

Unlocking the new UAE Data Protection Law: Cross Border Data Transfers

Introduction

A common issue multinational companies (“MNCs”) have to deal with in the evolving privacy landscape is how and when they can lawfully transfer personal information across borders. MNCs doing business in the UAE now have a new consideration in the form of the new UAE Data Protection Law when doing so.

This alert is intended to provide a high-level overview of the respective data transfer mechanisms under the Federal Law No. 45 of 2021 Regarding the Protection of Data, issued on 20 September 2021 (“**UAE Data Protection Law**”), the European Union’s (“EU”) General Data Protection Regulation (“**GDPR**”), including as retained in the United Kingdom, and the California Consumer Privacy Act of 2020 (“**CCPA**”), so MNCs in the UAE can consider how they may need to change the way in which they transfer data from the UAE into the EU and California.¹

We are also following the ongoing development of a new data protection law in the Kingdom of Saudi Arabia and will be releasing a follow-up alert on how that law is taking shape.²

Impact of the UAE Data Protection Law

The UAE Data Protection Law adds a new level of considerations for MNCs operating in the UAE³. Some questions that the law raises includes::

- can employers in the UAE store personal information on their UAE employees on databases hosted in foreign jurisdictions?
- can U.S.-based MNCs collect personal information of UAE users to be analyzed on their servers located in either the EU or California?

¹ There are separate data protection laws issued by the different States in the USA. This piece considers California as a prominent jurisdiction in the United States. If you need to consider other U.S. states, we can provide such analysis

² Personal Data Protection Law, promulgated by Royal Decree No. M/19, dated 09/02/1443H (corresponding to 16 September 2021).

³ Please note there is already separate legislation in the UAE covering the transfer of healthcare data, and the transfer of personal data from certain specific financial free zones in the UAE, namely the ADGM in Abu Dhabi and the DIFC in Dubai. That separate legislation in the UAE is not considered herein.

- can companies compliant with the GDPR or the CCPA transfer personal information beyond the borders of the UAE without taking additional action?

Although the UAE Data Protection Law came into effect on 02 January 2022, the executive regulations (“**UAE Data Protection Law Regulations**”) designed to provide additional detail on the UAE Data Protection Law’s provisions, along with certain specific compliance requirements are still yet to be issued. Upon issuance of the UAE Data Protection Law Regulations, companies will then have only six (6) months to comply with the UAE Data Protection Law and the UAE Data Protection Law Regulations.

Further, the UAE Data Protection Law refers to the establishment of the UAE Data Office (“**Data Office**”) pursuant to Federal Law No. 44 of 2021, which will have responsibility for overseeing and enforcing the UAE Data Protection Law. There have been no announced developments about the UAE Data Office contemplated in the UAE Data Protection Law.

We will provide further updates as and when the timing of the UAE Data Protection Law Regulations and the establishment of the Data Office become clear.

Data Transfer Considerations: UK, EU and UAE

The UAE Data Protection Law is aligned to GDPR in several key aspects when it comes to cross-border data transfers, but significant differences exist in the details. Both laws require a specific mechanism for organizations to transfer personal information to a third country or an international organization, with the UAE Data Protection Law, so far, providing fewer restrictions on the use of data transfer mechanisms.

UAE and GDPR Comparison: Cross-Border Data Transfer Mechanisms

Ultimately both the UAE Data Protection Law and GDPR/UK GDPR apply the same principle that personal data may only be transferred to a third country⁴ if the transfer is based on a lawful transfer mechanism under which the data transfer is performed.

⁴ A third country is a country other than the EU member states and the three additional EEA countries (Norway, Iceland, and Liechtenstein) that have adopted a national law implementing the General Data Protection Regulation (GDPR).

Set out below is a summary comparison of the provisions under Articles 22 and 23 of the UAE Data Protection Law alongside those in Chapter V of the GDPR, which set out the lawful transfer mechanisms and how they can be applied:

UAE Data Protection Law	GDPR
International agreements and adequacy decisions	
<p>The UAE Data Protection Law authorizes the transfer of personal data to countries approved by the Data Office as having an “adequate level of protection”.</p> <p>More specifically, this would include countries that either have “special legislation” in place for the protection of personal data or where the specific country has acceded to bilateral or multilateral agreements relating to the protection of personal data.</p> <p>Any countries falling within this group have not been identified in the UAE Data Protection Law. The UAE Data Protection Law Regulations will likely include details of these approved countries.</p>	<p>Where the European Commission has decided that a third country or an international organization ensures an adequate level of data protection to data subjects in the EU, it issues an “adequacy decision.” This means that personal data can be transferred to these countries without further security measures.</p>
Standard Model Clauses	
<p>For those countries not listed by the Data Office as having an adequate level of protection, the UAE Data Protection Law provides for the transfer of personal data under a standard contract.</p>	<p>The European Commission provides approved model data protection clauses, namely standard contractual clauses (“SCCs”), which enable the free flow of personal data to third</p>

UAE Data Protection Law	GDPR
<p>Although the details of the requisite standard contract remain unclear, we assume that the UAE Data Protection Law and its Regulations will provide for or recognize standard contract clauses similar to those used under other global data protection laws, such as the GDPR.</p>	<p>countries that lack an adequacy decision.</p> <p>The SCCs set out contractual obligations on both the exporter and importer of the personal data, as part of any cross border transfer.</p>
<p>Binding Corporate Rules (“BCRs”)</p>	
<p>We await the position on BCRs—or a similar framework— under the UAE Data Protection Law Regulations.</p>	<p>BCRs can be used to form an internal code of conduct applicable to the transfer of personal data within a multinational group, from the group’s EU entities to the group’s non-EU entities.</p> <p>These BCRs are made legally binding and are subject to approval by competent data protection authorities.</p>
<p>Other transfer mechanisms</p>	
<p>The UAE Data Protection Law also allows for the transfer of personal data offshore in circumstances where: (1) the data subject’s express consent to such transfer has been obtained (provided such consent does not conflict with public and security interests of the UAE); (2) if the transfer is necessary for the execution of a contract between the controller and the data subject (or as part of a contract between the controller and a third party that achieves the interests of a data</p>	<p>Enshrined in GDPR Article 49, these mechanisms (also known as derogations) are valid in certain specific situations, such as where consent is obtained, for the performance or conclusion of a contract with the data subject, for the exercise of legal claims, to protect the vital interests of a data subject who cannot give consent, or for important reasons of public interest.</p>

UAE Data Protection Law	GDPR
<p>subject); (3) if the transfer is necessary for international judicial cooperation; or (4) if the transfer is necessary to protect the public interest.</p> <p>More details are expected on the scope of and any conditions around these transfer mechanisms in the UAE Data Protection Law Regulations.</p>	

Data Transfer Considerations: California and UAE

The CCPA, as a state law, does not specifically regulate the transfer of personal information across international borders. The CCPA does, however, require that companies who hold personal data meet some of the same contractual obligations as required under the GDPR and which have been alluded to in the UAE Data Protection Law. These include, for example, contractual addendums that: (i) specify the limited purpose for the sharing or disclosure of personal information; and (ii) obligate the third-party recipients to undertake the same level of privacy protection as required under the CCPA.

In practice, MNCs subject to both the CCPA and the UAE Data Protection Law may want to consider using existing CCPA addendums or the GDPR data processing addendums as a starting point to prepare for meeting the forthcoming contractual requirements for cross-border data transfers under the UAE Data Protection Law.

Closing

As discussed above, although the UAE Data Protection Law has established a general framework governing the cross-border transfer of personal information, until the release of its implementing regulations, it is unclear quite how strict this framework will be. Key questions will be whether the UAE Data Protection Law will follow the European approach of primarily requiring the use of model clauses for cross-border data transfers and if so, what these model clauses will look like.

Baker Botts is currently advising clients on strategies to develop compliant data transfer mechanisms in preparation for the release of the UAE Data Protection Law's Regulations and the 6-month compliance countdown. Please also note that in addition to the transfer mechanisms requirement, both the UAE Data Protection Law and the GDPR impose other compliance obligations on organizations transferring personal data overseas.

Baker Botts L.L.P.