DATA IMPORT RISK RATING ASSESSMENT FOR DP LAW COMPLIANCE

United States of America 2022

Commissioner of Data Protection

CONTENTS

USA

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 / 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		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.
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 / 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		USA 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.
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+ 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 issued an adequacy decision in favor of USA, but has certain provisions in place for sharing data with government authorities such as the SEC. Please see the letter provided to the SEC for further information.

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.	*There is no single comprehensive data protection law in the USA. Data protection is governed in number of different laws at both federal and state level and the USA has several sector-specific privacy or data security laws, including laws and regulations that apply to financial institutions, telecommunications companies, personal health information, credit report information, children's information, telemarketing and direct marketing. Certain states, such as California, have quite a sophisticated data protection regime whereas other states are dependent on the patchwork federal framework.*
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.	*Most US businesses are required to take reasonable technical, physical and organizational measures to protect the security of sensitive personal information (e.g., health or financial information, telecommunications usage information, biometric data, or information that would require security breach notification). A few states have enacted laws imposing more specific security requirements for such data. For example, Massachusetts has enacted regulations that apply to any company that collects or maintains sensitive personal information (e.g., name in combination with Social Security number, driver's license, passport number, or credit card or financial account number) on Massachusetts residents.* *There numerous federal and state laws pertaining to privacy and cybersecurity.*
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.	*USA has a number of sectoral data privacy and security laws and regulations that impose specific requirements on regulated entities in the financial, insurance and health sectors, as well as regulating privacy and security of children online. Individual states have such laws as well.*

Assessment Criteria	Risk Weighting Rationale	Assessment
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.	*USA regulates marketing communications, including email and text message marketing, as well as telemarketing and fax marketing. There is no specific federal law that regulates the use of cookies, web beacons and other similar tracking mechanisms but some states, such as through the California Consumer Privacy Act (**CCPA**) in California, regulate the use of website tracking. Also, the GDPR and e-privacy in communications laws in Europe apply to many companies based in the USA.*
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 yet issued an adequacy decision in favor of USA, but has certain provisions in place for sharing data with government authorities such as the SEC. Please see the letter provided to the SEC for further information.*
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.	*There is no constitutional "right to privacy", but instead a right to due process, and specific rights that address private matters and choices. In addition, sectoral laws and state laws (currently in at least 10 states) provide for a right to privacy or privacy rights of some form.*
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.	*E.O. 12333, discussed at length in Schrems II, deals with the organization and allocation of foreign intelligence surveillance by US authorities. In addition, the CLOUD Act and other laws require quite detailed agreements, providing permissions that support access to personal data abroad for specific purposes. FISA 702 also permits such extra-territorial reach and considers privacy-related elements.*

Assessment Criteria	Risk Weighting Rationale	Assessment
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.	*The US Federal Trade Commission (FTC) has jurisdiction over most commercial entities and has authority to issue and enforce privacy regulations in specific areas (e.g., for telemarketing, commercial email, and children's privacy) and to take enforcement action to protect consumers against unfair or deceptive trade practices, including materially unfair privacy and data security practices.* *Many state attorneys general have similar enforcement authority over unfair and deceptive business practices, including failure to implement reasonable security measures and violations of consumer privacy rights that harm consumers in their states.* *The California Attorney General has the authority to enforce the CCPA and most California consumer privacy laws.* *In addition, there is a range of sector-specific regulators, particularly those in the healthcare, financial services, telecommunications and insurance sectors, have authority to issue and enforce privacy and security regulations, with respect to entities under their jurisdiction*
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.	*See above.*
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.	*There is no national requirement to register databases or personal information processing activities. States have certain requirements however. As previous members of Privacy Shield, and as members of CBPRs and PRPs vis a vis APEC, where US companies can certify, certain registration requirements exist.*
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.	*There is no regulator with general authority to issue guidance. There is however state based information and support available, and the FTC are heavily involved in Global CBPR forum development as well as one of the 9 member economies to adopt the APEC CBPR.*
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.	*All 50 US states, Washington, DC, and most US territories (including, Puerto Rico, Guam and the Virgin Islands) have passed breach notification laws that require notifying state residents of a security breach involving more sensitive categories of information e.g., social security numbers.*

Assessment Criteria	Risk Weighting Rationale	Assessment
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.	*All 50 US states, Washington, DC, and most US territories (including, Puerto Rico, Guam and the Virgin Islands) have passed breach notification laws that require notifying state residents of a security breach involving more sensitive categories of information e.g., social security numbers.*
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.	*While there is no national law at this time, the constitutional basis for ensuring basic rights is taken quite seriously in the USA. Culturally, privacy is an issue for various reasons, which is evident in laws around healthcare, banking and finance, protection of children online, and with respect to fraud and identity theft.*
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.	*There is no general requirement to appoint a data privacy officer in national law. State laws may require it as needed for specific compliance purposes, however. All above-named laws account for similar accountability and privacy principles and best practices to some degree.*
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.	*USA has sector-specific laws for data in the financial services, healthcare, telecommunications, and education sectors and specific federal legislation for children's data.*
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 national schemes or codes, but there are industry codes of conduct generally.*

Assessment Criteria	Risk Weighting Rationale	Assessment
Prohibitions on specific types of data processing?	See above	*This depends on the specific sector law. The federal Children's Online Privacy Protection Act for example prohibits the collection of any information from a child under the age of 12 online and from digitally connected devices.*
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.	*Individuals can enforce their rights in the USA's judicial system. The difficulty to enforce rights in local courts coupled with the issue of bulk surveillance was key factor in Schrems II ruling.*[1]
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.	*Certain states facilitate some data protection rights.*
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.	*None.*
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.	*While surveillance is undertaken for various reasons in the USA, including in bulk, there are specific obligations on government organisations that provide for elements of necessity and proportionality. This view is not necessarily shared by all external assessors, and is the subject of EU case law.*

[1] In Schrems II, the CJEU concluded there is not effective ex-post legal redress for data subjects in respect of Section 702 of FISA and E.O. 12333. According to the CJEU, Article 47 of the Charter entitles "everyone whose rights and freedoms" are violated "to a hearing by an independent and impartial tribunal." The CJEU explained that the surveillance programs based on Section 702 of FISA and E.O. 12333, even as limited by PPD-28, fail to meet this standard because they do not give data subjects actionable rights in the courts against the US authorities. The CJEU further rejected the position that the Privacy Shield Ombudsperson could provide sufficient redress, as nothing indicated that "*the ombudsperson has the power to adopt decisions that are binding on those intelligence services*." Given these reasons, the CJEU invalidated Privacy Shield as a US-EU data transfer tool.

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.	*Subject to warrant, judicial review, other requirements.*
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.	*Subject to warrant, judicial review, other requirements.*
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

Appendix A: Individual States

California

Florida

New York

Virginia