



DATA IMPORT RISK RATING ASSESSMENT FOR DP LAW COMPLIANCE

Egypt 2022

Commissioner of Data Protection

CONTENTS

Egypt	3
1. Thematic Risk Rating Assessment	3
2. Itemized Assessment Criteria and Rating	5

Egypt

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	Low	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 / High	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.
Privacy Culture and Environmental Factors	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.

Thematic Group	Thematic Risk Rating	Thematic Rationale
Accountability and Transparency Rating	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 / High	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	Egypt TI Risk Rating High	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.
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 High	Recommendations EDMRI+ : Completing EDMRI+ is strongly recommended in order to understand potential risks of the importing entity breaching relevant data protection laws. In addition, please review both your own and the importing entity's technical, contractual, and organisation measures for controlling access to and processing of Personal Data, and mitigate as needed with addition policies, assurances and audit obligations. Adequacy: DIFC Commissioner's Office has recognised Egypt 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.	<p>Keystone piece of legislation is Law on the Protection of Personal Data (the "Egypt DP Law") introduced on 13 July 2020.</p> <p>The law is subject to Executive Regulations which are yet to be published.</p>
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.	<p>Article 4 of the Egypt DP Law requires controllers take all technical and regulatory procedures and apply the standard criteria necessary for the protection and security of personal data to ensure its confidentiality non-breach, hacking, alteration or manipulation through any illegal procedure. The Egypt DP Law does not contain any detailed cyber controls, however.</p> <p>Egyptian Computer Emergency Readiness Team ("EG-CERT") is a government agency staffed by a team of 40 full-time professionals and provides 24-hour support to protect critical information infrastructure. EG-CERT provides support to entities across the ICT, banking and government sectors and also provides general guidance to the public on protecting children online, avoiding phishing scams etc.</p>

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.	<i>Egypt has a number of sectoral data security laws and regulations that impose specific data requirements on entities in the financial, telecommunications and consumer sectors.</i>
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.	<i>Article 17 prohibits electronic marketing unless a number of conditions apply, which includes obtaining the consent of the data subject and setting clear and uncomplicated mechanisms to allow the data subject to refuse the communication or withdraw his or her consent. The sender of electronic marketing communications also has to maintain electronic records evidencing the consent received from data subjects.</i>
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.	<i>Egypt is not deemed adequate by the European Commission, and we are not aware of any other adequacy decision.</i>

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.	<p><i>Article 2 of the Egypt DP Law specify that the law applies to any person that commits any of the violations stipulated in the accompanying law, if:</i></p> <ul style="list-style-type: none"> <i>(a) the offender is an Egyptian national inside or outside of Egypt, or</i> <i>(b) a non-Egyptian residing within Egypt, or</i> <i>(c) a non-Egyptian outside of Egypt provided that the act is punishable in any form in the country where it occurred, and the data subject to the crime belongs to Egyptian nationals or non-Egyptians residing within Egypt.</i> <p><i>There is therefore an element of extra-territorial reach but it depends in part on the law of the third country in question.</i></p>
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.	<p><i>Along with the Constitution, there are data protection requirements contained in consumer protection and telecommunications laws.</i></p>
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.	<p><i>Article 19 establishes the Personal Data Protection Centre (“Centre”) to protect Personal Data and regulate the activities of processing and granting access to such personal data.</i></p> <p><i>The Centre is being established currently and will be operational in the near future.</i></p>
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.	<p><i>See above.</i></p>

Assessment Criteria	Risk Weighting Rationale	Assessment
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.	<p><i>Controllers and processors have to obtain a licence or permit from the Centre to process personal data. The Executive Regulations are intended to set out the types of licences required and conditions to apply. However, Article 26 specifies that a licence would be required for activities such as:</i></p> <ul style="list-style-type: none"> • <i>performing data safeguarding, handling and processing operations;</i> • <i>engaging in electronic marketing;</i> • <i>processing sensitive data; and</i> • <i>conducting cross-border transfers of personal data.</i> <p><i>A maximum fee payable for a licence shall be 2,000,000 Egyptian Pounds (approximately US\$125,000).</i></p>
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.	<p><i>This function falls to the Centre when it becomes operational.</i></p>
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.	<p><i>Pursuant to Article 7, each of the controller and the processor, as the case may be, must notify the Centre with any personal data infringement, within seventy-two (72) hours of such infringement. In the event that such infringement relates to national security protection concerns, the notification shall be immediate.</i></p>
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.	<p><i>In all events, the controller and the processor, as the case may be, shall notify the data subject within three (3) days from the date of notifying the Centre, with the infringement and the adopted procedures related thereto.</i></p>

Assessment Criteria	Risk Weighting Rationale	Assessment
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.	<p><i>Article 99 of the Egyptian Constitution makes any violation of personal freedom, or the sanctity of the private life of citizens, or any other public rights and freedoms which are guaranteed by the Constitution and the Egyptian Law is a crime.</i></p> <p><i>The affected party shall have the right to bring a direct criminal action. The State shall guarantee fair compensation for the victims of such violations. The National Council for Human Rights may file a complaint with the Public Prosecution of any violation of these rights, and it may intervene in the civil lawsuit in favor of the affected party at its request. All of the foregoing is to be applied in the manner set forth by Law.</i></p>
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.	<p><i>Article 8 requires all organisations that act as controllers or processors to appoint a "competent employee to be responsible for the protection of Personal Data" as DPO. The employee will have to be registered with the Centre.</i></p> <p><i>The Egypt DP Law also contains analogous data subject rights and data processing principles as the GDPR.</i></p>
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.	<p><i>EG-CERT publishes guidance on cybersecurity. Once established, the Centre will publish guidance on the processing of personal data.</i></p>

Assessment Criteria	Risk Weighting Rationale	Assessment
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.	<i>Article 12 of the Egypt DP Law requires controllers and processors to obtain a licence for the processing of sensitive personal data. The explicit written consent of the data subject is also required and, in the case of children, the legal guardian's consent.</i>
Prohibitions on specific types of data processing?	See above	<i>No, all personal data can be processed but we note a licence is required to process sensitive personal data.</i>
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.	<i>Article 33 empowers data subjects and any relevant person to file a complaint with the Centre about the processing of their personal data. The Centre's employees, who are appointed by a decision of the Minister of Justice upon the proposal of the Minister of Telecommunications and Information Technology who is the competent minister in this regard, shall have judicial control powers in relation to violations of the Law.</i>
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.	<i>Yes, the Egypt DP Law contains analogous data protection rights as the GDPR.</i>
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.	<i>Until the Centre is established data subjects seem to have a limited ability to enforce their data protection rights.</i>

Assessment Criteria	Risk Weighting Rationale	Assessment
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.	<i>Although a warrant is required to intercept communications, it would seem in practice that the Government and law enforcement have broad access to personal data.</i>
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.	<p><i>According to the Egyptian Criminal Code (Law 58 of 1937) and the Criminal Procedures Code (Law 150 of 1950), a prosecutor or investigative judge may issue a warrant authorizing the interception and recording of individual communications when investigating a possible crime.¹</i></p> <p><i>Under Article 95 of the Criminal Procedures Code, reasoned warrants from a prosecutor or investigative judge can be issued where they assist in the investigation of any felony or misdemeanor attracting a sentence of over three months, for no more than 30 days and can be renewed once; or by a direct order from an authorized member of the armed forces or security agencies. There are no explicit regulations regarding the latter.²</i></p>
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.	<p><i>The Freedom on the Net 2021 Report³ published by Freedom House, an independent NGO, notes that the government has considerable control over internet infrastructure. The Report notes that Article 67 of the Telecommunication Regulation Law (No. 10 of 2003) provides Egyptian authorities with the power to commandeer telecommunication services and networks of any operator or service provider and “call operation and maintenance employees of such services and networks in case of natural or environmental disasters or during declared periods of general mobilization in accordance with the provisions of Law No. 87 of 1960 or any other cases concerning national security.”</i></p> <p><i>Freedom House report that “surveillance is a significant concern for internet users in Egypt” and it rated Egypt 26/100 in terms of freedom on the net (0 being the least free and 100 the freest).</i></p>

¹ [Egypt | Global Network Initiative](#) (accessed 10 February 2022)

² [Egypt | Global Network Initiative](#) (accessed 10 February 2022)

³ [Egypt: Freedom on the Net 2021 Country Report | Freedom House](#) (accessed 10 February 2022)

Assessment Criteria	Risk Weighting Rationale	Assessment
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