforcement and compliance mechanisms and localising GDPR compliant frameworks to meet the differences under Qatar Law) will also apply.

#### 4.4. Emerging Trends and Best Practices

Some emerging trends include:

- **Enhanced data security measures:** Organizations are advised to implement advanced security measures to protect personal data from unauthorized access, loss, or disclosure. This may involve using encryption, secure storage systems, and conducting regular security audits.
- **Data breach notification:** In the event of a data breach, organizations are expected to promptly notify the affected individuals and their respective data protection authorities. This helps to ensure transparency and allows individuals to take necessary steps to protect themselves from potential harm.
- **Data protection impact assessments (DPIAs):** Organizations should conduct DPIAs to identify and mitigate privacy risks associated with their data processing activities. This involves assessing the potential impact on individuals' privacy and implementing appropriate measures to address any identified risks.
- **Privacy by design and default:** Organizations are encouraged to incorporate privacy considerations into the design and development of their products, services, and systems. This includes implementing privacy-friendly default settings and minimizing the collection and retention of personal data.

---

<sup>152</sup> Oman Law, Article 5, Oman Law and Article Chapter 2 of the Oman Executive Regulations.

- **Employee training and awareness:** Organizations should provide regular training and awareness programmes to employees regarding their obligations under data protection laws. This helps to foster a culture of privacy within the organization and ensures that employees handle personal data appropriately.
- **Cross-border data transfers:** Organizations transferring personal data outside of Bahrain should ensure that appropriate safeguards are in place, such as implementing standard contractual clauses or relying on adequacy decisions by the Data Protection Authority.
- **Proactive monitoring and compliance:** Organizations should regularly monitor their data processing activities to ensure compliance with their respective data protection law's requirements and industry best practices. This may involve conducting internal audits, appointing a data protection officer, and implementing compliance management systems.

## 5. FUTURE DIRECTIONS AND POTENTIAL CHANGES

### 5.1 Strengthening GCC Data Protection Laws and Regulations

Essentially all of the Data Protection Laws examined in this paper are relatively recent. In some cases, key pieces of the relevant framework are still work-in-progress and/or not yet fully operative. The process ahead may be long: as shown in jurisdictions with decades of data protection enforcement, building public awareness, acquiring the required regulatory resources and expertise, securing international cooperation, and establishing a culture of effective enforcement can take some time. This is bound to be also the case in the GCC region, even if the lessons learnt from international best practice can help accelerate the process.

Consequently, there are two obvious next steps to strengthen the emerging GCC data protection regimes: first, any remaining pieces of the regulatory jigsaw puzzle, such as implementing regulations, guidelines, notices etc., must be completed as soon as possible. Second, regulators must be adequately equipped with the necessary human, technical and legal resources to exercise their tasks effectively. Such essential regulatory actions are not a luxury that can wait: the processing of personal data is now at the heart of modern economies and administrations, feeding industries and technologies the GCC region relies on to stay at the forefront of economic development.

Our comparative review of Data Protection Laws has identified broad similarities, but also significant differences, especially when it comes to the national provisions' details. Some of these differences affect the regimes' cornerstones of data protection and thus pose a further obstacle to a stronger and more effective regional data protection regime. Examples of such differences include the

conditions for consent; the legal bases for data processing and their exceptions; and the rights of data subjects. The challenges arising from such differences can be addressed from two complementary viewpoints: that of data users and that of the state agencies entrusted with data protection (secondary) regulation and enforcement. Each is discussed briefly below.

## **5.2 What can data controllers do to comply across the GCC region?**

Data controllers active in a single GCC jurisdiction will generally not be affected by discrepancies between the GCC data protection regimes. The position will be different, however, for enterprises with a broader regional presence or those seeking cross-border expansion. For such market players, ensuring data protection compliance through country-specific and hence diverse customer and supplier terms and conditions, IT arrangements, databases, data processing arrangements, consent management forms etc. will likely be a disproportionate operational burden. A more realistic alternative for them would be the adoption of a uniform internal data protection policy across the whole GCC region. However, to meet this objective, such a policy may need to follow a “strictest common denominator” approach. This may be less burdensome than it sounds, at least for larger market players, such as online platforms, with an international footprint, and hence cross-border experience from the strict data protection rules of the GDPR and other regions. Building on this experience, such market players can adjust their current data protection policies to a “GCC-compliant” model, instead of having to build one from scratch. Moreover, and despite national variations, it is reasonable to assume that the data protection requirements for GCC region compliance are generally less burdensome, detailed and intrusive than those already in place elsewhere, notably in the EU.

## **5.3 What can national GCC authorities do to ease compliance across the GCC region?**

Ultimately, regional alignment of GCC data protection rules would offer an optimal solution for a more effective and reliable data protection regime across the region. However, even if cooperation between the GCC countries for the gradual harmonization of their Data Protection Laws is an obviously commendable goal, regional agreement on a full alignment of national provisions and its subsequent legislative implementation may take years to achieve. A more realistic short term goal would be for GCC authorities to focus on an area of particular importance for personal data processing on a regional basis, namely that of cross-border data transfers based on “adequate standard of protection” arrangements or other common standards.

As mentioned earlier, in Section 2.1.1.6 of this Paper, the Data Protection Laws generally follow, at least at a high level, an approach of identifying “adequate” jurisdictions for cross-border data transfers, even if the number of adequate jurisdictions can vary widely from one country to the other. There are also additional, but even more varied, means for enabling cross-border data transfers to countries not deemed to be adequate, such as the use of consent, certain contractual conditions, standard contract clauses, binding

corporate rules, etc. Against this background, and as concluded earlier, there are clear benefits in targeting, as a first and more realistically achievable goal, regional “adequacy” arrangements, and perhaps other means (e.g., standard contractual clauses and binding corporate rules) to allow personal data to flow more easily across the region. Such arrangements can be negotiated between GCC countries both bilaterally (e.g. as a start, if this is politically easier and can get the process underway) and on a GCC level – a solution that would seem to make more sense, at least in the longer term.

A second key data protection issue that could be the focus of such regional alignment would be the conditions for obtaining consent as a lawful basis for the processing of personal data (see Section 2.1.1.1, above). Various interpretation issues can arise in connection with this key concept including, in particular, the conditions under which the data subject’s consent can be considered free, specific, express, informed and unambiguous. In this, and other areas of possible alignment, data protection authorities could proceed on the basis of joint guidelines or similar measures that should be much easier to adopt than a legislative harmonization. As regards the question of consent, for example, data protection authorities could list, in such a joint text, the conditions they consider sufficient for the grant of consent under their national laws while also mentioning their differences and providing a “strictest common denominator” set of consent conditions, which all of the data protection authorities concerned would consider sufficient for the purposes of their national rules.

Such a soft law instrument would still be more authoritative, and hence offer more legal certainty, than any private initiative, even if the latter can help highlight gaps and the benefits of a more harmonized regime, and thus pave the way towards a regionally coordinated regulatory approach.

## ANNEX 1

The GCC includes several countries in the GCC. Here are the data protection authorities in these countries:

Country	Authority	Link
<b>Bahrain</b>	The Personal Data Protection Authority	<a href="http://pdp.gov.bh">Personal Data Protection Authority   Kingdom Of Bahrain (pdp.gov.bh)</a>
<b>Saudi Arabia</b>	Saudi Data and Artificial Intelligence Authority – National Data Management Office	<a href="http://sdaia.gov.sa">National Data Management Office (sdaia.gov.sa)</a>
<b>United Arab Emirates</b>	UAE Data Office	<a href="#">Data protection laws - The Official Portal of the UAE Government</a>
<b>Qatar</b>	Data Protection Department within the Ministry of Transport and Communications	<a href="#">MOTC Releases Guidelines on Personal Data Privacy Protection Law   Ministry of Transport</a>
<b>Kuwait</b>	Data Privacy Protection Regulation issued by the Communication & Information Technology Regulatory Authority	<a href="#">Data Privacy Protection Regulation.pdf (citra.gov.kw)</a>
<b>Oman</b>	Sultanate of Oman Ministry of Transport, Communications, and Information Technology	<a href="http://ita.gov.om">MTCIT   Home (ita.gov.om)</a>

## **ANNEX 2 - DATA PROTECTION LAWS IN GCC COUNTRIES**

The below table provides a multi-jurisdictional analysis of some key principles in data protection regimes in the GCC region. More specifically, it is a side-by-side comparison of each of the principles across the various jurisdictions (GCC Comparison).

The analysis covers the data protection laws of the United Arab Emirates (“UAE”), Saudi Arabia (“KSA”), Oman, Bahrain, Qatar, Kuwait and looks into whether or how some key principles (applicability, data protection principles, record of processing activities requirements, notice requirements, transfer requirements, Data Protection Officer requirements, Data Processing Impact Assessment requirements, breach requirements and fines/penalties) are reflected in these laws.

For the purposes of this analysis, capitalised terms in the below tables reflect the definitions under the respective data protection laws.

## GCC COMPARISON

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
<b>Who does the law apply to</b>	<p>UAE Federal Decree-Law No. 45/2021 (“<b>UAE Data Protection Law</b>”) applies to the Processing of Personal Data by:-<sup>154</sup></p> <p>any Data Subject who resides or has a place of business in the State;</p> <p>any Controller or Processor located in the State who carries out the activities of Processing Personal Data of Data Subjects inside or outside the State; and</p> <p>any Controller or Processor located outside the State who carries out the activities of Processing Personal Data of Data Subjects inside the State.</p> <p>The UAE Data Protection Law has</p>	<p>Saudi Arabia Cabinet Decision No. 98/1443 Personal Data Protection Law, as amended (“<b>KSA Data Protection Law</b>”) applies to the Processing of Personal Data related to individuals that take place in the Kingdom, including the Processing of Personal Data of individuals residing in the Kingdom by an entity outside the Kingdom. The KSA Data Protection Law, therefore, has extra-territorial effect.</p> <p>It also applies to data of a deceased person if it would lead to identifying him or a family member specifically.</p> <p>The KSA Data Protection Law and the</p>	<p>Oman Sultani Decree No. 6/2022 (“<b>Oman Data Protection Law</b>”) applies to Personal Data that is processed.</p> <p>It is prohibited to process the Personal Data:-</p> <p>related to Genetic data, Biological Data, Health Data, ethnic origins, sexual life, political or religious opinions or beliefs, criminal convictions, or security measures (i.e data similar to sensitive personal data as set out in other data protection laws) except after obtaining a permit therefor from the Ministry, in accordance with the controls and procedures under Oman Ministerial Decision No. 34/2024 Issuing the</p>	<p>Bahrain Law No. 30/2018 (“<b>Bahrain Data Protection Law</b>”) applies to the following processes:-<sup>161</sup></p> <p>Data processing using automated means; and</p> <p>Data processing that is part of a filing system or is intended to form part of this system, by non-automated means.</p> <p>The Bahrain Data Protection Law applies to the following persons:-<sup>162</sup></p> <p>every natural person who normally resides in or has a place of business in the Kingdom;</p>	<p>Qatar Law No. 13/2016 (“<b>Qatar Data Protection Law</b>”) applies to personal data that is processed electronically, or obtained, collected, or extracted in any other manner as a preliminary step towards being processed electronically, or those processed in combination between electronic processing and traditional processing.</p> <p>The Qatar Data Protection Law does not apply to the processing of personal data by individuals in connection with personal or family matters, or for the aim to obtain official statistical data according to the</p>	<p>Kuwait Administrative Decision No. 26/2024 Concerning the Issuance of the Data Privacy Protection Regulation (“<b>Kuwait Law</b>”) applies to all Service Providers<sup>168</sup>, licensed by the Authority, who collect, process and store Personal Data and user Data content in whole or in part, whether permanently or temporarily by automated means or by any other means that form part of the Data storage system, whether the Processing takes place within the State of Kuwait or outside it.</p> <p>Exceptions to the Kuwait Law are to practices related to security investigations, monitoring of violations, or practices violating</p>

<sup>153</sup> Kindly note the Executive Regulations to the UAE Data Protection Law have not yet been issued.

<sup>154</sup> UAE Federal Decree-Law No. 45/2021, Article 2(1).

<sup>161</sup> Bahrain Law No. 30/2018, Article 2(1)

<sup>162</sup> Bahrain Law No. 30/2018, Article 2(2)

<sup>168</sup> Service Provider/Licensee: The person licensed to provide one or more telecommunication services to the public or licensed to manage, establish or operate a telecommunication network or internet service to provide telecommunication services to the public. This includes providers of information or content through the telecommunication network.

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
	<p>extra-territorial effect applying to companies incorporated in the UAE, as well as companies incorporated outside the UAE and which process Personal Data of Data Subjects inside the UAE.</p> <p>However, the UAE Data Protection Law does not apply to:-<sup>155</sup></p> <p>government data;</p> <p>government authorities that control or process Personal Data;</p> <p>Personal Data held with security and judicial authorities;</p>	<p>Implementing Regulation of the Personal Data Protection Law issued by Saudi Data &amp; AI Authority (“<b>KSA Implementing Regulations</b>”), however, do not apply to an individual Processing Personal Data for personal or family use (i.e Processing Personal Data within their family or limited social circle as part of any social or family activity).<sup>156</sup></p> <p>Publishing Personal Data to the public, disclosing it to any person outside the aforementioned scope or using Personal Data for professional, commercial or non-profit purposes is not considered as personal</p>	<p>Implementing Regulation of the Personal Data Protection Law (“<b>Oman Implementing Regulations</b>”); and<sup>158</sup></p> <p>of a child without the consent of his/her guardian, unless such the Processing is in the best interest of the child, in accordance with the controls and procedures specified in the Oman Implementing Regulations.<sup>159</sup></p> <p>The law does not apply to the Processing of Personal Data in the following cases:-<sup>160</sup></p> <p>protection of the national security or the public interest;</p>	<p>every legal person that has a place of business in the Kingdom; and</p> <p>every natural or legal person who does not normally reside in the Kingdom and has no place of business in the Kingdom processing data using means available in the Kingdom, unless the purpose of using such means is merely to transfer data through the Kingdom.</p> <p>The law does not apply to:-<sup>163</sup></p> <p>data processing by any individual for purposes not exceeding personal or family affairs; and</p> <p>national security-related processes handled by the Ministry</p>	<p>provisions of Law No. 2 of 2011.<sup>165</sup></p> <p>Similarly, companies should consider the regulatory guidelines to the Qatar Data Protection Law issued by the National Cyber Governance and Assurance Affairs of the National Cyber Security Agency (“<b>NCGAA Guidelines</b>”) for regulated entities.</p> <p>The NCGAA Guidelines also provide individuals with information on their rights under the Qatar Data Protection Law<sup>166</sup>, along with data privacy protection measures<sup>167</sup>.</p>	<p>the laws, decisions, judicial rulings, or financial claims arising from the subscription contract.<sup>169</sup></p>

<sup>155</sup> UAE Federal Decree-Law No. 45/2021, Article 2(2).

<sup>156</sup> KSA Implementing Regulation of the Personal Data Protection Law, Article 3

<sup>158</sup> Oman Sultani Decree No. 6/2022, Article 5

<sup>159</sup> Oman Sultani Decree No. 6/2022, Article 6

<sup>160</sup> Oman Sultani Decree No. 6/2022, Article 3

<sup>163</sup> Bahrain Law No. 30/2018, Article 2(4)

<sup>165</sup> Qatar Law No. 13/2016, Article 2

<sup>166</sup> Individuals’ Rights – Guideline for Individuals, Article 2

<sup>167</sup> Social Media – Guideline for Individuals, Article 2

<sup>169</sup> Kuwait Administrative Decision No. 26/2024 Concerning the Issuance of the Data Privacy Protection Regulation, Article 1

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
	<p>a Data Subject who processes his/her data for personal purposes;</p> <p>health personal data that is subject to legislation regulating the protection and Processing thereof;</p> <p>banking and credit personal data and information that is subject to legislation regulating the protection and Processing thereof; and</p> <p>companies and institutions located in the free zones of the State and are subject to special legislation on Personal Data Protection.</p> <p>The UAE Data Protection Law does not apply to certain sectors and jurisdictions that have their own data protection laws or laws with data protection considerations (for example, the Dubai International Financial Centre (“DIFC”), Abu Dhabi Global Market</p>	<p>or family use and is in the scope of the law and KSA Implementing Regulations.<sup>157</sup></p>	<p>performance by the units of the administrative apparatus of the State and other public legal persons of the competencies prescribed for them by law;</p> <p>performance of a legal obligation imposed on the Controller under any law, judgment or decision of a court;</p> <p>protection of the economic and financial interests of the State;</p> <p>protection of a vital interest of the Personal Data Owner;</p> <p>detection or prevention of any criminal offense based on an official written request from the investigation authorities;</p> <p>executing a contract to which the Personal Data Owner is a party;</p>	<p>of Defense, the Ministry of the Interior, the National Guard, the National Security Apparatus or other security services of the Kingdom.</p> <p>The law shall not prejudice the confidentiality requirements of the Bahrain Defense Force.<sup>164</sup></p> <p>Accompanying the Bahrain Data Protection Law are Ministerial Decisions including Bahrain Ministerial Decision No. 42/2022 On the Transfer of Personal Data Outside the Kingdom of Bahrain and the Bahrain Ministerial Decision No. 43/2022 Defining the Requirements to be Met in Technical and Organisational Measures to Protect Personal Data (“<b>Bahrain Regulations</b>”).</p>		

<sup>157</sup> KSA Implementing Regulation of the Personal Data Protection Law, Article 3(3)

<sup>164</sup> Bahrain Law No. 30/2018, Article 2(5)

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
	("ADGM") or UAE Central Bank).		<p>if the Processing is in a personal or family context;</p> <p>the purposes of historical, statistical, scientific, literary or economic research, by the authorities authorized to carry out such works, provided that no indication or reference related to the Personal Data Owner is used in the research or statistics they publish, to ensure that Personal Data is not attributed to an identified or identifiable natural person; or</p> <p>if the data is available to the public in a manner that does not violate the provisions of this Law.</p>			
<b>Principles</b>	<p>The principles under the UAE Data Protection Law include:-<sup>170</sup></p> <p>processing must be made in a fair, transparent and lawful manner;</p>	<p>There is no explicit "principles" provision in the KSA Data Protection Law, however, similar (if not identical) concepts can be found across the law, for example:-</p> <p>purpose of collecting Personal Data shall be</p>	<p>Article 10 of the Oman Data Protection Law sets out that Personal Data may only be processed within a framework of transparency, honesty, and respect for human dignity, and after obtaining the express</p>	<p>The personal data processed shall be as follows:-<sup>176</sup></p> <p>processed fairly and legally;</p> <p>collected for a legitimate, specific and clear purpose, not to be altered subsequently,</p>	<p>The Qatar Data Protection Law sets out principles to processing in various provisions including:-</p> <p>every individual has the right to the protection of the privacy of personal data, where those data may only be processed</p>	<p>Although no explicit principles provision, these principles can be found throughout the law.</p>

<sup>170</sup> UAE Federal Decree-Law No. 45/2021, Article 5.

<sup>176</sup> Bahrain Law No. 30/2018, Article 3

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
	<p>Personal Data must be collected for a specific and clear purpose, and may not be processed at any subsequent time in a manner incompatible with that purpose. However, Personal Data may be processed if the purpose of Processing is similar or close to the purpose for which such data is collected;</p> <p>Personal Data must be sufficient for and limited to the purpose for which the Processing is made;</p> <p>Personal Data must be accurate and correct and must be updated whenever necessary;</p> <p>appropriate measures and procedures must be in place to ensure erasure or correction of</p>	<p>directly related to the purposes of the Controller, and it shall not conflict with any provision established by law;<sup>171</sup></p> <p>Personal Data collected shall be appropriate and limited to the necessary level needed to achieve the purpose of the legislation, while avoiding the inclusion of whatever leads to recognising its owner specifically whenever the purpose of its Collection is achieved; and<sup>172</sup></p> <p>Personal Data should not be processed without taking sufficient steps to verify its accuracy, completeness, up-to dateness and relevance to the purpose for which it is collected.<sup>173</sup></p>	<p>consent of the Personal Data Owner.<sup>175</sup></p>	<p>and that no subsequent processing is in a manner inconsistent with the purpose for which it was collected. Processing is not considered incompatible with the purpose of subsequently processing data for historical, statistical or scientific research, provided that it is not to support any decision or action regarding a specific individual;</p> <p>adequate, relevant and not excessive given the purpose of collection or subsequent processing;</p> <p>correct and accurate, and subject to updates when necessary; and</p> <p>not remain in a form that allows the Data Owner to be identified after the completion of</p>	<p>within the scope of transparency, integrity, respect of human dignity and accepted practices, in accordance with the provisions of the present Law; and<sup>178</sup></p> <p>the controller must verify that the personal data collected by him or on his behalf, are adequate and relevant to the Legitimate Purposes. The controller must verify that such data are accurate, complete and kept up-to-date to meet the Legitimate Purposes, and shall not be kept for longer than is necessary to achieve such purposes.<sup>179</sup></p> <p>Additionally, the controller shall comply with the following:-<sup>180</sup></p>	

<sup>171</sup> Saudi Arabia Cabinet Decision No. 98/1443, Article 11(1).

<sup>172</sup> Saudi Arabia Cabinet Decision No. 98/1443, Article 11(3)

<sup>173</sup> Saudi Arabia Cabinet Decision No. 98/1443, Article 14

<sup>175</sup> Oman Sultani Decree No. 6/2022, Article 10

<sup>178</sup> Qatar Law No. 13/2016, Article 3

<sup>179</sup> Qatar Law No. 13/2016, Article 10

<sup>180</sup> Qatar Law No. 13/2016, Article 8

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
	<p>incorrect Personal Data; and</p> <p>Personal Data must be kept securely and protected from any breach, infringement, or illegal or unauthorized Processing by establishing and applying appropriate technical and organizational measures and procedures in accordance with the laws and legislation in force in this regard.</p> <p>Personal Data may not be kept after fulfilling the purpose of Processing thereof. It may only be kept in the event that the identity of the Data Subject is anonymized using the “Anonymization” feature.</p> <p>Any other controls set by the Executive Regulations of this Decree Law. Kindly note that the executive regulations or implementing regulations to the UAE Data Protection Law</p>	<p>Additionally, if it appears that the collected Personal Data is no longer necessary to achieve the purpose of its Collection, the Controller shall discontinue collecting it and shall promptly destroy what was previously collected thereof.<sup>174</sup></p> <p>The KSA Implementing Regulations also references principles throughout including (but not limited to) data minimisation in Article 19.</p>		<p>the purpose for collection or for which subsequent processing is performed. Data that are stored for longer periods for historical, statistical or scientific purposes shall be kept in an anonymised format by putting them in a form that does not enable such data to be related to the owner. It should not be possible to decode the identity of their owners from this.</p> <p>An exception to this requirement is processing for journalistic, artistic or literary purposes so long as:<sup>177</sup></p> <p>the data is correct, accurate and subject to update and correction;</p> <p>measures are available to ensure that data are not used for any purpose other than for journalistic, artistic or literary purposes; and</p>	<p>processing personal data with integrity and lawfully;</p> <p>complying with the controls on designing, amending or developing products, systems and services relating to the processing of personal data;</p> <p>taking appropriate administrative, technical and material precautions to protect the personal data, as specified by the competent Department; and</p> <p>policies for the protection of privacy, set down by the competent Department and issued by decision of the Minister.</p> <p>Additionally, the NCGAA Guidelines include “Principles of Data Privacy” which set out and explain the principles in the Qatar Data Protection Law in</p>	

<sup>174</sup> Saudi Arabia Cabinet Decision No. 98/1443, Article 11(4)

<sup>177</sup> Bahrain Law No. 30/2018, Article 6

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
	have not yet been issued.			without prejudice legislation on press, printing and publishing.	further detail. These are <sup>181</sup> : <ul style="list-style-type: none"> <li>• transparency, honesty and respect for human dignity;</li> <li>• data minimisation;</li> <li>• accuracy;</li> <li>• storage limitation;</li> <li>• integrity and confidentiality;</li> <li>• purpose limitation; and</li> <li>• accountability.</li> </ul>	
<b>Lawful basis of processing</b>	Under the UAE Data Protection Law, it is prohibited to process Personal Data without the consent of the Data Subject. Such consent must also be obtained in accordance to the law.  There are, however, exceptions to the prohibition and where another lawful basis	Under Article 5 of the KSA Data Protection Law, Personal Data may not be processed (or the purpose of its Processing changed) without the Consent of the Data Subject. The KSA Implementing Regulations clarify under Article 11 the conditions of obtaining such consent.	Article 10 of the Oman Data Protection Law sets out that Personal Data may only be processed after obtaining the express consent of the Personal Data Owner. The request for Processing Personal Data must be in writing, in a clear, explicit and understandable manner, and the	The processing of personal data is prohibited without the consent of the owner, unless such processing is necessary for any of the following:- <sup>188</sup>  implementation of a contract to which the Data Owner is a party;	A controller may not process the personal data except with the consent of the individual, unless such processing is necessary to achieve a Legitimate Purpose pursued by the controller or a third party to whom such data are sent. <sup>191</sup> NCGAA Guidelines may suggest that a	The Service Provider shall, before providing the service to the User obtain the consent of the service applicant to collect or process Personal Data and ensure his knowledge and acceptance of all conditions, obligations and provisions of data

<sup>181</sup> Principles of Data Privacy, Article 1

<sup>188</sup> Bahrain Law No. 30/2018, Article 4

<sup>191</sup> Qatar Law No. 13/2016, Article 4

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
	<p>can be relied upon instead. These exceptions are:-<sup>182</sup></p> <p><b>Public Interest:-</b> Processing is necessary to protect the public interest;</p> <p><b>Public Data:-</b> Processing involves Personal Data available and made public by that the Data Subject;</p> <p><b>Legal Actions:-</b> Processing is necessary for legal proceedings, rights claims, or related to judicial or security procedures;</p> <p><b>Occupational or Preventive Medicine:-</b> Processing is necessary for medical reasons, including (but not limited to) occupational medicine,</p>	<p>There are, however, exceptions to the prohibition and where another lawful basis can be relied upon instead. These exceptions are where processing:-<sup>183</sup></p> <p>achieves a fulfilled interest for the data owner, and it is impossible or difficult to contact them. The KSA Implementing Regulations define Actual Interest<sup>184</sup> and requires evidence of such interest to be retained along with that it is difficult to contact or communicate with the Data Subject;<sup>185</sup></p> <p>is required by another law or is in implementation of an earlier agreement to which the Personal Data Owner is a party;</p>	<p>Controller is required to prove the written consent of the Personal Data Owner to the Processing of his/her data.<sup>187</sup></p> <p>Article 4 of the Oman Implementing Regulations sets out the consent conditions for obtaining explicit consent before processing personal data. These are:</p> <ul style="list-style-type: none"> <li>the consent shall be issued by a fully qualified person;</li> <li>the consent shall be issued in a clear manner and without coercion; and</li> <li>the approval shall be given in writing, or electronically, or by any other</li> </ul>	<p>taking steps at the request of the Data Owner with a view to concluding a contract;</p> <p>implementation of a duty prescribed by the Law, contrary to a contractual obligation, or an order issued by a competent court or the Public Prosecution;</p> <p>protecting the vital interests of the Data Owner; and</p> <p>directly for the legitimate interests of the Data Manager or any third party to whom the data is disclosed unless this conflicts with the fundamental rights and freedoms of the Data Owner.</p> <p>Further lawful basis is required for processing sensitive personal data</p>	<p>Lawful Purpose also includes legal or contractual obligation or legitimate interest.</p> <p>The competent authority may decide to process some personal data to achieve any of the following objectives:-<sup>192</sup></p> <ul style="list-style-type: none"> <li>safeguarding the national security and public security;</li> <li>protecting the international relations of the State;</li> <li>protecting the economic or financial interests of the state; and</li> <li>preventing any felony, or collecting relevant information or</li> </ul>	<p>collection and processing.<sup>196</sup></p> <p>The collection and processing of data shall be deemed legitimate and legal only in one of the following cases:-<sup>197</sup></p> <p>obtaining the consent of the data owner;</p> <p>it shall be necessary to ensure compliance with a legal obligation to which the Service Provider is subject;</p> <p>it shall be necessary to protect User data;</p> <p>if the purposes carried out by the Service Provider require identification of the data subject; and</p> <p>obtaining the written consent of the minor's</p>

<sup>182</sup> UAE Federal Decree-Law No. 45/2021, Article 4.

<sup>183</sup> Saudi Arabia Cabinet Decision No. 98/1443, Article 6.

<sup>184</sup> Actual Interest:- refers to any moral or material interest of the Data Subject that is directly linked to the purpose of Processing Personal Data, and the Processing is necessary to achieve that interest.

<sup>185</sup> KSA Implementing Regulation of the Personal Data Protection Law, Article 14

<sup>187</sup> Oman Sultani Decree No. 6/2022, Article 10

<sup>192</sup> Qatar Law No. 13/2016, Article 18

<sup>196</sup> Kuwait Administrative Decision No. 26/2024 Concerning the Issuance of the Data Privacy Protection Regulation, Article 2(2).

<sup>197</sup> Kuwait Administrative Decision No. 26/2024 Concerning the Issuance of the Data Privacy Protection Regulation, Article 3.

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
	<p>health or social care, treatment or health insurance services;</p> <p><b>Public Health:</b>- Processing is necessary to protect public health, including (but not limited to) protection against communicable diseases and ensuring safety and quality of healthcare;</p> <p><b>Archival, Scientific, Historical, or Statistical Purposes:</b>- Processing is necessary for archival, scientific, historical research, or statistical studies;</p> <p><b>Data Subject's Interests:</b>- Processing is necessary to protect the interests of the Data Subject;</p> <p><b>Employment and Social Rights:</b>- Processing is necessary for fulfilling obligations and exercising rights in employment, social</p>	<p>is done by a Public Entity for security or judicial reasons; or</p> <p>is necessary to achieve the legitimate interest of the Controller (except if it prejudices the rights of the data owner, conflicts with their interest or is Sensitive Data). The KSA Implementing Regulations under, Article 16(1), does not offer this lawful basis to Public Entities and also sets out conditions if this lawful basis is to be relied upon. This includes (but is not limited to) the purpose not violating any laws in KSA; a balance between the rights and interests of the Data Subject and the Legitimate Interest of the Controller so that the interest of the Controller does not affect the rights and interests of the Data Subject; the Processing not include Sensitive Data; and the processing should be within reasonable</p>	<p>means determined by the Controller.</p> <p>Written consent is also required under Article 22 before sending the Personal Data Owner any advertising or marketing material or material of commercial purpose. The Regulations is expected to provide more detail once issued.</p> <p>Kindly note that Article 3 excludes instances where the law does not apply (these instances can be seen as similar lawful basis in other data protection laws e.g performance of a legal obligation imposed on the controller under law, judgment or decision of a court or executing a contract to which the data subject is a party).</p> <p>Kindly also note the processing restrictions for sensitive personal data and children data</p>	<p>under Bahrain Data Protection Law.<sup>189</sup> Article 5 of the Bahrain Data Protection Law prohibits the processing of sensitive personal data without the consent of the owner. The following exceptions are permitted:-</p> <p>processing required by the Data Manager for their duties and the exercise of their legally prescribed rights in the field of labour relations that binds them to their employees;</p> <p>processing necessary to protect any person if the Data Owner - or custodian, guardian or trustee - is not legally able to give their consent thereto, and subject to obtaining prior permission from the Authority in accordance with Article 15 of this Law;</p>	<p>initiating investigation thereof.</p> <p>The controller shall be exempt from the obligation to comply with the provisions of Articles 4 in any of the following cases:-<sup>193</sup></p> <ul style="list-style-type: none"> <li>performing a task related to the public interest according to Law;</li> <li>fulfilling a legal obligation or order from a competent order;</li> <li>protecting the vital interests of the individual;</li> <li>achieving the purposes of scientific research conducted for the public interest; and</li> <li>collecting information necessary for investigation in any felony, based on an official request from the investigating authorities.</li> </ul>	<p>guardian if he is less than 18 years old.</p> <p>In all cases, the Service Provider shall be able to prove the consent of the data subject to process the data.</p>

<sup>189</sup> Bahrain Ministerial Decision No. 45/2022 Defining the Rules and Procedures for Processing Sensitive Personal Data provide further regulation to the processing sensitive personal data.

<sup>193</sup> Qatar Law No. 13/2016, Article 19

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
	<p>security, or social protection laws;</p> <p><b>Contractual Obligations:-</b> Processing is necessary to perform a contract with the Data Subject or to take steps for concluding, amending, or terminating a contract; and</p> <p><b>Legal Obligations:-</b> Processing is necessary to fulfil obligations imposed by other UAE laws on the Controller.</p> <p><b>Other Cases:-</b> Any other cases set by the Executive Regulations of the UAE Data Protection Law, which as of now, is yet to be released.</p> <p>Kindly note under the UAE Data Protection Law, legitimate interest is not a lawful basis to process personal data.</p>	<p>expectation of the Data Subject. The KSA Implementing Regulations under Article 16(2) further clarify that Legitimate interest includes the Disclosure of fraud operations, the protection of network and information security, and other Legitimate Interests that meet the conditions outlined in paragraph (1) of this article. Lastly, before processing Personal Data for Legitimate Interest the Controller must conduct an assessment of the processing and its impact on the rights and interests of the Data Subject. Article 16(3) of the KSA Implementing Regulations sets out what this assessment must include.</p> <p>Separately, Personal Data may also be collected or processed for scientific, research or statistical purposes without the owner's</p>	<p>mentioned in "Who does the law apply to."</p>	<p>processing the data provided by the owner to the public;</p> <p>processing necessary to initiate or defend any legal rights claim, including what is required in preparation for this matter;</p> <p>processing necessary for the purposes of preventive medicine, medical diagnosis, provision of health care, treatment or management of health care services by a licensed medical practitioner or any person legally bound to maintain confidentiality;</p> <p>processing carried out in the context of the activities of associations of all kinds, trade unions and other non-profit organisations, subject to the following:-</p> <ul style="list-style-type: none"> <li>processing shall be carried out within the limits of what is necessary for the purpose for which the</li> </ul>	<p>The above exemptions are also reflected in Qatar's exemptions guidelines for data controllers<sup>194</sup> and competent authorities which set out who the exemptions apply to and in what cases (among other things).<sup>195</sup></p>	

<sup>194</sup> Exemptions Applicable to Data Controllers (under Article 19) - Guideline for Regulated Entities, Article 2

<sup>195</sup> Exemptions Applicable to Competent Authorities (under Article 18) - Guideline for Regulated Entities, Article 2

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
		consent in certain instances. <sup>186</sup>		<p>association, union or organisation was established;</p> <ul style="list-style-type: none"> <li>○ processing shall be based on data belonging to the members of that association, union or organisation or to individuals with whom they have regular contact by virtue of the nature of their activity; and</li> <li>○ the data shall not be disclosed to any other person unless the Data Owner agrees;</li> </ul> <p>processing by a competent public authority to the extent required by the performance of the tasks entrusted to it by law; and</p> <p>processing data of the ethnic origin, ethnic group or religion, if necessary to ascertain the equal opportunity or treatment of members of society of different ethnic origin, ethnic group or religion, and</p>		

<sup>186</sup> Saudi Arabia Cabinet Decision No. 98/1443, Article 27.

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
				<p>subject to appropriate safeguards for the rights and freedoms of Data Owners established by law.</p> <p>An exception to these requirements is processing for journalistic, artistic or literary purposes so long as:<sup>190</sup></p> <p>the data is correct, accurate and subject to update and correction;</p> <p>measures are available to ensure that data are not used for any purpose other than for journalistic, artistic or literary purposes; and</p> <p>without prejudice legislation on press, printing and publishing.</p> <p>Article 7 of the Bahrain Data Protection Law sets out the instances where processing of personal data is permitted relating to the prosecution, initiation and rulings of criminal proceedings.</p>		

<sup>190</sup> Bahrain Law No. 30/2018, Article 6

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
<b>Record of Processing Activities</b>	<p>Controllers must maintain a special record of Personal Data that includes:-<sup>198</sup></p> <p>Controller and Data Protection Officer's information;</p> <p>description of the categories of Personal Data held;</p> <p>details of individuals authorized to access the Personal Data;</p> <p>processing durations, restrictions, and scope;</p> <p>mechanism of erasure, modification, or processing of Personal Data;</p> <p>purpose of Processing;</p> <p>Data related to the movement and Cross-Border Processing of such data; and</p>	<p>Subject to the retention requirements under the law, the Controller shall keep records of the Personal Data Processing activities.<sup>200</sup></p> <p>The KSA Data Protection Law requires the record to include:-<sup>201</sup></p> <p>the Controller's contact details;</p> <p>the purpose of the Processing the Personal Data;</p> <p>a description of the categories of Personal Data Owners;</p> <p>the entity to which the Personal Data was (or will be) disclosed;</p> <p>whether the Personal Data was (or will be) transferred outside the Kingdom or disclosed</p>	<p>Articles 28 and 29 of the Oman Implementing Regulations require controllers or processors (as the case may be) to create special record of personal data processing activities with at least the following:</p> <p>Data of the Personal Data Protection Officer.</p> <p>A description of the categories of Personal Data categories they have and the details of the persons permitted to access the Personal Data.</p> <p>Processing time periods, restrictions and scope.</p> <p>The mechanism for erasing, modifying or Processing Personal Data.</p>	<p>The Data Protection Controller shall maintain a record of the processing operations that the Data Manager shall notify the Authority of, in accordance with the provisions of Article 14 of Bahrain Data Protection Law. The Data Manager is obliged to maintain this record in the absence of a Data Protection Controller. This record shall include, at a minimum, the data to be submitted in accordance with the provisions of the said Article. The Data Protection Controller shall provide the Authority with an updated copy of this record once a month.<sup>204</sup></p>	<p>Whilst the Qatar Data Protection Law does not explicitly require a record of processing activities (ROPA), the MCGAA Guidelines on Record of Processing Activities, set out its importance. The MCGAA Guidelines state that controllers will require a ROPA to enable compliance with the requirements to<sup>205</sup>:</p> <ul style="list-style-type: none"> <li>● track consent: keep track of processing activities for which consent is obtained (Articles 4, 5.1, 17.2, 22);</li> <li>● publish a privacy notice: notify individuals of information about how the controller processes individuals' personal data via a privacy notice (Articles 6.1 and 9);</li> <li>● manage privacy assessments: keep track of Data Protection</li> </ul>	<p>The Service Provider shall:-<sup>207</sup></p> <p>keeping records of processing activities, provided that such records include the following:-</p> <ul style="list-style-type: none"> <li>○ name and contact details of the Service Provider, his representative if he is outside the State of Kuwait, and the data protection official;</li> <li>○ purposes of data processing;</li> <li>○ description of the categories of data subjects and other categories of Personal Data;</li> <li>○ transfer of Personal Data, if necessary, to a country outside the State of Kuwait with the</li> </ul>

<sup>198</sup> UAE Federal Decree-Law No. 45/2021, Article 7(4).

<sup>200</sup> Saudi Arabia Cabinet Decision No. 98/1443, Article 31

<sup>201</sup> Saudi Arabia Cabinet Decision No. 98/1443, Article 31.

<sup>204</sup> Bahrain Law No. 30/2018, Article 10(E)

<sup>205</sup> Record of Processing Activities - Guideline for Regulated Entities, Article 3

<sup>207</sup> Kuwait Administrative Decision No. 26/2024 Concerning the Issuance of the Data Privacy Protection Regulation, Article 5(4)-(5).

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
	<p>details on the technical and organizational procedures related to information security and Processing operations.</p> <p>Processors must also maintain a similar record of Personal Data processed on behalf of the Controller, and the obligations are identical as above except processors must also provide Controller, Processor, and Data Protection Officer's information.<sup>199</sup></p> <p>Such records should be provided by the Controller and Processor to the Office whenever requested to do so.</p>	<p>to an entity outside the Kingdom; and</p> <p>the expected period for retaining the Personal Data.</p> <p>The KSA Implementing Regulations clarify that a written record of Personal Data Processing activities be retained during the period of Processing, in addition to five years starting from the date of completing of the activity. This record should be accurate and up to date and should be provided upon request by the Competent Authority.</p> <p>The KSA Implementing Regulations also sets out that the record of Personal Data Processing activities shall include, at a minimum:<sup>202</sup></p> <p>Controller's name and relevant contact details.</p> <p>Information about the Data Protection Officer, where required in</p>	<p>The purpose of Processing the Personal Data.</p> <p>The entities whose Personal Data is disclosed and the purposes of disclosure.</p> <p>Data of any entity to which Personal Data is transmitted or transferred.</p> <p>Any data related to the transmission and Processing of Personal Data across borders.</p> <p>Technical and organisational procedures for information security and Processing operations.</p> <p>Any Personal Data Breach, including the facts surrounding the Breach, its effects, and the remedial or corrective action taken.</p> <p>Controllers must update the record on an ongoing basis and submit it to the</p>		<p>Impact Assessments (DPIAs) (Article 11.1);</p> <ul style="list-style-type: none"> <li>plan training: track personal data within their organisation to ensure staff who handle personal data are trained and aware of their responsibilities (Article 11.3);</li> <li>manage breaches and notifications: respond quickly and effectively to breaches involving personal data (Articles 11.5 and 13);</li> <li>verify processors' compliance: keep track of personal data shared with third parties (Article 11.8);</li> <li>manage cross-border data flows: keep track of personal data transferred to a location outside of Qatar (Article 15); and</li> <li>manage special nature processing: keep track of the processing of special nature personal data and manage</li> </ul>	<p>identification of such country; and</p> <ul style="list-style-type: none"> <li>a general description of the technical and organisational security measures used;</li> </ul> <p>making the records available for review by the Authority upon request.</p>

<sup>199</sup> UAE Federal Decree-Law No. 45/2021, Article 8(7).

<sup>202</sup> KSA Implementing Regulations, Article 33(5)

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
		<p>accordance with Article (32) of the KSA Implementing Regulation.</p> <p>Purposes of the Personal Data Processing.</p> <p>Description of the categories of Personal Data being processed and the categories of Data Subjects.</p> <p>Retention periods for each category of Personal Data, where possible.</p> <p>Categories of recipients to whom the Personal Data is disclosed.</p> <p>Description of Personal Data Transfers outside the Kingdom, including the legal basis for the Transfers and the recipients of the Personal Data.</p> <p>Description of the procedures and the organizational, administrative, and technical measures in place that ensure the</p>	Competent Department whenever requested.		<p>permissions (Article 16).</p> <p>The NCGAA set out examples of what information to include in ROPAs which are (without limitation)<sup>206</sup>:</p> <ul style="list-style-type: none"> <li>• the name and contact details of the senior responsible staff member for privacy at the organization;</li> <li>• the name and contact details of the owner of each process;</li> <li>• the purpose of the processing;</li> <li>• the permitted reason for processing;</li> <li>• the categories of individuals whose personal data is processed;</li> <li>• the categories of personal and/or special nature personal data processed;</li> <li>• information regarding the DPIA for the processing activity;</li> </ul>	

<sup>206</sup> Record of Processing Activities - Guideline for Regulated Entities, Article 4.2

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
		<p>security of Personal Data, where possible.</p> <p>A template of such record is to be provided by the Competent Authority.<sup>203</sup></p>			<ul style="list-style-type: none"> <li>any internal parties with whom personal data is shared e.g. another department within the controller's organisation;</li> <li>if applicable, the name or category and geographic location of any external third parties or organisations that personal data is transferred to;</li> <li>information on how long the controller retains the personal data being processed; and</li> <li>a general description of the controller's administrative, technical and financial precautions specifically related to security.</li> </ul>	
<b>Notice</b>	<p>Controllers must provide Data Subjects with the following information before Processing their Personal Data:<sup>208</sup></p>	<p>Under Article 12 of the KSA Data Protection Law, a Controller must adopt a privacy policy and make it available to Personal Data Owners</p>	<p>The Controller shall, before proceeding with the Processing of any Personal Data, notify the Personal Data</p>	<p><b>Data Owner - direct</b></p> <p>In cases where the data is obtained directly from the Owner, the Data Manager shall inform them when registering</p>	<p>The controller shall, prior to the processing of any personal data, inform the individual of the following:-<sup>222</sup></p> <p>the data of the controller or any other</p>	<p>The Service Provider shall, before providing the service to the User, do the following:-<sup>223</sup></p> <p>provide all service information and conditions and</p>

<sup>203</sup> KSA Implementing Regulation of the Personal Data Protection Law, Article 33(6)

<sup>208</sup> UAE Federal Decree-Law No. 45/2021, Article 13(2).

<sup>222</sup> Qatar Law No. 13/2016, Article 9

<sup>223</sup> Kuwait Administrative Decision No. 26/2024 Concerning the Issuance of the Data Privacy Protection Regulation, Articles 2.

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
	<p>purposes of Processing;</p> <p>sectors or establishments with which Personal Data is to be shared, whether inside or outside the UAE; and</p> <p>protection measures for Cross-Border Processing made in accordance with the law.</p> <p>Such information can be provided in a privacy policy along with other information including how Data Subjects can communicate with the Controller and request the exercise of any of their rights.<sup>209</sup></p>	<p>when collecting their data.</p> <p>The privacy policy must specify the purpose of the Collection, the content of the Personal Data to be collected, the method of Collection, the means of storage, the method of Destruction, the rights of the data owner in relation thereto and the method of exercising these rights.</p> <p><u>Direct</u></p> <p>Where the Controller collects Personal Data from its owner directly, it must inform him of:<sup>210</sup></p> <p>the legal justification for collecting his Personal Data;</p> <p>the purpose of collecting his Personal Data, and whether the Collection of all or some of it is obligatory or</p>	<p>owner in writing of the following:-<sup>212</sup></p> <p>Data of the Controller and the Processor;</p> <p>contact information with the Personal Data protection officer;</p> <p>the purpose of Processing the Personal Data, and the source from which it was collected;</p> <p>a comprehensive and accurate description of the Processing and its procedures, and the degrees of disclosure of Personal Data;</p> <p>the rights of the Personal Data Owner, including the right to access, correct, transfer and update the data; and</p> <p>any other information that may be necessary for fulfilling the</p>	<p>the data of the following:-<sup>216</sup></p> <p>full name of the Data Manager, the scope of their work or their occupation, as appropriate, and their address;</p> <p>the purposes for which the data are intended to be processed; and</p> <p>any other necessary information, depending on the circumstances of each case, which would ensure that the processing is fair to the Data Owner, including the following:-</p> <ul style="list-style-type: none"> <li>o names or categories of data providers;</li> <li>o a statement on whether the answer to any questions addressed to the Data Owner is mandatory or optional and,</li> </ul>	<p>party that is engaged in the processing of data on behalf of the controller or for exploitation;</p> <p>Legitimate Purposes pursued by the controller or any other party for which the personal data are being processed;</p> <p>comprehensive and accurate description of the processing activities, and degrees of disclosure of personal data for Legitimate Purposes. In case the controller is unable to perform so, then he must enable the individual to have a general description of the same; and</p> <p>any other information deemed significant and necessary to fulfil the requirements for processing of personal data.</p>	<p>requesting change or cancellation of data, clarified in easy terms, to be available in both English and Arabic;</p> <p>obtain the consent of the service applicant to collect or process Personal Data and ensure his knowledge and acceptance of all conditions, obligations and provisions of data collection and processing; and</p> <p>clarify the purpose of collecting the User's Personal Data that is necessary to provide the service and how such data is used.</p> <p>Additionally, the Service Provider shall, during the provision of the service or after its termination, collect and process data according to the following conditions:-<sup>224</sup></p> <p>providing clear and easily accessible</p>

<sup>209</sup> UAE Federal Decree-Law No. 45/2021, Article 19.

<sup>210</sup> Saudi Arabia Cabinet Decision No. 98/1443, Article 13

<sup>212</sup> Oman Sultani Decree No. 6/2022, Article 14

<sup>216</sup> Bahrain Law No. 30/2018, Article 17(1)

<sup>224</sup> Kuwait Decision No. 42/2021 On the Data Privacy Protection Regulation as amended by virtue of Article 1 of Kuwait Decision No. 244/2023, Articles 4.

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
		<p>optional, as well as informing him that his data will not be processed in a manner inconsistent with the purpose of its Collection or in cases other than those provided for in Article (10);</p> <p>the identity and reference address of the person collecting the Personal Data when necessary, unless the Collection is for security purposes;</p> <p>the entity or entities to which the Personal Data will be disclosed, their capacity, and whether the Personal Data will be transferred, disclosed or processed outside the Kingdom;</p> <p>the possible effects and risks of the failure to complete the Personal Data Collection procedure;</p> <p>his rights under the law; and</p>	<p>conditions of Processing.</p> <p>The Oman Implementing Regulations, require the Controller or the Processor - as the case may be - shall be obligated to put a Personal Data Protection policy in a visible place that allows the Personal Data Subject to view it before Processing their data, provided that this policy includes - at a minimum - the mechanism and procedures for the Personal Data Subject to exercise their rights as stipulated in the Law and these Regulation.<sup>213</sup></p> <p>Before sending any advertising, marketing or commercial material to the Personal Data Subject, the Controller must (among other things) obtain the written consent of the Personal Data Subject and notify them of the means of sending advertising, marketing</p>	<p>where appropriate, the consequences of not answering;</p> <ul style="list-style-type: none"> <li>○ a statement on the right of the Data Owner to be notified, if so requested, of their data in full and of its right to be corrected;</li> <li>○ a statement on whether the data will be used for direct marketing purposes; and</li> <li>○ any other information requiring the Data Owner to exercise their rights under the provisions of this Law.</li> </ul> <p><b>Data Owner - indirect</b></p> <p>If data of a Data Owner is obtained from a non-Owner, the Data Manager must inform the Data Owner within five days of starting the registration of the data of the following:-<sup>217</sup></p>	<p>The Privacy Notice NCGAA Guidelines also provides further information on privacy notices including what it should include, for example in brief:</p> <ul style="list-style-type: none"> <li>● what details to include about the controller;</li> <li>● what details to include about third party processors;</li> <li>● the permitted reasons for processing;</li> <li>● permitted reasons for any third party processors; and</li> <li>● a comprehensive and accurate description of the processing activities.</li> </ul> <p>According to the NCGAA Guidelines on Privacy Notice, if controllers obtain personal data from other sources, they must provide individuals with privacy information within a reasonable period of</p>	<p>information about the relevant practices and policies with respect to Personal Data to ensure that collection and processing is conducted transparently; and</p> <p>the Service Provider shall create and maintain a written privacy policy that:-</p> <ul style="list-style-type: none"> <li>○ describe in detail the Service Provider's processes and procedures with respect to the collection, use and disclosure of Personal Data, including the method of compliance; and</li> <li>○ shall be published on the website of the Service Provider and be provided to Users when contracting for services.</li> </ul> <p>Additionally, the Service provider under Article 5 shall developing and</p>

<sup>213</sup> Oman Ministerial Decision No. 34/2024, Article 21

<sup>217</sup> Bahrain Law No. 30/2018, Article 17(2)

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
		<p>the other elements determined by the Regulations according to the nature of the activity carried out by the Controller.</p> <p>The KSA Implementing Regulations in Article 4(1) further sets out the information a Controller must inform a Data Subject before (directly) collecting their personal data. The following information must be provided to the Data Subject if not already and if it doesn't conflict with any KSA laws. Such information is the:-</p> <p>Controller's identity, its contact details, and any other details related to the channels established by the Controller for the purpose of communicating in relation with Personal Data protection. Article 10 of KSA Implementing Regulations sets out the means to process requests including (but not limited to) email,</p>	<p>or commercial materials.<sup>214</sup></p> <p>Additionally, when processing a child's personal data, the controller or processor (as the case may be) is required for the purpose of the processing to be clear, direct, safe and free of fraud or misleading.<sup>215</sup></p>	<p>the information referred to above;</p> <p>the purposes for which the data were collected; and</p> <p>any other necessary information, depending on the circumstances of each case, which would make the processing fair for the Data Owner, including the following:-</p> <ul style="list-style-type: none"> <li>○ the information referred to in Item 1/C of this Article;</li> <li>○ Data categories; and</li> <li>○ the data source, except in cases where a legal obligation to preserve the secrets of a profession requires a lack of disclosure.</li> </ul> <p>The aforementioned requirements of obtaining data from a</p>	<p>obtaining the data and no later than one month.</p>	<p>adhering to internal policies for protection and data privacy.</p>

<sup>214</sup> Oman Ministerial Decision No. 34/2024, Article 22

<sup>215</sup> Oman Ministerial Decision No. 34/2024, Article 12

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
		<p>text messages and communication via electronic applications;</p> <p>contact details of the data protection officer appointed by the Controller;</p> <p>the legal basis and a specific, clear, and explicit purpose for collecting and Processing Personal Data;</p> <p>the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;</p> <p>explanation about Data Subject's rights, as stipulated in Article (4) of the Law and the mechanisms for exercising those rights;</p> <p>explanation on how to withdraw consent given to process of any Personal Data; and</p> <p>explaining whether collecting or Processing</p>		<p>non-Owner do not apply:<sup>218</sup></p> <p>if the data is processed for historical, statistical or scientific purposes, and the control of the Data Owner of the data referred to is not possible or requires extraordinary cumbersome efforts. The Board of Directors shall issue a decision specifying the conditions and status of such cases; and</p> <p>if the processing of the data is for the purpose of implementing an obligation established by law, contrary to a contractual obligation, or an order from a competent court, the Public Prosecutor, an investigating judge, or the Military Prosecution.</p> <p><u>Authority</u></p> <p>For completeness, Article 14 sets out the notification conditions and requirement to the Authority. Apart from the cases set out in Article 14(1)(A-D), the</p>		

<sup>218</sup> Bahrain Law No. 30/2018, Article 17(3)

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
		<p>Personal Data is mandatory or optional.</p> <p><u>Indirect</u></p> <p>If Personal Data is collected indirectly (i.e from an individual other than the Data Subject) the information from Article 4(1) of the KSA Implementing Regulations along with the categories of Personal Data being processed and the source from which the Controller obtained it, must be provided to the Data Subject without undue delay and within 30 days. There are certain exceptions to this including if:-</p> <p>the information is already available to the Data Subject;</p> <p>the implementation is not possible or requires disproportionate effort;</p> <p>the Controller obtained the data in accordance with a law;</p> <p>the Controller is a Public Entity and the</p>		<p>Data Manager shall notify the Authority before the start of the processing operations that are automated in whole or in part, or for a group of operations for the purpose of achieving one or several related purposes. Such a notice must include:-<sup>219</sup></p> <p>the name and address of the Data Manager and the Data Processor, if any;</p> <p>the purpose for processing;</p> <p>a description of the data and statement of categories of Data Owners and recipients of these data or their categories;</p> <p>any intended transfer of data to a country or territory outside the Kingdom; and</p> <p>a statement that enables the Authority to assess in principle the adequacy of the measures available to meet the security requirements referred</p>		

<sup>219</sup> Bahrain Law No. 30/2018, Article 14(2)

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
		<p>Collection of Personal Data is for security purposes, or to fulfil judicial requirements, or to achieve a Public Interest; and</p> <p>the Personal Data is subject to professional confidentiality provisions established by law.</p> <p><u>Continuous and large-scale Processing, continuous monitoring of Data Subjects, adoption of new technologies or making automated decisions</u></p> <p>Under Article 4(5) of the KSA Implementing Regulations, the Controller must inform the Data Subject of the information in Article 4(1) as well as the following information when it requires continuous and large-scale Processing on individuals that fully or partially lack legal capacity, continuous monitoring of Data Subjects, adoption of</p>		<p>to in Article 8 of this Law.</p> <p>The Board of Directors issued a decision to instead provide a simplified notification which should follow the information set out in Article 14(3).<sup>220</sup></p> <p>The Data Manager must inform the Authority of any changes to the information within 30 days from the date of change.</p> <p>Additionally, it is prohibited to carry out the following processing without prior written permission from the Authority:-<sup>221</sup></p> <p>automatic processing of sensitive personal data, in the case referred to in Item 2 of Article 5 of this Law;</p> <p>automated processing of biometrics data that are used for personal identification;</p>		

<sup>220</sup> Bahrain Ministerial Decision No. 44/2022 On the Rules and Procedures for Submitting a Notification to the Personal Data Protection Authority and an Application for Prior Authorisation for Processing and Deciding Thereon

<sup>221</sup> Bahrain Law No. 30/2018, Article 15(1)

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
		<p>new technologies or making automated decisions:-</p> <p>means and methods of collecting and Processing Sensitive Data;</p> <p>means and procedures taken to protect Personal Data; and</p> <p>indicate whether decisions will be made based solely on automated Processing of Personal Data.</p> <p><u>Additional purpose</u><sup>211</sup></p> <p>The Controller must provide Data Subjects with the necessary information where processing of Personal Data is done for a purpose other than the one it was initially collected for. This must be done before conducting the additional Processing.</p> <p>According to Article 4(7) of the KSA Implementing Regulations, the Controller shall provide</p>		<p>automated processing of genetic data, except for processing by doctors and specialists in a licensed medical facility and that necessary for preventive medicine, medical diagnosis, treatment or health care;</p> <p>automated processing involving the linking of personal data files of two or more Data Managers handled by them for different purposes; and</p> <p>processing that is an optical recording used for monitoring purposes.</p> <p>Pease see Articles 14 and 15 of the Bahrain Data Protection Law along with Bahrain Ministerial Decision No. 44/2022 On the Rules and Procedures for Submitting a Notification to the Personal Data Protection Authority and an Application for Prior Authorisation for Processing and</p>		

<sup>211</sup> KSA Implementing Regulation of the Personal Data Protection Law, Article 4(6)

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
		the required information in an appropriate language as stipulated in this Article when aware that the Data Subject fully or partially lacks legal capacity.		Deciding for more information.		
<b>Transfer</b>	<p><b>Cross-Border Data Transfer (with adequate protection)</b><sup>225</sup></p> <p>Personal Data may be transferred outside the UAE in the following cases approved by the Office:-</p> <p>the destination country or territory has specific data protection legislation including the most important provisions for protecting the privacy and confidentiality of Personal Data, Data Subject's ability to exercise their rights and provisions related to imposing appropriate measures on the Controller or Processor</p>	<p>Under the KSA Data Protection Law, Personal Data may be transferred or disclosed to an entity outside the Kingdom for the following purposes:-<sup>227</sup></p> <p>to meet an obligation under an agreement to which the Kingdom is a party;</p> <p>if it serves the interests of the Kingdom;</p> <p>to meet an obligation to which the Personal Data Owner is a party; and</p> <p>to achieve other purposes as</p>	<p>Without prejudice to the competencies prescribed for the Cyber Defense Centre, the Controller may transfer Personal Data outside Oman, so long as the personal data transferred has not been processed in violation of the Oman Law, nor cause harm to the Personal Data Owner<sup>229</sup>.</p> <p>The Oman Implementing Regulations also require transfers of personal data to not result in violation of national security or the</p>	<p><u>Transfer of personal data to countries and territories that provide adequate protection.</u><sup>235</sup></p> <p>The Data Manager is prohibited from transferring personal data outside the Kingdom, except in the following cases:-</p> <p>transfer to a country or territory included in a statement prepared and updated by the Authority, including the names of the countries and territories that the Authority ascertains have legislation or regulations in place to ensure an adequate level of protection for personal data, and such a disclosure shall</p>	<p>Without prejudice to the obligations set forth in the present Law, the controller may not take any decision or measure that may restrict the cross-border data flows, except if the processing of such data violates the provisions of the present Law, or may inflict serious damage to the personal data or privacy of the individual.<sup>238</sup></p> <p>The controller must, when disclosing or transmitting personal data to the processor, ensure their compliance with Legitimate Purposes, and that such data are processed in accordance with the</p>	<p>The Service Provider shall, during the provision of the service or after its termination, collect and process data according to the following conditions:-<sup>241</sup></p> <p>providing information on the place where Personal Data is stored, if it is inside or outside the State of Kuwait;</p> <p>notifying the data subject if the Service Provider intends to transfer his Personal Data outside the State of Kuwait; and</p> <p>There are separate non-disclosure and</p>

<sup>225</sup> UAE Federal Decree-Law No. 45/2021, Article 22.

<sup>227</sup> Saudi Arabia Cabinet Decision No. 98/1443, Article 29(1)

<sup>229</sup> Oman Sultani Decree No. 6/2022, Article 23

<sup>235</sup> Bahrain Law No. 30/2018, Article 12

<sup>238</sup> Qatar Law No. 13/2016, Article 15

<sup>241</sup> Kuwait Administrative Decision No. 26/2024 Concerning the Issuance of the Data Privacy Protection Regulation, Article 6.

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
	<p>through a supervisory or judicial authority; and</p> <p>if the UAE has bilateral or multilateral agreements related to data protection with the destination countries.</p> <p><b>Cross-Border Data Transfer (without adequate protection)</b><sup>226</sup></p> <p>Personal Data may be transferred to a jurisdiction not recognised by the Office as having adequate data protection in the following cases:-</p> <p>under a contract or agreement obliging the company in the destination jurisdiction to implement the provisions, measures, controls and requirements as under the UAE Data Protection Law. Eg.</p>	<p>determined by the Regulations.</p> <p>Regulation on Personal Data Transfer Outside the Kingdom (“<b>Transfer Regulations</b>”) set out under Article 2 other purposes including:</p> <p>to perform necessary operations for central processing to enable the controller to conduct its activities. Operational Processes is defined under the Transfer Regulations a set of procedures related to the operational processes essential for the controller’s activities, including human resources operations, billing, accounting, and other workflow-related procedures. to include human resources operations, billing, accounting, and other workflow-related procedures;</p>	<p>supreme interests of Oman.<sup>230</sup></p> <p>Before transmitting or transferring Personal Data outside Oman, the Controller must:</p> <ol style="list-style-type: none"> <li>1. obtain the express consent of the Personal Data Subject. This is not required if:<sup>231</sup> <ul style="list-style-type: none"> <li>• the transfer or transmission is carried out in implementation of an international obligation under an agreement to which Oman is a party; or</li> <li>• the transfer or transmission is carried out in a way that leads to concealing the identity of the Personal Data Subject, not linking this data to him and making him</li> </ul> </li> </ol>	<p>be published in the Official Gazette; or</p> <p>transfer with permission issued by the Authority on a case-by-case basis, if it is estimated that the data will have an adequate level of protection. The assessment of the Authority shall take into account all the circumstances surrounding the data transfer process, in particular the following:-</p> <ul style="list-style-type: none"> <li>○ the nature of the data to be transferred, the purpose and duration of the data processing;</li> <li>○ the measures in place to protect personal data in the source and destination country or territory; and</li> <li>○ international conventions and relevant legislation</li> </ul>	<p>provisions of the present Law.<sup>239</sup></p> <p>According to the Qatar guidelines on exemptions, if a competent authority processes any personal data in relation to the purposes stated in Article 18 of the Qatar Data Protection Law, it will not need to comply with the requirements for cross-border transfers, and may transfer such personal data outside of Qatar and to any free zone not subject to the requirements of the Qatar Data Protection Law (for example the QFC), as required<sup>240</sup>.</p> <p>We would note that the Personal Data Management System NCGAA Guidelines set out checklist for cross border transfers which include:</p>	<p>confidentiality provisions in the law.</p>

<sup>226</sup> UAE Federal Decree-Law No. 45/2021, Article 23.

<sup>230</sup> Oman Ministerial Decision No. 34/2024, Article 37

<sup>231</sup> Oman Ministerial Decision No. 34/2024, Article 37

<sup>239</sup> Qatar Law No. 13/2016, Article 12

<sup>240</sup> Exemptions Applicable to Competent Authorities (under Article 18) - Guideline for Regulated Entities, Article 6.3

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
	<p>Standard Contractual Clauses (SCCs);</p> <p>obtaining explicit Consent from the Data Subject;</p> <p>if the transfer is necessary to fulfil obligations and establish, exercise or defend rights before judicial authorities;</p> <p>if the transfer is necessary to enter into or execute a contract between the Controller and Data Subject, or between the Controller and third party for the Data Subject's interest;</p> <p>if the transfer is necessary to perform a procedure relating international judicial cooperation; and</p> <p>if the transfer is necessary to protect public interest.</p> <p>The Executive Regulations, once issued, will set out the</p>	<p>to provide a service or benefit to the subject of the personal data; or</p> <p>to conduct scientific research and studies.</p> <p>Where Personal Data is transferred or disclosed under these permitted purposes, the following conditions should also be met (except in cases of extreme necessity to preserve the life or vital interests of the Personal Data Owner or to prevent, examine or treat an infectious disease). The transfer or disclosure must:<sup>228</sup></p> <p>not cause any prejudice to the national security or the vital interests of the Kingdom;</p> <p>be an appropriate level of protection for Personal Data outside the Kingdom; and</p> <p>be limited to the minimum amount of Personal Data needed.</p>	<p>unidentifiable in any way.</p> <p>2. Ensure that the Third Party Processor has adequate degree of protection for Personal Data that is not less than the level of protection established in accordance with the <b>Oman Data Protection Law</b> and <b>Oman Implementing Regulations</b>.<sup>232</sup></p> <p>3. Conduct an assessment of the level of protection provided by the Third Party Processor and the risks of transmitting or transferring Personal Data, provided that the assessment includes in particular the following.<sup>233</sup></p>	<p>in force in the country or territory to which the data will be transferred. Such a declaration may be conditional or for a specified period of time.</p> <p>Bahrain Ministerial Decision No. 42/2022 On the Transfer of Personal Data Outside the Kingdom of Bahrain contains the list of countries and territories that ensure an adequate level of protection for personal data as well as sets out the process for submitting an application for the Authority's authorisation to transfer personal data outside Bahrain.<sup>236</sup> The regulations also set out the transfer obligations for transfers of personal data outside Bahrain within a regional or international group; or to a data manager or third party outside</p>	<p>● "we recognise when conducting cross-border data transfers that 'may cause serious damage to an individual's personal data or privacy' appropriate safeguards must be put in place to protect individuals and have a process for doing so.</p> <p>● we have identified our processing activities that involve cross-border data transfers and have put appropriate safeguards in place to protect the personal data involved, unless an exception can be provided for."</p> <p>The NCGAA Guidelines on Data Protection Impact Assessments explain that the Qatar Data Protection Law PDPPL explicitly states two specific ways of processing that may cause serious damage. These are:</p>	

<sup>228</sup> Saudi Arabia Cabinet Decision No. 98/1443, Article 29(2)

<sup>232</sup> Oman Ministerial Decision No. 34/2024, Article 38

<sup>233</sup> Oman Ministerial Decision No. 34/2024, Article 39

<sup>236</sup> Bahrain Ministerial Decision No. 42/2022 On the Transfer of Personal Data Outside the Kingdom of Bahrain

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
	controls and requirements for these cases.	<p>The Transfer Regulations set out under Article 3 the procedures and standards for evaluating the level of Personal Data protection outside the Kingdom.</p> <p><b>Exceptions</b></p> <p>Article 4 of the Transfer Regulations sets out cases where the controller is exempt from complying with the aforementioned conditions of appropriate level of protection and minimum amount of personal data. These are where appropriate safeguards are used in certain cases such as:</p> <p>A. If the transfer or disclosure of personal data is to be made between public bodies to implement an agreement to which the Kingdom is a party or to serve its interests, the controllers must include standard provisions for the protection of personal data in the relevant agreements or</p>	<ul style="list-style-type: none"> <li>• A description of the nature and size of the Personal Data to be transmitted or transferred, and its sensitivity degree.</li> <li>• The purpose of Personal Data Processing, the scope of Processing, and the parties with whom the Personal Data will be shared.</li> <li>• The time period for Personal Data Processing, and whether it will be carried out in a restricted or occasional manner only once or repeatedly and regularly over a limited period.</li> <li>• The stages of transmission or transfer of Personal Data, the countries it may pass through, and the determination of the final</li> </ul>	<p>Bahrain based on a contract.</p> <p><u>Exceptions – transfers to non-adequate jurisdictions:</u><sup>237</sup></p> <p>The Data Manager may transfer personal data outside the Kingdom to a country or territory that does not provide adequate data protection in any of the following cases:-</p> <p>if the Data Owner agrees to such a transfer;</p> <p>if such a transfer of data is derived from a registry created in accordance with the Law for the purpose of providing information to the public, whether access to this registry is available to all or limited to stakeholders under certain conditions. In such a case, such information shall satisfy the conditions prescribed for the registry; and</p>	<ul style="list-style-type: none"> <li>• transferring personal data outside Qatar, known as a cross-border data transfer; and</li> <li>• processing personal data of a special nature, specific categories of personal data also known as sensitive personal data.</li> </ul> <p>This could mean that a DPIA should be done for such processing.</p>	

<sup>237</sup> Bahrain Law No. 30/2018, Article 13

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
		<p>memoranda of understanding.</p> <p>B. If the transfer or disclosure is non-recurring or for a limited period and involves a limited number of data subjects, the controller must comply with the standard contractual clauses. Alternatively, if the transfer or disclosure is made to a body that has received an approval certificate from an entity licensed by the competent authority and the data is not sensitive.</p> <p>C. If the transfer or disclosure of personal data is necessary to perform central operations and the controller is part of a group of multinational entities, the controller and its affiliates must comply with binding common rules or standard contractual clauses that ensure adherence to the requirements stipulated by the Law and Regulations. Alternatively, the entity to which the personal</p>	<p>destination of the Personal Data.</p> <ul style="list-style-type: none"> <li>The effects and risks that may result from the transmission or transfer process, and the extent of their impact on the Personal Data Subject.</li> </ul> <p>The Ministry may request a copy of the assessment report prepared by the Controller to check the extent of adequacy of the level of protection provided by the Third Party Processor.<sup>234</sup></p>	<p>if such a transfer is necessary for any of the following:-</p> <ul style="list-style-type: none"> <li>implementing a contract between the Data Owner and the Data Manager, or taking preliminary steps at the request of the Data Owner with a view to concluding a contract;</li> <li>execution or conclusion of a contract between the Data Manager and a third party for the benefit of the Data Owner;</li> <li>protecting the vital interests of the Data Owner;</li> <li>implementation of an obligation prescribed by law, different to a contractual obligation, or an order issued by a competent court, the public prosecutor, the investigating judge, or the</li> </ul>		

<sup>234</sup> Oman Ministerial Decision No. 34/2024, Article 40

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
		<p>data will be transferred or disclosed must obtain a certificate of approval issued by a body licensed by the competent authority.</p> <p>D. If the transfer or disclosure is made to provide a service or benefit directly to the data subject in a manner that does not violate their expectations or conflict with their interests, and if the transfer or disclosure is to a party that has received an approval certificate from a body licensed by the competent authority, provided that the data must not be sensitive.</p> <p>E. If the transfer or disclosure of personal data is necessary for conducting scientific research and studies, it must be limited to the minimum amount of data required. The controller must either comply with standard contractual clauses or ensure that the transfer or disclosure is made to a body that has received an approval certificate from an entity licensed by the</p>		<p>military prosecution; and</p> <ul style="list-style-type: none"> <li>o investigation of, directly claiming or defending a legal claim.</li> </ul> <p>Without prejudice to the above, the Authority may authorize the transfer of personal data, or a group thereof, to a country or territory that does not provide an adequate level of protection, if the Data Manager provides adequate safeguards for the protection of the privacy, fundamental rights and freedoms of individuals. In particular, such guarantees may be in accordance with the contract of one of the parties to the Data Manager, and the Authority shall in this case grant approval, meeting certain conditions.</p>		

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
		<p>competent authority, provided that the data must not be sensitive.</p> <p>If a controller relies on the Article 4 appropriate safeguards instead of meeting all the conditions, it must conduct a transfer risk assessment before transferring or disclosing personal data to a party outside the Kingdom. The risk assessment should include and meet the requirements set out under Article 7 (2) of the Transfer Regulations.</p> <p>A risk assessment is also required where sensitive personal data is being transferred or disclosed to entities outside the Kingdom on a continuous or widespread basis.</p> <p>We would note that SDAIA has issued a Risk Assessment Guideline for Transferring Personal Data Outside the Kingdom.</p>				

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
<b>Data Protection Officer</b>	<p>A Data Protection Officer, with sufficient skills and knowledge of Personal Data Protection, must be appointed (whether inside or outside the UAE) by the Controller and Processor where the processing:-<sup>242</sup></p> <p>would cause high-level risk to the privacy of Personal Data of the Data Subject due to adopting technologies that are new or associated with the amount of data;</p> <p>involves a systematic and comprehensive assessment of Sensitive Personal Data (including Profiling and Automated Processing); or</p> <p>is made on a large amount of Sensitive Personal Data.</p> <p>The Executive Regulations, once issued, will provide more information on the types of technologies</p>	<p>Under Article 32 of the KSA Implementing Regulations, a data protection officer should be appointed where:-</p> <p>the Controller is a Public Entity that provides services involving Processing of Personal Data on a large scale;</p> <p>primary activities of the Controller consist of Processing operations that require regular and continuous monitoring of individuals on a large scale; and</p> <p>core activities of the Controller consist of Processing sensitive Personal Data.</p> <p>The data protection officer may be an official, an employee or an external contractor of the Controller.<sup>244</sup></p> <p>Article 32(3) sets out the responsibilities of the data protection officer and clarifies in</p>	<p>Controllers are required to appoint a Personal Data Protection Officer, according to the following controls:<sup>245</sup></p> <ul style="list-style-type: none"> <li>• They shall be qualified to carry out the tasks stipulated in Article (35) of The Oman Implementing Regulation.</li> <li>• They shall be familiar with the Law, Regulation, and the Personal Data Protection practices followed by the Controller or the Processor.</li> <li>• They shall be professionally competent and capable of dealing regularly and correctly with all issues related to the Personal Data Protection.</li> </ul> <p>Controllers must publish data relating to the Personal Data Protection Officer,</p>	<p>Data Manager is defined under the Bahrain Data Protection Law as a person who decides, individually or in association with others, the purposes and means of processing certain personal data. Where such purposes and means are established by the Law, the person responsible for the processing shall be the Data Manager.</p> <p>There are various provisions in relation to the Data Manager including processing requirements under Article 8.</p> <p>Under Article 10(4), the Data Manager may appoint an observer for data protection. However, the Board of Directors may issue a decision requiring certain categories of Data Managers to appoint an observer for data protection. In all cases, the Data Manager shall notify the Authority of the</p>	<p>No clearly defined DPO requirement, however, the Data Privacy Impact Assessment (DPIA) NCGAA Guidelines, states that a DPIA should be completed by a person or group of people that bring together, among others, sufficient understanding of Qatar Law No. 13/2016 requirements and data protection concepts and practices, which is often provided by a "data protection officer or champion".</p>	<p>There is no clearly defined DPO requirement.</p>

<sup>242</sup> UAE Federal Decree-Law No. 45/2021, Article 10.

<sup>244</sup> KSA Implementing Regulation of the Personal Data Protection Law, Article 32(2)

<sup>245</sup> Oman Ministerial Decision No. 34/2024, Article 34

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
	<p>and criteria to determine the amount of data requiring a Data Protection Officer.</p> <p>Separately, the Controller or Processor should specify and notify the Office of the contact address of the Data Protection Officer.<sup>243</sup></p> <p>The UAE Data Protection Law further sets out the responsibilities of the Data Protection Officer (Article 11) and the obligations of the Controller and Processor toward the Data Protection Officer (Article 12).</p>	<p>Article 32(4) that the Competent Authority shall issue rules for the appointment and instances of appointment.</p>	<p>including their name and contact information, by any means, and the Personal Data Subject shall have the right to contact the Personal Data Protection Officer in all matters related to the Processing of their Personal Data.<sup>246</sup></p>	<p>appointment referred to within three working days of doing so.</p> <p>Bahrain Ministerial Decision No. 46/2022 On Data Protection Controllers sets out (among other things) the conditions and procedures for registering an external data protection controller<sup>247</sup> (for physical or juristic person) or internal data protection controller.<sup>248</sup> The obligations of both internal and external data controllers are also set out the regulations under Article 13 and include:</p> <ul style="list-style-type: none"> <li>disclosing to the Data Manager any conflict of interests with his/ its task;</li> <li>not disclosing any information or data related to the Data Manager or the nature or secrets of the work that</li> </ul>		

<sup>243</sup> UAE Federal Decree-Law No. 45/2021, Article 10(2).

<sup>246</sup> Oman Ministerial Decision No. 34/2024, Article 36

<sup>247</sup> External Data Protection Controller: Any physical or juristic person who is registered in the Data Protection Controllers Register.

<sup>248</sup> Internal Data Protection Controller: Any physical person who works for the Data Manager to exercise the duties of a data protection controller and is registered in the Data Protection Controllers Register.

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
				<p>reached his knowledge or were under his/ its sight or accessible thereto by virtue of his/ its work as a Data Protection Controller or using any of this information or data for his/ its personal benefit or the interest of others unlawfully. Such information and data include, but are not limited to, business secrets, data of customers, employees and clients of the Data Manager, data of informational, technical, and technical systems, and other similar information and data.</p> <p>Under Article 2(3) of the Bahrain Data Protection Law, every legal person who does not normally reside in the Kingdom and has no place of business in the Kingdom processing data using means available in the Kingdom, unless the purpose of using such means is merely to transfer data through</p>		

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
				the Kingdom, shall appoint a representative authorised by them in the Kingdom to carry out their duties under the provisions of this Law and shall notify the Authority immediately upon making such an appointment and any change thereof. Such an appointment does not preclude the Authority or third parties from taking any legal action against the Data Manager in the event of breach of any of its duties referred to.		
<b>Data Processing Impact Assessment</b>	A Controller, in coordination with the Data Protection Officer, is required to conduct a Data Protection Impact Assessment, before processing, when using any modern technologies that would pose a high risk to the privacy and confidentiality of the Personal Data of the Data Subject where:- <sup>249</sup>	The KSA Data Protection Law requires Controllers to conduct an assessment of the Processing for any product or service provided to the public. <sup>251</sup>  The KSA Implementing Regulations under Article 25 set out the conditions and instances of conducting an impact assessment.	Kindly note the transfer impact assessment requirement in the "Transfer" column.  Otherwise, under Article 13 of the Oman Data Protection Law, the Controller shall establish the controls and procedures to be complied with when Processing Personal Data, including, in	Under Article 3 of Bahrain Ministerial Decision No. 43/2022 Defining the Requirements to be Met in Technical and Organisational Measures to Protect Personal Data, Data Managers may conduct a Data Protection Impact Assessment during processing procedures, taking into account the nature, scope, context, purposes, and high	Under Article 11.1 of the Qatar Data Protection Law, controllers should take the following measures:- <sup>258</sup>  reviewing the measures for protection of privacy before listing new processing operations;  identifying the processors responsible	There is no clearly defines DPIA requirement.

<sup>249</sup> UAE Federal Decree-Law No. 45/2021, Article 21(2).

<sup>251</sup> Saudi Arabia Cabinet Decision No. 98/1443, Article 22

<sup>258</sup> Qatar Law No. 13/2016, Article 11

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
	<p>the Processing involves a systematic and comprehensive assessment of the personal aspects of the Data Subject based on Automated Processing, including Profiling, which would have legal consequences or would seriously affect the Data Subject; and</p> <p>if the Processing will be made on a large amount of Sensitive Personal Data.</p> <p>The Data Protection Impact Assessment should:<sup>250</sup></p> <p>have a clear and systematic explanation of the impact of the proposed Processing and the purpose of such Processing;</p> <p>assess the necessity and suitability of Processing for the purpose thereof;</p> <p>assess the potential risks to the privacy and confidentiality of the</p>	<p>Under Article 25(1) Controllers must prepare a written and documented assessment of the potential impact and risks affecting the Data Subject where the:-</p> <p>the processing is of Sensitive Data;</p> <p>collecting, comparing, or linking two or more sets of Personal Data obtained from different sources;</p> <p>the activity of the Controller includes - continuous and large scale – Processing of Personal Data of those who fully or partially lack legal capacity, or Processing operations that by their nature require continuous monitoring of Data Subjects, or Processing Personal Data using new technologies, or making decisions based on automated Processing of Personal Data; and</p>	<p>particular, the following:-</p> <p>identifying the risks that the Personal Data Owner may sustain as a result of the Processing;</p> <p>the procedures and controls for transmitting and transferring Personal Data;</p> <p>technical and procedural measures to ensure that the Processing is carried out in accordance with the provisions of this Law; and</p> <p>any other controls or procedures specified in the Regulations.</p>	<p>risks of the processing on the rights and freedoms of individuals, and one assessment may address a group of similar processing operations that represent similar high risks.<sup>255</sup></p> <p>Such impact assessments must be conducted in the following cases:<sup>256</sup></p> <ul style="list-style-type: none"> <li>in cases of automated data processing referred to in Clause (1) of Article (22) of the Law, or when automated processing is carried out to conduct a systematic and comprehensive assessment of the personal aspects related to individuals, including identifying the profiling on which decisions that produce legal effects relating to, or significantly affect, the physical person, are based;</li> <li>extensive processing of data or high-risk</li> </ul>	<p>for protection of personal data;</p> <p>training and raising awareness of processors for protection of personal data;</p> <p>setting down internal regulations to receive and examine complaints, applications to access data, applications for rectification or erasure, and making such matter available to individuals;</p> <p>setting down internal regulations for effective management of personal data, and reporting of any violation of protection measures;</p> <p>using appropriate means of technology to enable individuals to exercise their right of direct access, review, and rectification of personal data;</p>	

<sup>250</sup> UAE Federal Decree-Law No. 45/2021, Article 21(3).

<sup>255</sup> Bahrain Ministerial Decision No. 43/2022 Defining the Requirements to be Met in Technical and Organisational Measures to Protect Personal Data, Article 3(a)

<sup>256</sup> Bahrain Ministerial Decision No. 43/2022 Defining the Requirements to be Met in Technical and Organisational Measures to Protect Personal Data, Article 3(c)

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
	<p>Personal Data of the Data Subject; and</p> <p>set out the proposed procedures and measures to minimize the potential risks to Personal Data Protection.</p> <p>Further requirements regarding Data Protection Impact Assessments are set out in Article 21 of the UAE Data Protection Law.</p>	<p>providing a product or service that involves Processing Personal Data that is likely to cause serious harm to the privacy of Data Subjects.</p> <p>The impact assessment must include:-<sup>252</sup></p> <p>purpose of the Processing and its legal basis;</p> <p>description of the nature of the Processing to be conducted, the types and sources of Personal Data to be processed, and any entities to whom the Personal Data is to be Disclosed;</p> <p>description of the scope of the Processing, which identifies the type of Personal Data and the geographical scope of the Processing;</p> <p>description of the context of the Processing, which identifies the relationship between</p>		<p>data, or data related to filing and initiating criminal cases and the judgments issued therein and referred to in Article (7) of the Law;</p> <ul style="list-style-type: none"> <li>• systematic observation of an area widely available to the public; and</li> <li>• data processing by visual recording or automated processing of biometric data.</li> </ul> <p>Data Processing Impact assessments must contain, at a minimum, the following:<sup>257</sup></p> <ul style="list-style-type: none"> <li>• a systematic description of the assessment processes and their purposes, including, where applicable, the legitimate interest pursued by the Data Manager;</li> <li>• assessing the importance and proportionality of processing operations</li> </ul>	<p>conducting comprehensive audit and review operations regarding the extent of compliance with protection of personal data; and</p> <p>verifying the compliance of the processor with instructions given to him, and taking appropriate precautions for protection of personal data, as well as monitoring and following-up such matter on regular basis.</p> <p>According to the DPIA NCGAA Guidelines, controllers should carry out a DPIA before beginning any new activity that involves processing personal data or before making significant changes to an existing activity.</p> <p>DPIAs are particularly important when carrying out a processing activity that “may cause serious damage” to the individuals whose personal data</p>	

<sup>252</sup> KSA Implementing Regulations, Article 25(2)

<sup>257</sup> Bahrain Ministerial Decision No. 43/2022 Defining the Requirements to be Met in Technical and Organisational Measures to Protect Personal Data, Article 3(d)

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
		<p>the Data Subjects, the Controller, and the Processors, as well as any other relevant circumstances;</p> <p>necessity and proportionality of the measures to be taken to enable the Controller and Processors to process the minimal Personal Data necessary to achieve the purposes of the Processing;</p> <p>impact of the Processing, based on the severity of its impact, materially and morally, and the likelihood of any negative impact on Data Subjects, including any psychological, social, physical, or financial impact, and the likelihood of their occurrence;</p> <p>measures that will be taken to prevent or limit the risks; and</p> <p>the suitability of the measures envisaged to avoid identified risks.</p>		<p>in relation to the purposes;</p> <ul style="list-style-type: none"> <li>• assessing the risks to the rights and freedoms of data subjects; and</li> <li>• assessing the measures taken to confront risks, including safeguards, security measures, and mechanisms to protect data in order to comply with the Law and the decisions issued in implementation thereof, taking into account the legitimate rights and interests of data subjects and other relevant persons.</li> </ul>	<p>controllers are processing. This means that although they have not yet assessed the level of risk in detail, controllers need to screen for factors that point to the potential for a widespread or serious impact on individuals.</p> <p>Examples of activities that may trigger a DPIA are<sup>259</sup>:</p> <ul style="list-style-type: none"> <li>• technology implementations or upgrades;</li> <li>• changes to existing processes; and</li> <li>• changes to products or services.</li> </ul> <p>As noted in the “Transfer” column, the NCGAA Guidelines on Data Protection Impact Assessments explain that the Qatar Data Protection Law PDPPL explicitly states two specific ways of processing that may cause serious damage. These are:</p>	

<sup>259</sup> Data Privacy Impact Assessment (DPIA) - Guideline for Regulated Entities, Article 5

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
		<p>A copy of the impact assessment should be provided to any Processor (relevant to the Processing) acting on the Controller's behalf.<sup>253</sup></p> <p>If an assessment shows that the Processing will harm the privacy of the Data Subjects, the Controller should address the reasons for that and re-conduct the assessment.<sup>254</sup></p>			<ul style="list-style-type: none"> <li>transferring personal data outside Qatar, known as a cross-border data transfer; and</li> <li>processing personal data of a special nature, specific categories of personal data also known as sensitive personal data.</li> </ul> <p>This could mean that a DPIA should be done for such processing.</p>	
<b>Breach</b>	<p><u>Notifying the authority</u></p> <p>Controllers must immediately upon becoming aware of any infringement or breach of Personal Data that would prejudice the privacy, confidentiality and security of such data, report such infringement or breach and the results of the investigation to the Office.<sup>260</sup> We expect the</p>	<p><u>Notifying the authority</u></p> <p>The Controller must notify the Competent Authority upon becoming aware of a leak, damage or illegal access of Personal Data.<sup>263</sup></p> <p>This should be done without delay and not exceeding 72 hours of becoming aware of the incident if such incident</p>	<p>Under Article 30 of the Oman Implementing Regulations, the Controller shall report to the Competent Department within a period not exceeding seventy-two (72) hours from the time they learned of the Breach<sup>269</sup> if it would lead to a threat to the rights of Personal Data Subjects. The Article</p>	<p>Under Article 4 of Bahrain Ministerial Decision No. 43/2022 Defining the Requirements to be Met in Technical and Organisational Measures to Protect Personal Data, the Data Manager shall open communication channels that allow direct communication with data subjects or their legal representatives to</p>	<p>The controller and the processor must take necessary precautions to protect personal data against loss, destruction, modification, or disclosure, or accidental or unauthorized access to or use of such data. The processor must inform the controller of any failure to comply with the aforementioned precautions, or in case</p>	<p>The Service Provider shall notify the Authority in the event that Users' Personal Data is disclosed to any company that is an associate or owner of the Service Provider or a third party, directly or indirectly, provided that the Service Provider is responsible for protecting the privacy of</p>

<sup>253</sup> KSA Implementing Regulations, Article 25(3)

<sup>254</sup> KSA Implementing Regulations, Article 25(4)

<sup>260</sup> UAE Federal Decree-Law No. 45/2021, Article 9(1).

<sup>263</sup> Saudi Arabia Cabinet Decision No. 98/1443, Article 20(1)

<sup>269</sup> Personal Data Breach: Unlawful access to Personal Data in a way that leads to unlawful destruction, alteration, disclosure, access or Processing of such Data.

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
	<p>Executive Regulations (which are not yet issued) to provide further detail into the procedures and conditions of this requirement.</p> <p>The report sent to the Office under the notification obligation must include the following details about the infringement or breach:<sup>261</sup></p> <p>the nature, form, causes, approximate number and records;</p> <p>the data of the Data Protection Officer;</p> <p>the potential and expected effects;</p> <p>measures taken and proposed to address</p>	<p>potentially causes harm to the Personal Data or to the Data Subject or conflict with their rights or interests.<sup>264</sup> If notification with 72 hours is not possible, the Controller shall provide it as soon as possible along with justification for the delay.<sup>265</sup></p> <p>The KSA Implementing Regulations in Article 24(1) requires the notification to the Competent Authority to include:<sup>266</sup></p> <p>a description of the Personal Data Breach incident, including the time, date, and circumstances of the breach and the time when the Controller became aware of it;</p>	<p>also sets out what the report should contain.</p> <p>Under Article 32 of the Oman Implementing Regulations, In the event of a Breach of Personal Data, the Controller shall notify the Personal Data Subject within a period not exceeding seventy-two (72) hours from becoming aware of the Breach, if such Breach would cause serious harm or high risks to the Personal Data Subject. The Article also sets out what the notification should contain.</p> <p>The Controller must also document cases of Personal Data Breach, state their causes and the consequences of their occurrence, and the corrective measures or technical</p>	<p>report a penetration or breach.<sup>271</sup></p> <p>The Data Manager shall document cases of data penetration or breach, and to indicate their causes, effects of their occurrence, and corrective measures taken, and he shall establish specific procedures to notify the Authority of a data breach within a period not exceeding seventy-two hours from the time of its discovery, unless it is unlikely that a data breach would jeopardise the rights of data subjects.</p> <p>In the event that the Data Manager fails to notify the Authority within the specified period, the notification shall be accompanied by justifications for the</p>	<p>of any threat, in any way, to the personal data of individuals, immediately upon having knowledge of the same.<sup>276</sup></p> <p>The controller must inform the individual and the competent Department (National Cyber Governance and Assurance Affairs), of any failure to comply with the precautions set forth in the preceding Article, if such matter may inflict serious damage to personal data or to the privacy of an individual.<sup>277</sup></p> <p>The Personal Data Breach Notifications NCGAA Guidelines says the timeline for this is 72 hours of becoming aware of the personal data breach.</p>	<p>the Data in which he is involved.<sup>280</sup></p> <p>If the Personal Data stored by the Service Provider is improperly disclosed and such disclosure or access caused harm to a large number of Users, the Service Provider shall notify the Authority, the Users and law enforcement authorities as soon as possible within no more than 72 hours in any case.<sup>281</sup></p> <p>When a Personal Data breach occurs, and within a period not exceeding 24 hours after becoming aware of it, the Service Provider shall send a notification of a Personal Data Breach to the Communications and Information Technology Regulatory</p>

<sup>261</sup> UAE Federal Decree-Law No. 45/2021, Article 9(1).

<sup>264</sup> KSA Implementing Regulation of the Personal Data Protection Law, Article 24(1)

<sup>265</sup> KSA Implementing Regulation of the Personal Data Protection Law, Article 24(2)

<sup>266</sup> KSA Implementing Regulations, Article 24(1)

<sup>271</sup> Bahrain Ministerial Decision No. 43/2022 Defining the Requirements to be Met in Technical and Organisational Measures to Protect Personal Data, Article 4(a)

<sup>276</sup> Qatar Law No. 13/2016, Article 13

<sup>277</sup> Chapter 3, Article 14

<sup>280</sup> Kuwait Administrative Decision No. 26/2024 Concerning the Issuance of the Data Privacy Protection Regulation, Article 4(5)

<sup>281</sup> Kuwait Administrative Decision No. 26/2024 Concerning the Issuance of the Data Privacy Protection Regulation, Article 4(15).

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
	<p>the breach and reduce its negative effects;</p> <p>documentation and corrective actions; and</p> <p>any other requirements by the Office.</p> <p><u>Notifying Data Subjects</u></p> <p>In all cases, the Controller must also notify the Data Subject if a data breach or infringement would prejudice the privacy, confidentiality, and security of their data, and advise them of the procedures taken.<sup>262</sup> We expect the Executive Regulations (which are not yet issued) to provide further detail into the procedures and conditions of this requirement.</p>	<p>data categories, actual or approximate numbers of impacted Data Subjects, and the type of Personal Data;</p> <p>description of the risks of the Personal Data Breach, including the actual or potential impact on Personal Data and Data Subjects, and the actions and measures taken by the Controller to prevent or limit the impact of those risks and mitigate them, as well as the future measures that will be taken to avoid a recurrence of the breach;</p> <p>a Statement if the Data Subject has been notified of the breach of their Personal Data, as stipulated in Paragraph (5) of this Article; and</p>	<p>and organisational measures that have been taken, and retain them according to the time limit determined by the Competent Department, in record of processing activities.<sup>270</sup></p>	<p>delay. If the Data Manager does not take the initiative to notify the data subjects of the breach, the Authority may impose thereon to do so if it deems that the incident may lead to high risks.<sup>272</sup></p> <p>The Data Manager is not obligated to notify the data subject of the data penetration or breach incident in the following cases:<sup>273</sup></p> <ul style="list-style-type: none"> <li>• if the data that has been penetrated is incomprehensible to any person who is not authorised to access the same, such as if it is encrypted; and</li> <li>• the Data Manager shall take subsequent measures to ensure that high risks to the rights and freedoms of</li> </ul>	<p>Some examples of personal data breaches include<sup>278</sup>:</p> <ul style="list-style-type: none"> <li>• Theft or loss of IT equipment containing personal or business sensitive data.</li> <li>• Inappropriately accessing personal data about customers/staff.</li> <li>• Leaving confidential / sensitive files that may contain personal data unattended.</li> <li>• Inadequate disposal of confidential files that may contain personal data material.</li> <li>• Unauthorised disclosure of client data.</li> </ul>	<p>Authority through official communication channels.<sup>282</sup></p> <p>Article 6(2) of the Kuwait law sets out what the notification shall include.</p> <p>Notifying the Personal Data Subject in the event of breaches of their Personal Data.<sup>283</sup></p> <p>Personal Data Subject notification, however, is not required where the Service Provider has taken appropriate technical and organisational protection measures, and these measures have been applied to the Personal Data affected by the breach.<sup>284</sup></p> <p>Taking subsequent measures to ensure that risks to the rights</p>

<sup>262</sup> UAE Federal Decree-Law No. 45/2021, Article 9(2).

<sup>270</sup> Oman Ministerial Decision No. 34/2024, Article 33

<sup>272</sup> Bahrain Ministerial Decision No. 43/2022 Defining the Requirements to be Met in Technical and Organisational Measures to Protect Personal Data, Article 4(b)

<sup>273</sup> Bahrain Ministerial Decision No. 43/2022 Defining the Requirements to be Met in Technical and Organisational Measures to Protect Personal Data, Article 4(c)

<sup>278</sup> Personal Data Breach Notifications - Guideline for Regulated Entities, Article 3

<sup>282</sup> Kuwait Administrative Decision No. 26/2024 Concerning the Issuance of the Data Privacy Protection Regulation, Article 6.

<sup>283</sup> Kuwait Administrative Decision No. 26/2024 Concerning the Issuance of the Data Privacy Protection Regulation, Article 6(3).

<sup>284</sup> Kuwait Administrative Decision No. 26/2024 Concerning the Issuance of the Data Privacy Protection Regulation, Article 6(4).

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
	<p><u>Notifying Controllers</u></p> <p>Processors must immediately upon becoming aware of any infringement or breach of Personal Data notify the Controller in order for the Controller to report it to the Office.</p>	<p>contact details of the Controller or its data protection officer, if any, or any other official having information regarding the reported incident.</p> <p>The Controller is expected to keep a copy of the reports submitted and document the corrective measures taken, as well as any relevant documents or supporting evidence.<sup>267</sup></p> <p>Controllers should also adhere to any notification obligations issued by the National Cybersecurity Authority or any laws and</p> <p>Regulations applicable in the Kingdom.</p> <p><u>Notifying Data Subjects</u></p> <p>The KSA Data Protection Law also requires Data Subjects to be notified where such breach would</p>		<p>data subjects are not likely to arise.</p> <p>If the notification of the data subject requires extraordinary strenuous efforts, in this case the notification shall be by a public means.<sup>274</sup></p> <p>The regulations also set out in Article 4(e) the information required in notifications to data subjects and to the Authority.</p> <p>For completeness, under the Bahrain Data Protection Law, a Data Protection Controller must notify the Authority of irregularities that it has serious evidence of the occurrence and for which the Data Manager has not removed the causes or made the necessary corrections to them, despite the passage of more than ten days notice.<sup>275</sup></p>	<ul style="list-style-type: none"> <li>Using client data for personal gain.</li> </ul> <p>The NCGAA Guidance also provides further guidance on how to prevent data breaches, such as<sup>279</sup>:</p> <ul style="list-style-type: none"> <li>implementing a robust information security framework;</li> <li>setting up a personal data breach response framework;</li> <li>defining roles and responsibilities for personal data breach response;</li> <li>conducting a DPIA for relevant processing activities;</li> <li>training employees on personal data breach detection and notification;</li> </ul>	<p>and freedoms of Data Subjects do not increase.<sup>285</sup></p>

<sup>267</sup> KSA Implementing Regulation of the Personal Data Protection Law, Article 24(3)

<sup>274</sup> Bahrain Ministerial Decision No. 43/2022 Defining the Requirements to be Met in Technical and Organisational Measures to Protect Personal Data, Article 4(d)

<sup>275</sup> Bahrain Law No. 30/2018, Article 10(D)

<sup>279</sup> Personal Data Breach Notifications - Guideline for Regulated Entities, Article 5

<sup>285</sup> Kuwait Administrative Decision No. 26/2024 Concerning the Issuance of the Data Privacy Protection Regulation, Article 6(5).

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
		<p>cause damage to his data or conflict with his rights or interests.<sup>268</sup></p> <p>Under Article 24(5) of the KSA Implementing Regulations, Controllers must notify the Data Subject of a Personal Data Breach, without undue delay, if it may cause damage to their data or conflict with their rights or interests, provided that the notification is in simple and clear language, and that it includes the following:-</p> <p>description of the Personal Data Breach;</p> <p>description of the potential risks arising from the Personal Data Breach, and the measures taken to prevent or limit those risks and limit their impact; and</p> <p>name and contact details of the Controller and its data protection officer, if any, or any other appropriate means of</p>			<ul style="list-style-type: none"> <li>defining responsibilities of the controller and the processor in the event of a breach in contracts; and</li> <li>conducting breach response exercises and drills regularly to test breach response plans.</li> </ul>	

<sup>268</sup> Saudi Arabia Cabinet Decision No. 98/1443, Article 20(2)

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
		<p>communication with the Controller.</p> <p>Any recommendations or advice that may assist the Data Subject in taking appropriate measures to avoid the identified risks or limit their impact.</p>				
<b>Fines / penalties</b>	<p>Stipulated under the law, but not yet determined.</p> <p>We expect the Executive Regulations, once issued, to set out the penalties and whether there is civil and/or criminal liability for violation of the UAE Data Protection Law or Executive Regulations.</p>	<p><u>Without prejudice to any more severe penalty provided for in another law, disclosure or publishing of Sensitive Data in violation of the law if with intent to harm the data owner or to achieve a personal benefit.</u><sup>286</sup></p> <p>imprisonment for a term not exceeding two years;</p> <p>a fine not more than three million riyals, or by either of these two penalties; and</p>	<p>Without prejudice to any severer penalty stipulated in the Penal Code or any other law:<sup>289</sup></p> <p>Whoever violates the provisions of Article (14) of this Law shall be punished with a fine of no less than five hundred (500) Omani rials and no more than two thousand (2,000) Omani rials.</p> <p>Whoever violates the provisions of Articles (15), (16), (17), (18), (20) and (22) of this Law shall be punished with a fine of no less</p>	<p><u>Compensation</u><sup>290</sup></p> <p>Without prejudice to the provisions of the Civil Code, anyone who has suffered damage arising from the processing of their personal data by the Data Manager or the Data Protection Controller's violation of the provisions of this Law has the right to claim substantial compensation for the damage from the Data Manager or Data Protection Controller as the case may be.</p>	<p><u>Article 23 of the Qatar Data Protection Law</u></p> <p>Without prejudice to any greater penalty specified by any other Law, a person who violates any of the provisions of Articles 4, 8, 9, 10, 11, 12, 14, 15 and 22 of the present Law, shall be sentenced to a fine not exceeding one million (1, 000,000) riyals.</p> <p><u>Article 24</u></p> <p>Without prejudice to any greater penalty specified by any other Law, a person who</p>	<p>In the event of a violation of the provisions of this Regulation or the laws of the State of Kuwait, the Authority may apply the penalties and fines stipulated in Kuwait Law No. 37/2014 on the Establishment of the Communications and Information Technology Regulatory Authority as amended by Kuwait Law No. 98/2015..<sup>294</sup></p> <p>CITRA will have the authority to apply the penalties under the Telecom Law for any violation of the Telecom Law and/or the Data Privacy Protection</p>

<sup>286</sup> Saudi Arabia Cabinet Decision No. 98/1443, Article 35(1)

<sup>289</sup> Oman Sultani Decree No. 6/2022, Articles 24-32

<sup>290</sup> Bahrain Law No. 30/2018, Article 57

<sup>294</sup> Kuwait Administrative Decision No. 26/2024 Concerning the Issuance of the Data Privacy Protection Regulation, Kuwait Law No. 37/2014 On the Establishment of the Telecommunications and Information Technology Regulatory Authority, Chapters 10 to 11; Kuwait Law No. 63/2015 On Combating Cyber Crimes, Chapter 2, Articles 2-21.

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
		<p>court can double the fine in case of recidivism, even if this results in exceeding its maximum limit, if it does not exceed double this limit.<sup>287</sup></p> <p><u>Without prejudice to any more severe penalty provided for in another law, other violations of the law shall be punished by:-</u><sup>288</sup></p> <p>warning;</p> <p>fine not more than five million riyals; and</p> <p>fine may be doubled in case of recidivism even if this results in exceeding its maximum limit, if it does not exceed double this limit.</p>	<p>than one thousand (1,000) Omani rials and no more than five thousand (5,000) Omani rials.</p> <p>Whoever violates the provisions of Article (13) of this Law shall be punished with a fine of no less than five thousand (5,000) Omani rials and no more than ten thousand (10,000) Omani rials.</p> <p>Whoever violates the provisions of Articles (5), (6), (19), and (21) of this Law shall be punished with a fine of no less than fifteen thousand (15,000) Omani rials and no more than twenty thousand (20,000) Omani rials.</p> <p>Whoever violates the provisions of Article (23) of this Law shall be punished with a fine of no less than one hundred thousand (100,000) Omani rials and no more than five</p>	<p><u>Criminal Penalties</u><sup>291</sup></p> <p>Without prejudice to any more severe penalty provided for in any other law:-</p> <p>punishment of imprisonment for a period not exceeding one year and a fine not less than one thousand dinars and not exceeding twenty thousand dinars, or one of these two penalties, shall be imposed on:-</p> <ul style="list-style-type: none"> <li>○ processing sensitive personal data in violation of Article 5 of this Law;</li> <li>○ transfer of personal data outside the Kingdom to a country or territory in violation of the provisions of Articles 12 and 13 of this Law;</li> <li>○ processing personal data without notifying</li> </ul>	<p>violates any of the provisions of Articles 13, 16/Paragraph 3 and 17 of the present Law, shall be sentenced to a fine not exceeding five million (5,000,000) riyals.</p> <p><u>Article 25</u></p> <p>A juristic person that is the offender shall be subject to a fine not exceeding one million (1,000,000) riyals, if any of the crimes set forth in the present Law is committed in its name and for its account, without prejudice to the criminal liability of the subordinate physical person.</p>	<p>Regulations in addition to the penalties set out in the Combating Cyber Crimes Law.</p>

<sup>287</sup> Saudi Arabia Cabinet Decision No. 98/1443, Article 35(4)

<sup>288</sup> Saudi Arabia Cabinet Decision No. 98/1443, Article 36 (1)

<sup>291</sup> Bahrain Law No. 30/2018, Article 58

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
			<p>hundred thousand (500,000) Omani rials.</p> <p>Without prejudice to the criminal liability of natural persons, a legal person shall be punished with a fine of no less than five thousand (5,000) Omani riyals and no more than one hundred thousand (100,000) Omani riyals, if the crime has been committed in its name or for its account by the chairman or a member of its board of directors, its manager, or any other official, with its consent or with cover up or gross negligence on its part.</p> <p>The competent court within the scope of application of the provisions of this Law may, in addition to the fine, order confiscation of the tools used in committing the crime.</p> <p>Without prejudice to the penalties stipulated in this Law, the Ministry may impose administrative penalties for violations committed in violation of the provisions of this Law, the Regulations or the</p>	<p>the Authority in violation of Item 1 of Article 14 of this Law;</p> <ul style="list-style-type: none"> <li>○ failure to notify the Authority of any change in the data submitted to the Authority pursuant to the provisions of Item 1 of Article 14 of this Law, in violation of the provision of Item 6 of the same Article;</li> <li>○ processing personal data without the prior permission of the Authority in contravention of the provisions of Article 15 of this Law;</li> <li>○ providing false or misleading data to the Authority or to the Data Owner, or contrary to the records, data or documents at their disposal;</li> <li>○ withholding from the Authority any data, information, records or documents from</li> </ul>		

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
			<p>decisions issued in implementation thereof, provided that the administrative fine does not exceed two thousand (2,000) Omani rials.</p> <p>Additionally, under the Oman Implementing Regulations, the Minister may impose one of the following administrative penalties in the event of violating the provisions of the Oman Implementing Regulation:</p> <ul style="list-style-type: none"> <li>• Issuing a warning.</li> <li>• Suspension of the Permit until the violation is corrected.</li> <li>• Administrative fine that does not exceed OMR (2000) two thousand per violation.</li> <li>• Revocation of the Permit.</li> </ul>	<p>those to whom it is required to provide the Authority or to enable access to for the performance of its functions under this Law;</p> <ul style="list-style-type: none"> <li>○ causing obstruction to or disrupting the work of the Authority's inspectors or any investigation that the Authority is in the process of conducting;</li> <li>○ disclosing any information or data available to them by virtue of their work or using it for their benefit or for the benefit of others without any right to and in violation of the provisions of this Law;</li> </ul> <p>a penalty of a fine of no less than three thousand dinars and not more than twenty thousand dinars shall be imposed for violation of the provisions of Items 1 or 2 of Article 32 of this Law. In the case of conviction, the court shall order the</p>		

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
				<p>confiscation of the amounts derived from the crime; and</p> <p>a penalty of imprisonment for a period of up to one month and a fine of 100-500 dinars, or one of the two penalties, shall be imposed on any person who unlawfully uses the emblem of the Authority or a similar emblem.</p> <p><u>Liability of legal person</u><sup>292</sup></p> <p>Without prejudice to the criminal liability of a natural person, a legal person shall be punished not exceeding two times the fine prescribed for the offense if it is committed in their name, account or benefit, in any of the crimes stipulated in Article 58 of this Law, or the result of the conduct, omission, consent, concealment or gross negligence of any of the members of the Board of Directors of the legal person or any other authorized</p>		

<sup>292</sup> Bahrain Law No. 30/2018, Article 59

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
				<p>official of that legal person or acting in that capacity.</p> <p><u>Other</u></p> <p>Without prejudice to civil or criminal liability, when the violation is established, Board of Directors shall order the violator to cease the violation and remove its causes or effects immediately or within a period of time determined by the Board. In case of failure to comply with that obligation within the specified period, the Board of Directors may issue a reasoned decision as follows:- <sup>293</sup></p> <ul style="list-style-type: none"> <li>○ withdrawal of the prior authorisation issued by the Authority in accordance with the provisions of Article 15 of this Law, in the case of violation of this authorisation;</li> <li>○ imposition of a penalty fine calculated on a daily basis to</li> </ul>		

<sup>293</sup> Bahrain Law No. 30/2018, Article 55

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
				<p>compel the offender to stop the violation and remove its causes or effects, and that is to not exceed one thousand dinars per day when committing the violation for the first time, and two thousand dinars per day in case of committing another violation within three years from the date of issuing a decision in respect of the previous violation; and</p> <ul style="list-style-type: none"> <li>○ imposition of an administrative fine to not exceed twenty thousand dinars.</li> </ul> <p>In relation to B and C (above), the seriousness of the violation, the disobedience of the offender, the benefits they have earned, and the damage caused to the Data Owner as a result shall be taken into consideration. The collection of the fine shall be by the prescribed means for collection of amounts</p>		

	UAE <sup>153</sup>	KSA	Oman	Bahrain	Qatar	Kuwait
				<p>due to the State, and shall have the same level as the designation of customs taxes due to the Treasury.</p> <p>The Authority may, on the basis of a decision of the Board of Directors, publish a statement on the proven violation by the Data Manager or Data Protection Controller by the means and manner specified by the decision and commensurate with the seriousness of the violation. However, the publication shall not take place until after the date of appeal against the decision of the Authority to prove the violation or the issuance of a final ruling confirming the violation, as the case may be.</p> <p>If the Board of Directors deems that the investigation has resulted in the existence of a criminal offense, it must refer the papers to the Public Prosecution</p>		

