KARM
LEGAL CONSULTANTS

NEWSLETTER

TECH-TONIC

APRIL 2023

Navigating multi-jurisdictional personal data protection regimes by VASPs and FinTechs

INTRODUCTION

With businesses increasingly driven by personal data, jurisdictions globally have enacted legislations and regulations to safeguard the interests of data subjects' resident in their respective jurisdictions. This puts the data subjects' rights at the forefront of all business considerations, along with the institution of internal policies to manage personal data. Regional and global businesses must now navigate complex compliance obligations imposed by the various data protection frameworks existing the UAE.

Interestingly, businesses such as Virtual Assets (**"VA"**) Service Providers (**"VASP"**) and financial technology companies ("**FinTech"**), based in the UAE, ADGM or DIFC, have clients and operations spread across the globe, resulting in personal data collection and processing across jurisdictions. In this case, they must comply with the applicable data protection regimes of multiple jurisdictions. Particularly relevant for such businesses spread across geographical and jurisdictional boundaries, are regulations on cross border transfer of data and mechanisms for exercise of data subjects' rights.

This newsletter is aimed at VASPs and FinTechs with operations in more than one jurisdiction in the UAE. For example, an FSRA licensed virtual asset exchange with personal data processing capabilities in the UAE mainland. The newsletter intends to deliver a framework to better identify similarities and differences in personal data protection regimes in these jurisdictions so that they can streamline compliance processes and reduce duplication of effort.

This newsletter does not intend to provide legal advice, but just contours of such similarities and differences.

Data Protection Frameworks in the UAE

There are three primary data protection regimes in force in the UAE. In the UAE mainland, it is the Federal Decree Law No. 45 of 2021 which is the main Personal Data Protection Law ("PDPL") for the country. The Executive Regulations for the PDPL, which will give teeth to the law, are yet to be framed. For the two financial freezones, i.e., Abu Dhabi Global Markets ("ADGM") and Dubai International Financial Centre ("DIFC"), the ADGM Data Protection Regulations 2021 and the Data Protection Law 2020- DIFC Law No. 5 of 2020 (as amended by DIFC Law No. 2 of 2022) respectively hold the field. DIFC'S Data Protection Law is supplemented by the DIFC Data Protection Regulations 2020.

Uniformity of purpose across the three frameworks

Most reassuringly, all the three data protection regimes, recognize the centrality of personal data to the digital economy and strike a balance between protecting the privacy of the individual on one hand, while enabling businesses to innovate and grow on the other hand. Specifically, the provisions relating to cross border transfers of data appear to be facilitative, rather than restrictive. Similarly, while special categories of personal data and sensitive personal data are recognized, their processing is permitted under certain conditions, including among others, if express consent is obtained from the data subject or if such processing is required for employment related purposes. Businesses, in their role as data controllers and data processors must adapt their operations to the requirements of these regimes, in order to be able to leverage the personal data collected by them, while ensuring the privacy of data subjects (individuals) who have shared that data.

Broadly speaking, all three data protection regimes, i.e., require that companies which collect and process personal data must first seek and obtain consent from the individual, except in certain limited circumstances, such as, when the processing is in public interest or is for judicial or security reasons. VASPs and FinTechs may benefit from making these exceptions clear in their client onboarding/ account opening forms, as well as in their privacy policies.

Companies will also be required to take measures to secure the personal data under their control as well as maintain a record of the personal data processed. In addition, they will also need to report breaches of personal data to the appropriate authority – the UAE Data Office in case of the PDPL and the respective Commissioners in the ADGM and DIFC.

There are some elements of divergence in this general uniformity. Provided below is a comparative view of selected aspects of the three frameworks.

Concepts of Personal Data and Sensitive Personal Data

The concept of Personal Data is important because it defines and circumscribes the data in respect of which businesses need to comply with the data protection framework(s). The concept of Sensitive Personal Data (or special categories of personal data) is relevant because the processing of high volumes of such data will usually constitute high risk processing under all three data protection frameworks. Processing of Sensitive Personal Data and high-risk processing will trigger compliance requirements, including, but not limited to, designation of a Data Protection Officer.

To ensure compliance with the applicable data protection regimes, companies and businesses will have to internally assess the types of personal data they collect, and how much of it is really required for their business purposes. This will serve to streamline compliance obligations. In addition, they will need to draft privacy policies which provide details of their data collection and management practices.

The Table below indicates how the three data protection frameworks view the concepts of Personal Data and Sensitive Personal Data.

Concepts of Personal Data and Sensitive Personal Data / Special Categories of Personal Data

	UAE	ADGM	DIFC
Personal Data	Any data relating to an identified natural person, or a natural person who can be identified, directly or indirectly, through the linking of data, by reference to an identifier such as his name, voice, picture, identification number electronic identifier, geographical location, or one or more physical, physiological, cultural or social characteristics. Personal data includes Sensitive Personal Data and Biometric Data.	Any data relating to an identified or identifiable living natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic,	Any information referring to an identified or Identifiable Natural Person. An identifiable natural person means a natural living person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to his biological, physical, biometric, physiological, mental, genetic, economic, cultural or social identity (and "Identified Natural Person" is interpreted accordingly).

Sensitive Personal Data / Special Categories of Personal Data	Any information that directly or indirectly reveals a person's race, ethnicity, political or philosophical views, religious beliefs, criminal record, biometric data or any data related to such person's health such as his physical, psychological, mental, corporal, genetic or sexual state, including any information related to such person's provision with healthcare services that reveal his health condition.	Special Categories of Personal Data consist of (a) Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; (b) Genetic Data, Biometric Data for the purpose of uniquely identifying a natural person, Data Concerning Health or data concerning a natural person's sex life or sexual orientation; and (c) Personal Data relating to criminal convictions and offences or related security Measures.	Special Categories of Personal Data refers to Personal Data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life and including genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person.

VASPs and FinTechs collecting Personal Data may benefit from listing the collected data points and mapping them against the definitions reproduced above. Special obligations apply to Sensitive Personal Data. Further, if an entity wishes to process Sensitive Personal Data in large volumes or using novel technology, an assessment of which framework is most suited will prove useful.

Rights of Data Subjects:

The table below lists the rights granted to data subjects under the respective frameworks. The reader may note that while the categories of rights are similar, the specifics are not necessarily the same. These rights assume significance because businesses will need to operationalise mechanisms to enable data subjects to exercise these rights. In the digital age, rights conscious data subjects can be expected to be increasingly assertive about the exercise of their rights.

UAE	ADGM	DIFC
• Right of access to information • Right to request personal data portability • Right to rectification or erasure of personal data • Right to restriction of processing • Right to stop processing • Right to object to automated decision making	• Right to be informed • Right of access: • Right to rectification: • Right to erasure: • Right to object/opt-out: • Right to data portability: • Right to restriction of processing • Right not to be subject to a decision based solely on automated processing, including profiling	• Right to be informed • Right to access • Right to rectification • Right to erasure • Right to object/opt-out • Right to withdraw consent • Right to data portability • Right to restriction of processing • Right to object to any decision based solely on automated processing, including profiling • Right not to be discriminated against

As is evident above, there are differences in the scope of rights and their respective definitions across these jurisdictions. Companies must enable mechanisms to ensure that the data subjects can exercise the rights granted to them under the law without any friction. Companies with operations in two or more of the jurisdictions explored must assess which regime would govern rights for their users. Further, they must institute clear guidelines to distinguish users governed by one regime as opposed to another. Additionally, entities may examine whether a centralised platform enabling the exercise of rights under different regimes is possible, where required.

Cross Border Transfer of Personal Data

All three data protection regimes permit the cross-border transfer of personal data as long as there is an adequate level of protection in the receiving jurisdiction. However, as the Table below will indicate, they also make provisions for the transfer of personal data in the absence of such an adequacy determination. This is good news for businesses in a globalized, digital economy, wherein data protection regimes provide multiple mechanisms to enable cross border transfer of data. It is also one more reason why the UAE and its financial freezones are an attractive jurisdiction for existing as well as emerging businesses in the Virtual Assets, Artificial Intelligence and other emerging technologies space. Significantly, the mainland UAE has not been recognized as a jurisdiction offering adequate protection by the DIFC or the ADGM. It is expected that when the Executive Regulations are framed, this would change.

The Provisions relating to cross border transfers in each of the three jurisdictions are laid out in the table below:

UAE	ADGM	DIFC
Transfer of personal data to countries or territories outside the UAE is permitted as long as those countries provide an "adequate level of protection" for data subjects' rights and freedoms in connection to personal data processing. Additionally, the following conditions are provided for transfer of data to those jurisdictions which have not been determined to provide an "adequate level of protection":	Transfer of personal data is permitted to jurisdictions outside the ADGM, in respect of which an adequacy determination has been made by the Commissioner of Data Protection. In the absence of an adequacy determination, transfer of personal data outside the ADGM is still possible subject to appropriate safeguards. The appropriate safeguards which may be provided for without specific authorisation from the Commissioner are:	Transfer of personal data is permitted to jurisdictions outside the DIFC, in respect of which an adequacy determination has been made by the Commissioner. In the absence of an adequacy determination, transfer of personal data outside the ADGM is still possible subject to appropriate safeguards. The appropriate safeguards are:

a) In case of states outside the UAE where no data protection law exists, then establishments operating in the UAE and such states may transfer data under a contract binding such establishments to the measures and standards provided for under the UAE's PDPL. b) Express consent of the data subject for processing of his personal data outside the UAE in a manner that does not conflict with the security and public interest of the State. c) If the transfer is necessary to fulfil obligations and establish, exercise or defend rights before judicial authorities. d) If the transfer is necessary to perform a procedure relating to international judicial cooperation. e) 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 for the Data Subject's interest. If the transfer is necessary for the protection of public interest.	a) A legally binding and enforceable instrument between public authorities; b) Binding Corporate Rules c) Standard data protection clauses adopted by the Commissioner of Data Protection d) An approved code of conduct together with enforceable commitments of the recipient in the jurisdiction outside of ADGM to apply the appropriate safeguards, including as regards Data Subjects' rights; or e) An approved certification mechanism together with binding and enforceable commitments of the recipient in the jurisdiction outside of ADGM to apply the appropriate safeguards, including as regards Data Subjects' rights. Separately, it is also possible to transfer personal data to jurisdictions outside the ADGM which do not have an adequacy determination, subject to certain other appropriate safeguards, provided that these safeguards are authorised by the Commissioner. These safeguards are:	Transfer of personal data is permitted to jurisdictions outside the DIFC, in respect of which an adequacy determination has been made by the Commissioner. In the absence of an adequacy determination, transfer of personal data outside the ADGM is still possible subject to appropriate safeguards. The appropriate safeguards are: a) a legally binding and enforceable instrument between public authorities; b) Binding Corporate Rules c) Standard data protection clauses adopted by the Commissioner of Data Protection d) An approved code of conduct together with enforceable commitments of the recipient outside of DIFC to apply the appropriate safeguards, including as regards Data Subjects' rights; or e) An approved certification mechanism together with binding and enforceable commitments of the recipient outside of DIFC to apply the appropriate safeguards, including as regards Data Subjects' rights.

f) If the transfer is necessary for the protection of public interest.	a) Contractual clauses between the Controller or Processor and the Controller, Processor or the Recipient of the Personal Data outside of ADGM or the international organisation; or b) provisions to be inserted into administrative arrangements, including regulatory memorandums of understanding between public authorities or domestic or international bodies which include enforceable and effective data subject rights. Further, in the absence of an adequacy determination as well as absence of appropriate safeguards including Binding Corporate Rules, a transfer or a set of transfers of Personal Data outside of ADGM or to an International Organisation, must take place only on one of the following conditions: a) Explicit and informed consent of the data subject; or b) The transfer is necessary for one or more of the following: i. The performance of a contract between the Data Subject and the Controller or the implementation of pre-contractual measures taken at the Data Subject's request	Further, in the absence of an adequacy determination as well as absence of appropriate safeguards, a transfer Personal Data outside of DIFC can take place on one of the following conditions: a) Explicit and informed consent of the data subject; or b) the transfer is necessary for one or more of the following: i. The performance of a contract between the Data Subject and the Controller or the implementation of pre-contractual measures taken at the Data Subject's request; ii. Conclusion or performance of a contract that is in the interest of a Data Subject between a Controller and a Third Party; iii. For reasons of Substantial Public Interest; iv. In the interests of the DIFC v. The establishment, exercise of defence of a legal claim;

	ii. The conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller and another natural or legal person; iii. Requirements of law enforcement agencies of the UAE in accordance with Applicable Law iii. Requirements of law enforcement agencies of the UAE in accordance with Applicable Law iv. Establishment, exercise or defence of legal claims v. Protecting the vital interests of the Data Subject or of another person, where the Data Subject is physically or legally incapable of giving Consent.	vi. Protecting the vital interests of the Data Subject or of another person, where the Data Subject is physically or legally incapable of giving Consent; vii. The transfer is made in compliance with Applicable Law and data minimisation principles from a register intended to provide information to the public and is open for viewing; viii. For compliance with any obligation under Applicable law to which the Controller is subject ix. Made at the reasonable request of a regulator, police or other government agency or competent authority; x. To uphold the legitimate interests of a Controller recognized in international financial markets, except where such interests are overridden by the legitimate interests of the Data Subject relating to the Data Subjects's particular situation;

		xi. For complying with applicable anti money laundering or counter-terrorist financing obligations that apply to a Controller or Processor or for the prevention or detection of a crime. In addition to these, grounds, a transfer outside the DIFC may be made if all of the following conditions are fulfilled and the Controller informs the Commissioner of transfers made pursuant to these conditions and also informs the Data Subject of the transfer and the compelling legitimate interests. The conditions are: a) The transfer is not repeating or part of a repetitive course of transfers; b) Concerns only a limited number of Data Subjects; c) Is necessary for the purposes of compelling legitimate interests pursued by the Controller that are not overridden by the interests or rights of the Data Subject; and d) The Controller has completed a documentary assessment of all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of Personal Data.

It emerges from the above table that provisions have been made for cross border transfer of data in three circumstances, firstly, where the recipient's jurisdiction is deemed to provide an adequate level of jurisdiction. Secondly, where the recipient's jurisdiction does not benefit from an adequacy decision, but appropriate safeguards are put in place. Finally, in a situation where the recipient's jurisdiction does not benefit from an adequacy decision, and in the absence of adequate safeguards, transfer is still possible if certain conditions are met. These conditions include, among others, express and informed consent of the Data Subject. Accordingly, the intent of the frameworks to facilitate data transfers, subject to strict conditions, is evident.

CONCLUSION

Personal Data Protection frameworks are one important factor that data driven businesses consider, while assessing jurisdictions in which to set up business or expand operations. The three personal data protection frameworks in the UAE are detailed and elaborate in their provisions, which will help VASPs and FinTechs comply with obligations that may seem onerous at first glance. Accordingly, businesses should seek suitable internal and external advice to ensure they stay compliant with data protection regulations. This is particularly true at a time when businesses operate at the intersection of multiple regulated fields, such as Virtual Assets, finance and health, all of which have their respective data protection guidance.

Developments to watch out for

- While the ADGM and DIFC data protection regimes are effectively operationalised, the Executive Regulations which will operationalise the PDPL are still to be notified. This is expected to happen in the very near future.
- The DIFC has recently issued a consultation, seeking inputs on proposed amendment to the Data Protection Regulations 2020. The regulations proposed to be amended mainly concern data breach, inadvertent disclosure of information as well as use of personal data for business communication purposes.
- Looking outside the UAE, Saudi Arabia's Personal Data Protection law is expected to come into effect in September 2023, with a compliance deadline of September 2024.

KARM

LEGAL CONSULTANTS

THANK YOU FOR READING!

OUR SERVICES

VISIT WEBSITE

FOLLOW US

Reach us @ +971 56 411 0349
communications@karmadv.com