DATA IMPORT RISK RATING ASSESSMENT FOR DP LAW COMPLIANCE

United Arab Emirates 2022

Commissioner of Data Protection

CONTENTS

United Arab Emirates 3

1. Thematic Risk Rating Assessment 3

2. Itemized Assessment Criteria and Rating 6

United Arab Emirates

1. Thematic Risk Rating Assessment

KEY

Low	No concerns about importing entity complying with existing laws, including DP laws, and assuring data subjects' rights.	**Medium / High**	Increased concerns about importing entity complying with existing laws, including DP laws, and assuring data subjects' rights, and unlikely to be mitigated unless enhanced due diligence is undertaken.
Low / Medium	Almost no concerns about importing entity complying with existing laws, including DP laws, and assuring data subjects' rights.	**High**	Significant degree of concerns about importing entity complying with existing laws, including DP laws, and assuring data subjects' rights, and unlikely to be mitigated.
Medium	Concerns about importing entity complying with existing laws, including DP laws, and assuring data subjects' rights, but likely to be mitigated if enhanced due diligence is undertaken.		

Thematic Group		**Thematic Risk Rating**	**Thematic Rationale**
Laws and Regulations Rating		Medium	The combination of overall regulations and laws that reflect data protection and security principles creates a more positive impact and likelihood of implementation of privacy principles.
Regulators, Supervision and Enforcement Rating		Medium	The increased presence of regulatory authorities that directly or indirectly supervise and enforce privacy and security laws in a jurisdiction, as well as provision of clear, easily accessible guidance, results in a decreased likelihood that privacy principles and rights of data subjects will be breached. The impact of any such breach will be lower as a result the above-named factors in addition to robust, measurable enforcement measures.

Thematic Group		Thematic Risk Rating	Thematic Rationale
Privacy Culture and Environmental Factors		Low / Medium	Data Importers in the jurisdiction generally apply and respect privacy principles, tend to comply with data protection and security laws, and understand the supervisory authorities' interpretation and application of the relevant laws in the jurisdiction. In doing so, the likelihood and impact of good culture of privacy increases, fostering an ethical, suitable environment for fair and lawful processing to occur.
Accountability and Transparency Rating		Low / Medium	Data Importers must maintain and implement appropriate controls to safeguard and provide access to Personal Data, as well as provide clear notices and information to data subjects. With such measures in place, the likelihood and impact of an Importer's interests overriding individuals' interests is reduced.
Individual Rights and Redress Rating		Medium	Individuals have lawful, accessible options for controlling their own personal data, and redress for breaches of their rights. Importers ensure these principles are implemented, and the local judicial system permits for redress. Doing so mitigates the likelihood and impact of a breach of privacy principles.
Public Authority Access to Personal Data and Remedies Factors		Medium	Necessary and proportionate access to Personal Data by law enforcement or public authorities, as well as reasonably valid and proportionate investigatory powers reduce the likelihood and impact of infringement of the individual right to privacy and private life.
Transparency International Corruption Rating		UAE TI Risk Rating Low / Medium	Independent analysis of business conditions for ethical and compliant conduct of business. This factor is considered in light of general business attitude and risk factors that may influence understanding and implementation of privacy laws and regulations.

Thematic Group		Thematic Risk Rating	Thematic Rationale
Overall Risk Assessment This rating is not DIFC's assessment of the country or any political / economic analysis or judgment. It is an assessment of the risk of a Data Importer lawfully or unlawfully processing Personal Data in this jurisdiction.		**Medium**	**Recommendations** **EDMRI+ :** Completing EDMRI+ is not necessary in order to understand potential risks of the importing entity breaching relevant data protection laws. Best practice suggests reviewing both your own and the importing entity's technical, contractual, and organisation measures for controlling access to and processing of Personal Data in any case, and to mitigate as needed. **Adequacy:** DIFC Commissioner's Office has not yet recognised the UAE as an adequate jurisdiction.

2. Itemized Assessment Criteria and Rating

Assessment Criteria	Risk Weighting Rationale	Assessment
DP Law in the jurisdiction	Existence of a DP Law is a positive factor in ensuring lower risk when processing Personal Data in a jurisdiction, but it does not guarantee either effectiveness or enforcement. It also is not determinative that businesses will implement the law when processing Personal Data due to a variety of factors, including awareness.	*Keystone piece of onshore UAE legislation is the Federal Decree Law No. 45 of 2021 on the Protection of Personal Data (the "**UAE DP Law**"). The effective date of the UAE DP Law is 2 January 2022 however the law will not be enforced until 6 months after publication of the executive regulations. The timing of publication of the executive regulations is not currently known. There are also potential criminal penalties for processing personal data in breach of UAE laws contained in Federal Decree Law No. 34/2021 Cybercrime Law and the UAE Penal Code.*
Cyber security laws / policies?	Laws or policies regulating cyber security and advance IT risks, when implemented and enforced, reduces risk to Personal Data processing in the importing organisation.	*Article 5 of the UAE DP Law requires controllers to take appropriate technical and organizational measures to ensure the protection of personal data. The UAE DP Law does not contain any detailed cyber controls, however.* *The UAE's Telecommunications and Digital Government Regulatory Authority ("**TDGRA**") has developed the country's national cybersecurity strategy and publishes cybersecurity-related guidance focused on the telecommunications and government sectors.*

Assessment Criteria	Risk Weighting Rationale	Assessment
Non-privacy laws with DP Elements (HR, Consumer protection, Health data)	Laws other than a national privacy law may exist in a jurisdiction that provide as much if not more protection of Personal Data imported to it. Laws regulating processing of medical insurance information, criminal records, children's' privacy online, and consumer privacy may be considered as lower risk despite the lack of a national privacy law.	*UAE has a number of sectoral data security laws and regulations that impose specific data requirements on entities in the financial, telecommunications, IoT and health sectors.*
E-Privacy / direct marketing and digital footprint / tracking laws?	Laws or policies regulating marketing and tracking IT, when implemented and enforced, reduces risk to Personal Data processing in the importing organisation.	*Article 4(5) of Federal Law No. 15/2020 On Consumer Protection establishes the right for customers to not have their personal data used for promotional or marketing purposes. The UAE DP Law also affords data subjects the right to object to the processing of their personal data when used for direct marketing. There are no specific cookie regulations.*
Adequacy recognition from another jurisdiction	If another authoritative regulator has assessed the jurisdiction, it's likely, although not determinative, that processing operations by organisations in the importing jurisdiction will be properly undertaken. The risk is likely to be lower in such jurisdictions.	*DIFC Commissioner's Office has not currently recognised the UAE as an adequate jurisdiction.* *The UAE is also not deemed adequate yet by either the European Commission or the United Kingdom.*
Right to privacy principles in other laws	Where the right to privacy exists in a foundational legal tenant or instrument, such as constitution or founding laws, the importing jurisdiction is more likely to process data in an ethical way and the risk may be less.	*Article 31 of the UAE Constitution guarantees the secrecy of post, telegraph, and other means of communication in accordance with law. There are also criminal penalties for breaches of data protection law contained in the UAE Penal Code and Cybercrime Law and potentially under the Consumer Protection Law.*

Assessment Criteria	Risk Weighting Rationale	Assessment
Extra-territorial reach of any DP related laws?	Where privacy or similar laws of the exporting jurisdiction have sufficient, legally enforceable reach to protect Personal Data to the extent it is implemented by the importing entity, the risk of privacy lapses is reduced.	*The UAE DP Law applies to any entity located outside of UAE who is processing the personal data of individuals residing in the UAE. No particular quantitative threshold or qualitative tests are set out which means that any organisation theoretically becomes subject to the law as soon as any UAE resident interacts with them, even if their involvement with the UAE market is passive or incidental. This is a broader territorial scope than the GDPR which only applies to non-EU established entities who are engaged in targeting, offering goods or services to or monitoring EU individuals.*
Independent regulator managing any privacy related aspects, enforcement	Oversight by a regulator with the power to independently enforce the law significantly reduces the risk of privacy breaches.	*Federal Decree Law No. 44 of 2021 Establishing the UAE Data Office establishes the UAE Data Office. The UAE Data Office will be the regulator charged with overseeing, implementing and enforcing the UAE DP Law. It is presumed that that TDGRA will support the UAE Data Office initially.*
Independent regulator managing any security related aspects, enforcement	Oversight by a regulator with the power to independently enforce the law significantly reduces the risk of cybersecurity incidents.	*UAE Data Office.*
Notification or registration (or licensing) requirements for entities?	Notification to an independent regulator with the power to inspect / investigate for compliance with the law significantly reduces the risk of privacy breaches.	*The UAE DP Law introduces reporting requirements for personal data breaches and the requirement to notify the UAE Data Office of the contact address of a Data Protection Officer ("**DPO**") where one is required to be appointed. There is no general requirement for controllers or processors to register or obtain a licence under the UAE DP Law.*
Access to guidance / information?	Guidance and outreach provided by an independent regulator to help raise awareness and ensure compliance with the law significantly reduces the risk of privacy breaches.	*This is in the mandate of the UAE Data Office, although none has been published yet.*

Assessment Criteria	Risk Weighting Rationale	**Assessment**
Requirement to report data breaches to regulator?	Transparency with the regulator in a jurisdiction and an understanding of what causes data breaches is necessary for reducing risk.	*Controllers must immediately report data breaches to the UAE Data Office unless the breach would not prejudice the privacy, confidentiality and security of the data. In such circumstances, the controller must also contact the affected data subjects.*
Requirement to report data breaches to individual / data subjects?	Transparency with and accountability to individuals in a jurisdiction and an understanding of what causes data breaches is necessary for reducing risk.	*See explanation above.*
Cultural respect for privacy?	If the jurisdiction has a basic, ethical foundation of privacy and respect for human right to privacy, to the extent it can be ascertained, the risk is reduced.	*UAE has a culture of individual privacy with respect to interactions between people and businesses and Article 31 of the UAE Constitution guarantees the secrecy of post, telegraph and other means of communication in accordance with law.*
Accountability requirements? DPO, privacy policy, etc	Appointing a DPO and requiring privacy policies, compliance programs, etc., creates awareness within the processing organisation and ensures a better, more consistent overall application of the law. Thereby, a culture of privacy is more likely to exist, and risk is reduced.	*The UAE DP Law contains similar accountability requirements as the GDPR i.e., requirement to appoint DPO for certain types of processing, obligation to inform data subjects of processing.*

Assessment Criteria	Risk Weighting Rationale	Assessment
Industry specific codes of conduct or certification scheme?	Where a secondary, non-privacy regulator also requires accountability through a code of conduct requirement, or certification scheme is implemented by a privacy regulator, risk is reduced.	*It is not clear to what extent the UAE Data Office will publish guidance and codes of conduct, although such activities are within its mandate. For example, the TDGRA publishes guidance on cybersecurity with a focus on the telecommunications sector.*
Enhanced limitations on processing special category data?	Particularly sensitive data that may create or exasperate the vulnerability of an individual likewise creates risk for that individual when his or her data is processed without knowledge or express permission, where required. Enhanced limitations and controls existing in the local privacy or other similar laws supports a reduced risk assessment.	*Additional rules apply to sensitive personal data under the UAE DP Law.*
Prohibitions on specific types of data processing?	See above	*The UAE DP Law singles-out sensitive personal data as warranting a higher standard of protection than standard personal data, but the UAE DP Law does not prohibit processing these types of personal data. Where large amounts of sensitive personal data will be processed, the UAE DP Law requires a (a) DPO be appointed and (b) a data processing assessment be conducted.*
Judicial system / redress available for privacy violations	Where access to judicial redress is available in the importing jurisdiction, it is more likely that individual rights will be protected where Personal Data has been processed unlawfully.	*Complaints can be filed with the UAE Data Office by any data subject. The UAE DP Law does not specify whether data subjects can bring a claim before a competent court for compensation for material or non-material damage.*

Assessment Criteria	Risk Weighting Rationale	Assessment
Individual privacy rights (access, erasure, etc)	Transparency with and accountability to individuals in a jurisdiction by providing more control over how Personal Data is processed is necessary for reducing risk.	*Yes, the UAE DP Law contains analogous data protection rights to GDPR.*
Unusual limitations on individual privacy rights?	Transparency with and accountability to individuals in a jurisdiction by providing more control over how Personal Data is processed is necessary for reducing risk.	*Complaints can be filed with the UAE Data Office by any data subject. It is not clear at the time of writing how the UAE Data Office will discharge its functions, and how quickly it will be in a position to do so. As noted above, the TDGRA will support the UAE Data Office during its infancy.* *In terms of judicial rights, the UAE DP Law does not specify whether data subjects can bring a claim before a competent court for compensation for material or non-material damage.*
Surveillance / investigatory powers balanced with necessity and proportionality	Unsubstantiated, uncontrolled surveillance and the lack of access to judicial redress associated with inappropriate invasion of privacy rights through such surveillance increases risk of privacy violations.	*Unsure of the necessity and proportionality of surveillance activities. The UAE's Telecommunications Law grants the state powers to require licensed telecommunications providers to provide information and access to services on grounds related to the national interest.*
Access by government departments, agencies or international organisations	If government entities have unlimited, uncontrolled access to Personal Data for any purpose or without providing sufficient detail and support for requesting Personal Data, the risk is increased.	*The UAE DP Law includes a carve out for government entities that control or process personal data. Hence, such government access will not be subject to the UAE DP Law but rather to general laws.*

Assessment Criteria	Risk Weighting Rationale	Assessment
Access by law enforcement	If law enforcement has unlimited, uncontrolled access to Personal Data for any purpose or without providing sufficient detail and support for requesting Personal Data, the risk is increased.	*See explanation above.*
TI rating from DIFC AML Country List (to be provided as needed)	For the purposes of data sharing when required by other regulators, such as for financial crime prevention, the likelihood of government access to shared Personal Data in a high FC risk importing jurisdiction is higher and therefore a greater risk.	CONFIDENTIAL