



DATA IMPORT RISK RATING ASSESSMENT FOR DP LAW COMPLIANCE

Bangladesh 2022

Commissioner of Data Protection

CONTENTS

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

Bangladesh

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		High	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		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 / High	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		High	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		High	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		Bangladesh 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		High	Recommendations EDMRI+ : Completing EDMRI+ is required 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 not recognised Bangladesh as an adequate jurisdiction. Bangladesh is also not deemed adequate yet by either the European Commission or the United Kingdom.

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.	No
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.	<i>Digital Security Act 2018</i>
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.	No
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.	No
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.	No

Assessment Criteria	Risk Weighting Rationale	Assessment
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.	<i>Unknown, unlikely</i>
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.	<i>N/A</i>
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.	<i>No</i>
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.	<i>No</i>
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.	<i>No</i>
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.	<i>No DPA, no clear guidance</i>
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.	<i>N/A</i>
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.	<i>No</i>

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.	<i>Generally, there is a basic cultural respect for privacy.</i>
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.	<i>No requirement of conducting risk assessments regarding data processing activities, no law or other requirements for DPOs, etc.</i>
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.	N/A
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.	No
Prohibitions on specific types of data processing?	See above	N/A
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.	Yes

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.	<i>No – no DP law exists at this time</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.	N/A
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>Yes, with controls and safeguards, unsure however in practice how this plays out. Reports of imprisonment and severe corporal penalties have surfaced.</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.	<i>With controls / safeguards, as per Digital Security Act 2018</i>
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.	<i>With controls / safeguards, as per Digital Security Act 2018</i>
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