15 April 2024

# iManage Transfer Impact Assessment

## Purpose of this Transfer Impact Assessment

This Transfer Impact Assessment ("**TIA**") has been prepared in response to the Schrems II decision, the EDPB Recommendations (the "**Recommendations**"), the UK ICO's Transfer Risk Assessment guidance, and for the purposes of clauses 14(a) and 14(c) of the EU Standard Contractual Clauses and UK Addendum to the EU Standard Contractual Clauses. This TIA provides an assessment of whether the laws or practice of a third country, where iManage processes personal data, impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR/UK GDPR transfer tools. Where any risks have been identified, it provides details of the appropriate supplementary measures which iManage implements to mitigate these risks, aimed at maintaining a level of protection afforded by EEA and UK law standards. In addition to fulfilling iManage's data protection obligations under the Standard Contractual Clauses and UK IDTA, this TIA will assist iManage's customers with their own due diligence obligations as data controllers/data exporters.

## 1. Introduction

iManage is committed to enabling customers to use all iManage services in compliance with EEA and UK data protection laws, including the GDPR and UK GDPR. The steps laid out in this TIA outline how customers can conduct assessments of their use of the iManage services in accordance with the Schrems II ruling, the Recommendations, and the Standard Contractual Clauses, and as a result, enable them to comply with EEA and UK data protection regulations.

For purposes of this TIA, the following definitions shall apply:

- "**Cloud Services**" means the cloud-based software-as-a-service applications provided by iManage and subscribed to by a customer.
- "**Customer Data**" means data stored within the Cloud Services that is submitted to or uploaded to the Cloud Services by or on behalf of an iManage cloud customer or its authorized users.
- "**iManage Personnel**" means individuals involved in the performance of services as employees of iManage and other individuals engaged under contract by iManage to assist in delivery of services.
- "**Personal Data**" means any information processed by iManage that relates to a data subject.
- "**Professional Services Data**" means all data provided to iManage by or on behalf of a customer (or that a customer authorizes iManage to obtain from the Cloud Services), through an engagement with iManage to obtain professional services or support services.

## 2. What is the Schrems II Decision?

On 16 July 2020, the Court of Justice for the European Union ("**CJEU**") issued a ruling confirming the validity of the European Commission's standard contractual clauses ("**SCCs**") as a legal mechanism for the transfer of personal data outside the EEA. In the same ruling, the CJEU (a) declared the EU-US Privacy Shield framework invalid, and (b) confirmed that organizations transferring personal data outside the EEA (data exporters) must, in cooperation with the recipients of such personal data (data importers), assess whether there is a level of protection for the personal data transferred that is essentially equivalent to that guaranteed in the EEA by the GDPR.

## 3. What are the EDPB Recommendations?

After the Schrems II decision, in June 2021, the European Data Protection Board ("**EDPB**") published its final Recommendations for measures that supplement transfers. The Recommendations aim to assist controllers and processors acting as data exporters with their duty to identify and implement appropriate supplementary measures where they are needed to ensure an essentially equivalent level of protection to the data they transfer to third countries. As such, the Recommendations provide exporters with the following six-step data transfer assessment (the "**EDPB DTA**"):

- Step 1: Know your transfer;
- Step 2: Verify the transfer tool your transfer relies on;
- Step 3: Assess if anything in the law and/or practices of the third country impinges on the effectiveness of the appropriate safeguards of the transfer tools being relied upon;
- Step 4: Identify and adopt supplementary measures;
- Step 5: Take procedural steps that may be required for adoption of supplementary measures; and
- Step 6: Re-evaluate.

The UK ICO's Transfer Risk Assessment guidance adopts a similar approach and identifies three key steps to assess the transfer risk:

- Step 1: Assessing the transfer;
- Step 2: Is the transfer tool likely to be enforceable in the destination country; and

- Step 3: Is there appropriate protection for the data from third-party access.

For the purpose of this TIA, we adopt the EDPB six step plan and supplement with the UK ICO's Transfer Risk Assessment guidance where appropriate to do so.

## 4. EDPB DTA

### a. Step 1: Know your transfer

iManage EMEA Limited, a private limited company registered in England and Wales, is the iManage contracting party for customers located in EMEA. iManage may process Personal Data to provide certain Cloud Services, software support services, and/or related professional services pursuant to the applicable agreement it has entered with a customer, which, for a Cloud Service customer, is the iManage Cloud Services Agreement (the "**CSA**").

The location of where Customer Data will be hosted will depend on the Cloud Services being provided to the customer. For Cloud Service customers, all Customer Data shall be stored in the geographic region set forth in the applicable order form (e.g., the United Kingdom, Netherlands, etc.), which the customer chooses at the outset. The choice of the location for the storage of Customer Data cannot be changed by iManage without the customer's consent.

No matter where iManage agrees to store Customer Data, iManage may need to process Customer Data in other regions to provide support services and professional services, including, but not limited to, preventing, detecting, investigating, mitigating, and repairing problems, including security incidents. This may include regions where certain services are performed by iManage's affiliates or sub-processors. A full list of the locations where iManage, its affiliates, and sub-processors process Customer Data or Personal Data can be found on the iManage Sub-Processors page. All data importers will act in a processor capacity and are used to provide the relevant services to customers. iManage accepts the obligation of a controller of the processing of (i) any data or statistics associated with or generated in connection with use of the services (specifically excluding Customer Data and Professional Services Data), and (ii) Personal Data to support the business operations incidental to providing the services to a customer, which may include (1) delivering functional capabilities as licensed, configured, and used by a customer and its authorized users, (2) preventing, detecting, and repairing problems, including security incidents, and (3) providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services.

### b. Step 2: Verify the transfer tool your transfer relies on

As between iManage and its customers, for any transfers outside the EEA and/or the United Kingdom (or in respect of onward transfers), iManage relies on the EU standard contractual clauses, adopted as of 4 June 2021, or where

applicable the UK Addendum to the EU standard contractual clauses, effective from 21 March 2022 for transfers subject to the UK GDPR (together the "**Standard Contractual Clauses**" and in each cases as amended or replaced from time to time), except for transfers to any country which has a valid adequacy decision from the European Commission or the UK Government as applicable. Where applicable, the Standard Contractual Clauses are incorporated into the agreement between a customer and the relevant iManage entity which governs the provision of the iManage services (including the data protection agreement which fulfils iManage's Article 28 GDPR/UK GDPR obligations). Where iManage utilizes any third-party sub-processors, it ensures a lawful transfer mechanism is in place between iManage and the relevant sub-processor.

**c.** Step 3: Assess if anything in the law and/or practices of the third country impinges on the effectiveness of the appropriate safeguards of the transfer tools being relied upon[1]

**i. Australia**

***A. Are there laws which establish the rule of law, and which protect human rights and fundamental freedoms?***

The Australian Constitution (in particular Section 5) enshrines the rule of law in Australia, specifically including five human rights. There are also a variety of other federal laws that protect fundamental freedoms and basic human rights (e.g., the Australian Human Rights Commission Act 1986).

***B. Is there a comprehensive data protection / privacy law?***

Yes, the Privacy Act 1988 (No. 119, 1988) (as amended) (the "**Privacy Act**") protects the rights of individuals to their personal data that is collected, used and disclosed by 'APP entities' subject to the Privacy Act (including Federal public authorities). The Privacy Act includes the 13 Australian Privacy Principles (the "**APPs**").

***C. What are the laws that enable public authorities or law enforcement to access personal data held by private organizations?***

Australia is a federal system with eight States and Territories plus the Federal jurisdiction. While primarily regulated at a Federal level, each State and Territory also has its own laws relating to surveillance of personal data by its public authorities (and private organizations).

[1] The country assessment includes factors to be considered when assessing both: (i) the enforceability of contractual safeguards in the destination country; and (ii) the terms of regulating third party access to data (including surveillance).

The Federal laws regulating public authority surveillance of personal data are:

- Surveillance Devices Act 2004 ("**SDA**");
- Telecommunications Act 1997 ("**TA**");
- Telecommunications (Interception & Access) Act 1979 ("**AUS TIA**");
- Australian Security Intelligence Organisation Act 1979;
- Intelligence Services Act 2001; and
- The Privacy Act.

Generally, public authorities that seek to access and use the personal data held by a private organization must obtain a warrant from an eligible judge or magistrate beforehand. However, as discussed below, some public authorities can bypass this requirement in specific circumstances under a specific law, such as when requesting technical assistance from private organizations under the TA.

In addition, the Privacy Act includes express exceptions that permit law enforcement to process personal data in a manner otherwise precluded by the Privacy Act, such as when the use or disclosure of the personal data is reasonably necessary for enforcement activities (although there is a transparency/reporting requirement in such cases).

***D. What legal bases/purposes are there for public authorities to access personal data held by private organizations? Are these bases/purposes exhaustive or do public authorities have general discretion?***

Most legal bases for a public authority's access to personal data held by private organizations (e.g., under the AUS TIA, SDA, and Privacy Act) relate to law enforcement in relation to serious crimes, prevention of terrorism, child sex trafficking and abuse, and/or national security and they are exhaustive.

Some discretion is given to the National Intelligence Community ("**NIC**") and to law enforcement agencies under the 'assistance and access' provisions of the TA as regards to assistance required to crack encryption and other security measures.

The SDA enables Federal law enforcement agencies to seek a warrant in various circumstances to install and use surveillance devices and/or access data held in computers – cover surveillance is prohibited without first obtaining a warrant.

The AUS TIA permits law enforcement under a warrant from the Attorney-General or Director-General of Security for national security reasons or otherwise by a judge in relation to a serious criminal offence, access to transmitted or

stored communications. It is an offence for a person to intercept and access private telecommunications without the knowledge of those involved without such a warrant.

The AUS TIA also requires 'Carriage Service Providers' or 'CSPs' to retain a defined subset of telecommunications metadata during the course of providing services for two years and to provide access to law enforcement under a warrant obtained by that agency on the basis as noted above. This obligation does not relate to the content of the activities but rather information regarding the details of the communication (i.e., metadata) as set out under section 187AA of the AUS TIA.

The TA enables certain law enforcement agencies to require (without a warrant) assistance from certain private organizations to access the communication systems, products, and services, where necessary. It is focused on requiring private sector entities who may supply communications services or products that are used with or on the telecommunications network to assist those agencies to break any encryption or security measures in place (i.e., so they can gain access). A private organization which considers an agency's request to not be reasonable, proportionate, practicable or technically feasibly may make a complaint to the relevant oversight body, which for requests issued by national security agencies will be the Inspector-General of Intelligence and Security ("**IGIS**").

***E. Are there limitations and/or safeguards to the legal bases/purposes for public authorities to access personal data held by private organizations?***

Overall, Australia has generally strict conditions on access to and use of personal data by public authorities, such as requiring warrants issued by certain judges, the Attorney General or the Director-General of Security.

One exception relates to the recent amendments, primarily to the TA, introduced by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth). Under these new laws, all 'designated communications providers,' broadly defined so as to include not only telecommunications carriers and service providers but any entity that supplies an 'electronic service' (including websites and secure messaging apps), will be required upon receiving a technical assistance notice to provide technical assistance to law enforcement. In other words, certain Australian law enforcement agencies can require a cloud service provider, for example, to decrypt encrypted communications for the purposes of law enforcement.

Under the AUS TIA, service providers must retain metadata for two years following the closure of the account to which the information/document related or, otherwise, two years from the time the information/document came into existence, after which period, the metadata must be deleted.

***F. Has an independent supervisory authority been established which provides oversight for the protection of privacy, and what is its role?***

Yes, the Privacy Commissioner is responsible for oversight and enforcement of the Privacy Act and the APPs. The Privacy Commissioner also determines any complaints made by individuals about invasions of their privacy/breaches of the APPs affecting them.

Under the AUS TIA, the Commonwealth Ombudsman must inspect the records of enforcement agencies to determine the extent of compliance of the agency and its officers with key obligations under the AUS TIA.

An independent Inspector-General of Intelligence and Security examines the legality and propriety of the activities of the AIC. In addition, of the Australian Intelligence Community, most of the AIC agencies' activities and exercise of powers require the authorization of the responsible ministers.

Judicial oversight of AIC activities is limited, with the courts having little involvement in the issuing or monitoring of warrants. The only specialized tribunal is the Security Division of the Administrative Appeals Tribunal, which may conduct a merits review of most categories of adverse security assessments issued by ASIO.

The Independent National Security Legislation Monitor does not oversee the AIC agencies themselves but has a related function of reviewing the operation, effectiveness and implications of counterterrorism and national security legislation, including ASIO's special powers relating to terrorism.

***G. Is the supervisory authority completely independent and impartial when performing its duties and exercising its powers?***

Yes, the OAIC is an independent statutory agency. As noted under the Privacy Regulatory Action Policy, the OAIC acts independently and takes action that is impartial and objective. In line with 'rule of law' principles, the Privacy Act/APPs are enforced against public and private sector activities in the same way.

In addition, the IGIS and Commonwealth Ombudsman are independent oversight agencies, while the AAT conducts independent merit reviews of decisions made by the Government. Likewise, the ACCC operates as an independent

statutory authority and exercises powers in relation to consumer complaints that may overlap with privacy and data protection issues.

***H. Are there clear, precise, and accessible rules for the processing of personal data for surveillance/law enforcement purposes carried out by the competent supervisory authority?***

Yes, law enforcement bodies are required to comply with the Privacy Act to the extent it is consistent with carrying out relevant law enforcement functions. However, the Privacy Commissioner notes that various intelligence and national security agencies are not subject to the OAIC or provisions under the Privacy Act, meaning these entities will not be limited by or required to comply with the APP's provisions. Otherwise, the privacy framework does not itself set out precise rules for personal data that is processed for the purposes of law enforcement. Instead, such rules are contained in the establishing and/or empowering statute associated with each law enforcement agency. Such legislation generally: (a) clearly states the functions and powers of the relevant agency; (b) how they are to be exercised; and (c) consequences (usually criminal penalties) for misuse/abuse of those powers.

***I. What are the oversight mechanisms for the approval and review of relevant actions by public authorities? Are there oversight mechanisms in place for when actions by public authorities are conducted in secret?***

See sections F - H immediately above. These oversight mechanisms apply generally and to the covert or secret activities of public authorities, in particular law enforcement and NIC agencies.

***J. Are there legal remedies for data subjects?***

For any surveillance or access to personal data which is not authorized by law or a court (e.g., by a warrant) there are either or both criminal sanctions and/or civil redress under the relevant law (e.g., SDA, AUS TIA, and TA) or under the Privacy Act for an invasion of privacy/breach of the APPs. As such, an individual who experiences an unauthorized processing of personal data is entitled to bring a complaint to the Privacy Commissioner, who in turn may investigate and publish enforceable determinations. For unauthorized surveillance direct action in the Courts is available or by complaint to the police for criminal prosecution.

***K. Can an organization refuse to comply with a request and what remedies are available to them?***

No, not where such a 'request' is in accordance with the relevant law or a warrant. However, where the request is not pursuant to law or a warrant which obliges one to comply or if the request for 'access and assistance' under the TA is a voluntary request (i.e., a 'Technical Assistance Request'), an organization may refuse to comply with such a request.

L. ***Do the above provisions apply to both residents/citizens of the jurisdiction and to foreign data subjects? If not, what are the differences?***

Yes, the above laws are applied equally to both residents/citizens of Australia and to foreign data subjects.

M. ***Has the jurisdiction entered into international commitments, such as legally binding conventions or instruments related to data protection? For example, Convention 108.***

Australia has signed/adopted the following international privacy related commitments:

- International Covenant on Civil and Political Rights;
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data;
- Asia-Pacific Economic Cooperation Privacy Framework; and
- APEC Cross Border Privacy Rules.

N. ***Is there any further information that is relevant in regard to public authorities' access to personal data held by private organizations?***

Australia is part of the 'Five Eyes' international surveillance network run by the United States National Security Agency. As a result, Australia shares intelligence and possibly the personal data of individuals obtained from private organizations under/in accordance with Australian law with the other members of the network.

O. ***Risk?***

This TIA concludes that there are indications that the laws of Australia, at present, do not provide an equivalent level of protection considering fundamental rights under EEA and UK law. This may lead to a level of risk posed by this data transfer on rights and freedom of data subjects.

Risk: Low; requires supplementary measures

Transfer can go ahead because supplementary measures are in place.

iManage has never received a request for data from any public authority (Australia or otherwise).

## ii. Brazil

### A. *Are there laws which establish the rule of law, and which protect human rights and fundamental freedoms?*

Yes, Brazil has constitutional protection of human rights and fundamental freedoms, among which are the protection of people's intimacy, private life, honour and image (Article 5(X) of the Brazil Constitution) as well as the secrecy of correspondence and communications (Article 5(XII) of the Brazil Constitution). It is also worth noting that the Brazilian National Congress has recently passed the Draft Constitutional Amendment No. 17/2019, now into the Constitutional Amendment No. 115/2022, on including 'data protection' specifically as a fundamental right in the Brazil Constitution.

### B. *Is there a comprehensive data protection / privacy law?*

Yes, the Data Protection Directive with respect to Law Enforcement (Directive (EU) 2016/680) and Law No. 13.709 of 14 August 2018, General Personal Data Protection Law (as amended by Law No. 13.853 of 8 July 2019) ("**LGPD**"), which is a statutory law on data protection and privacy in Brazil. The LGPD entered effect on 18 September 2020 and the administrative sanctions provisions entered into force on 1 August 2021.

### C. *What are the laws that enable public authorities or law enforcement to access personal data held by private organizations?*

The LGPD excludes from its application the processing of personal data for the exclusive purposes of public security, national defence, State security or investigation or repression of criminal offenses (Article 4(III) of the LGPD). In order to elaborate a bill to regulate these activities, the National Congress created a Committee of Professors and Researchers in the field that are currently developing the first version of the document.

An exception to the constitutional rule of privacy protection is possible only by judicial order in criminal procedure, according to the Telephone Calls Interception Law (Law n. 9.296/1996) and the Brazilian Civil Rights Framework for the Internet (Law n. 12.965/2014).

### D. *What legal bases/purposes are there for public authorities to access personal data held by private organizations? Are these bases/purposes exhaustive or do public authorities have general discretion?*

LGPD states that processing of personal data by public authorities should be performed to achieve its public purpose, in the pursuit of the public interest, for the purpose of performing the legal attributions or duties of the public service. There is room for interpretation that public authorities can also process personal data using the same legal basis as private companies and individuals.

It is important to emphasize that activities carried out by public authorities with purposes of public security, national defense, state security or investigation, or repression of criminal offenses are out of the LGPD's scope.

***E. Are there limitations and/or safeguards to the legal bases/purposes for public authorities to access personal data held by private organizations?***

Public authorities only can process personal data to achieve its public purpose, in the pursuit of the public interest, for the purpose of performing the legal attributions or duties of the public service.

The LGPD defines in Article 25 that data held by public authorities must be maintained in an interoperable and structured format for shared use by public authorities, with a view to the implementation of public policies, the provision of public services, the decentralization of public activity and the dissemination and access of information by the general public.

***F. Has an independent supervisory authority been established which provides oversight for the protection of privacy, and what is its role?***

The Brazilian data protection authority ("**ANPD**") was established by Articles 55-A to 55-L of the LGPD. The ANPD's regimental structure was formalized by Decree n. 10.474 on 26 August 2020, and the first directors were appointed by the President of Brazil in October 2020. To date, the ANPD has conducted its work on the publication of guidance and regulation of the main topics foreseen in the LGPD.

***G. Is the supervisory authority completely independent and impartial when performing its duties and exercising its powers?***

The ANPD is a government body under the Executive Federal Power, endowed with technical and decision-making autonomy, with jurisdiction in the national territory. Although the ANPD is an authorized member of the Presidency, it has the independence to act, and it is not subordinate to the Federal Executive Power on the Article 1 of the Internal Regulation of ANPD.

***H. Are there clear, precise, and accessible rules for the processing of personal data for surveillance/law enforcement purposes carried out by the competent supervisory authority?***

The parties in judicial or administrative proceedings and defendants in general are ensured an adversary system and a full defense, with the means and resources inherent therein, by the Brazil Constitution.

Resolution CD/ANPD No. 1/2021 on the Inspection Process and the Sanctioning Administrative Process (only available in Portuguese here), and Resolution No 4/2023 for the regulation of the dosimetry and application of administrative penalties (only available in Portuguese here) will apply for these purposes.

I. ***What are the oversight mechanisms for the approval and review of relevant actions by public authorities? Are there oversight mechanisms in place for when actions by public authorities are conducted in secret?***

The LGPD applies also to public authorities (Articles 23 to 30), except their activities with purposes of public security, national defence, State security or investigation or repression of criminal offenses (Article 4(III)), that will be regulated separately (as it is done in the European Law Enforcement Directive 680/2016).

J. ***Are there legal remedies for data subjects?***

Yes, there are legal remedies, especially since 1988 Constitution with the institution of Habeas Data, later regulated also by Law n. 9.507/1997, and by Law of Access to Information (Law n. 12.527/2011). We must highlight that the LGPD adds new rights for data subjects (not only related to access, but also to correct, exclude, request anonymization, etc.) and these also apply for requests against public authorities.

K. ***Can an organization refuse to comply with a request and what remedies are available to them?***

It is only possible to refuse to comply with a request if there is a justification under the LGPD (for example: if the organization cannot exclude specific personal data that must be held for legal obligation). However, it is possible to discuss the matter with the judiciary.

L. ***Do the above provisions apply to both residents/citizens of the jurisdiction and to foreign data subjects? If not, what are the differences?***

Yes, applicable to both.

M. ***Has the jurisdiction entered into international commitments, such as legally binding conventions or instruments related to data protection? For example, Convention 108.***

Brazil is currently waiting as an observer under the Convention 108 (further information available here). Brazil is a party to the International Covenant on Civil and Political Rights ("**ICCPR**").

***N. Risk?***

This TIA concludes that there are indications that the laws of Brazil, at present, do not provide an equivalent level of protection considering fundamental rights under EEA and UK law. This may lead to a level of risk posed by this data transfer on rights and freedom of data subjects.

Risk: Low; requires supplementary measures

Transfer can go ahead because supplementary measures are in place.

iManage has never received a request for data from any public authority (Brazil or otherwise).

**iii. Canada**

This transfer benefits from an adequacy decision granted pursuant to the 2002/2/EC: Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC. Transfers subject to the UK GDPR benefit from the same adequacy decision position by virtue of Part 3, Schedule 21 of the Data Protection Act 2018.

Risk: adequacy decisions can be revoked and invalidated.

iManage will regularly monitor the status of the adequacy decision and carry out an additional TIA in the event of any change.

**iv. EEA**

Transfers to the EEA which are subject to the UK GDPR benefit from an adequacy decision granted pursuant to Part 3, Schedule 21 of the Data Protection Act 2018.

Risk: adequacy decisions can be revoked and invalidated.

iManage will regularly monitor the status of the adequacy decision and carry out an additional TIA in the event of any change.

**v. India**

***A. Are there laws which establish the rule of law, and which protect human rights and fundamental freedoms?***

Yes, the Constitution of India establishes the rule of law and protects various fundamental rights.

Some of these rights include: (i) the right to equality, where every person is guaranteed equality before the law and equal protection of laws within the territory of India; (ii) prohibition of discrimination by the State against any citizen on grounds of religion, race, caste, sex, or place of birth; (iii) the right to freedom, which includes the freedom of speech and expression and the freedom to carry on any occupation, trade, or business; (iv) the right to life and personal liberty (the scope of this right has been interpreted by courts to include the right to privacy); and (v) the right to constitutional remedies to enforce fundamental rights.

While the Constitution of India guarantees the protection of human rights and fundamental freedoms, different legislations also afford the protection of human rights.

**The Human Rights Act**

The Human Rights Act, 1993 as amended by the Protection of Human Rights (Amendment) Act, 2019, establishes the National Human Rights Commission ("**NHRC**") and various State Human Rights Commissions. These bodies have a range of powers for the protection and promotion of human rights. One of the functions of the NHRC is to initiate an inquiry, whether on a *suo moto* basis or due to a complaint, of violations of human rights, or negligence to prevent such violations, by public servants. For the purposes of inquiries, the NHRC has the powers of a civil court. These powers include summoning witnesses and examining them on oath, receiving evidence, requisitioning records from any court or office, and the discovery and production of any document.

**Laws for the protection of women**

Laws have been enacted to protect and promote the interests of women, including the National Commission for Women Act, 1990, the Maternity Benefit Act, 1961, the Protection of Women from Domestic Violence Act, 2005, and the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013.

**Laws for the protection of children**

Laws have been enacted to protect and promote the interests of children, including the Child and Adolescent Labour (Prohibition and Regulation) Act, 1986, the Protection of Children from Sexual Offences Act, 2012 and the Commissions for the Protection of Child Rights Act, 2006.

**Other Laws**. Some of the other laws that secure and promote human rights include the Mental Healthcare Act, 2017, which protects individuals with mental illnesses; the Rights of Persons with Disabilities Act, 2016, which protects individuals with disabilities; and the Transgender Persons (Protection of Rights) Act, 2019, which protects transgender individuals.

### *B. Is there a comprehensive data protection / privacy law?*

Yes, the Digital Personal Data Protection Act, 2023 ("**DPDP**") was enacted on 11 August 2023, and is estimated to come into force in a phased manner over 2024. It is intended as a comprehensive legal framework to regulate the digital ecosystem.

The DPDP, once in force, will replace Section 43A of the Information Technology Act, 2000 (the "**IT Act**") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the "**SPDI Rules**") in their entirety. Until such time as the DPDP comes into effect, the IT Act and SPDI Rules continue to apply, as such we also refer to them in this TIA.

### *C. What are the laws that enable public authorities or law enforcement to access personal data held by private organizations?*

**Digital Personal Data Protection Act**

Under the DPDP, organizations are permitted to disclose personal data to the State or agents of the State without consent or notice. While the DPDP generally empowers individuals with the right to access the identities of the organizations with whom their personal data has been shared, this right does not apply where the data has been shared with data fiduciaries authorized under law to obtain such data, and where such sharing is pursuant to a written request by another data fiduciary for the purpose of prevention, detection, or the investigation of offenses or cyber incidents, or for the prosecution or punishment of offenses.

**The Telegraph Act**

Under the Telegraph Act, 1885 and the rules thereunder, the Government has the power to temporarily possess licensed telegraphs and order the interception or disclosure of messages sent through such devices.

The definition of a 'telegraph' is fairly wide: it means any appliance, instrument, material, or apparatus used (or that is capable of being used) for transmission or reception of signs, signals, writing, images, and sounds or intelligence of any nature by wire, visual, or other electro-magnetic emissions, radio waves or Hertzian waves, or galvanic, electric, or magnetic means.

**The IT Act**

Both the central and state governments have the power to direct any government agency to intercept, monitor, or decrypt any electronic information.

The Government also has the power to authorize any government agency to monitor and collect traffic data or information that is exchanged through a computer resource. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (the "**Interception of Information Rules**") and the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 (the "**Monitoring of Traffic Data Rules**"), issued under the IT Act, establish procedural rules to carry out this interception and monitoring.

**The SPDI Rules**

Under the SPDI Rules, government agencies mandated under the law to obtain sensitive personal data or information (a limited category of personal data that includes passwords, financial data, health and medical-related data, biometrics, and sexual orientation) have the power to request such information from companies. Failure to comply with these requests is punishable by fines.

The SPDI Rules expressly require private organizations to share information with government agencies to verify identities of individuals or for the prevention, detection, investigation, prosecution, and punishment of offences. In this regard, government agencies are required to clearly state the purpose for which they seek access, and that the information will not be published or shared with any other third party (which is generally understood to not prohibit sharing within governmental organizations or departments).

To be held valid, any state action that violates an individual's right to privacy must pass constitutional tests on proportionality, necessity, and legality. These tests have been widely applied to the State's transgressions of violations of fundamental rights in the past.

**The CERT-In Directions**

The CERT-In Directions empower the Indian Computer Emergency Response Team ("**CERT-In**") to require service providers, intermediaries, data centres, and body corporates to take action, provide information, or any other assistance to CERT-In, which may contribute toward cybersecurity mitigation actions and enhance cybersecurity situational awareness.

**The Code of Criminal Procedure**

The Code of Criminal Procedure, 1973 enables law enforcement agencies to seize personal devices in the course of an investigation or inquiry into a criminal offence.

***D. What legal bases/purposes are there for public authorities to access personal data held by private organizations? Are these bases/purposes exhaustive or do public authorities have general discretion?***

**The Telegraph Act**

Under this law, messages may be intercepted on the following grounds: (i) on the occurrence of any public emergency; (ii) in the interest of public safety; (iii) in the interests of the sovereignty and integrity of India; (iv) in the interest of the security of the State; (v) in the interest of friendly relations with foreign states; (vi) for public order; or (vii) to prevent the commission of an offence.

**Digital Personal Data Protection Act**

The DPDP provides for a specific lawful basis under which data fiduciaries may disclose personal data to the State or any of its instrumentalities, subject to such processing being in accordance with the law on disclosure under other applicable laws.

**The IT Act**

Under this law, interception, monitoring, or decryption of electronic information can occur on the following grounds: (i) in the interest of sovereignty or integrity of India; (ii) in the interest of the security of the State; (iii) in the interest of friendly relations with foreign states; (iv) for public order; or (v) to prevent the commission of or investigate an offence.

The collection and/or monitoring of traffic data or information through any computer resource can occur on the following grounds: (a) to forecast imminent cyber incidents; (b) to monitor network applications; (c) to identify and determine viruses or computer contaminants; (d) to track cybersecurity breaches or incidents; (e) to track or identify any person who has breached or is suspected of having breached or being likely to breach cybersecurity; (f) to undertake forensic analyses as a part of investigations or internal audits of information security practices; (g) to access stored information for the enforcement of cybersecurity law; or (h) for any other cybersecurity-related matter.

Government agencies may seek sensitive personal data or information from companies to: (1) verify identities of individuals; or (2) prevent, detect, and investigate offences.

***E. Are there limitations and/or safeguards to the legal bases/purposes for public authorities to access personal data held by private organizations?***

**Digital Personal Data Protection Act**

The State is only permitted to process personal data as set out in law in India, in the interest of sovereignty, and in the interests of the integrity of India and the security of the State. iManage does not process personal data that is likely to be of interest to the State in India.

**The Telegraph Act**

Records in connection with interceptions should be destroyed by authorities every six months unless there are functional requirements for the records to be retained. Further, the telecom regulator (and all service providers who have been directed by the regulator) should destroy records that pertain to directions issued regarding interception of messages within two months of the discontinuance of the interception of such messages.

**The Interception of Information Rules**

All records of intercepted, monitored, or decrypted information should be destroyed by the relevant government security agency every six months, unless there are functional requirements for their retention.

Persons in charge of the underlying computer resource in question should destroy records that pertain to directions issued regarding the interception within two months of the discontinuance of the interception, monitoring, or decryption (as the case may be), unless the information is required for any ongoing investigation, criminal complaint, or legal proceedings.

**The Monitoring of Traffic Data Rules**

All records that pertain to the monitoring or collection of traffic data should be destroyed after the expiry of nine months from the receipt of direction for interception or the creation of the record, whichever is later, unless there are functional requirements for retention.

Persons in charge of the underlying computer resource in question should destroy records that pertain to directions to monitor or collect traffic data or information within six months of the discontinuance of such monitoring or collection, unless the information is required for any ongoing investigation, criminal complaint, or legal proceedings.

In addition to these specific safeguards, the Constitution of India would offer the general protection that any request to access data not be: (i) arbitrary; (ii) unreasonable; or (iii) disproportionate. India's constitutional history is littered with instances of the judiciary censuring executive action for overreach or arbitrariness.

**Digital Personal Data Protection Act**

The lawful bases for disclosures to the State only apply in the circumstances set out above. The legal basis of making a disclosure to fulfil an obligation under law only applies to laws in force in India.

***F. Has an independent supervisory authority been established which provides oversight for the protection of privacy, and what is its role?***

The DPDP established the Data Protection Board of India ("**Board**") as the adjudicatory body for data protection. The Board is responsible for overseeing compliance with the DPDP, including the State disclosure exemption.

Until such time as the DPDP comes into effect, there is no independent supervisory authority that oversees the protection of privacy. However, the Ministry of Electronics and Information Technology ("**MeitY**") supervises communication that occurs through electronic systems and data breaches may be reported to the Indian Computer Emergency Response Team, established by MeitY under the IT Act.

***G. What are the oversight mechanisms for the approval and review of relevant actions by public authorities? Are there oversight mechanisms in place for when actions by public authorities are conducted in secret?***

The law introduces certain accountability measures and processes.

**The Telegraph Act**

Procedure for issuing directions:

1. The interception of messages should not be undertaken if there are other reasonable methods to seek such information.

2. Directions for the interception of a message may only be issued by an order of the Secretary to the Government within the Ministry of Home Affairs, and in the cases of states, the Secretary to a state government who is in charge of the Home Department of that state, or a specifically authorized officer. This role may be delegated further in emergencies.

3. Specified authorities and a review committee should approve and confirm directions for interception. Interception should cease if this approval is not provided.

4. Approvals for interception are valid for a maximum of 180 days.

**Security safeguards**

Service providers should implement adequate internal checks to ensure that unauthorized interception of messages does not occur, extreme secrecy is maintained, and utmost care and precaution is taken with regard to the interception of messages. This process should also only be managed by senior officers.

**The IT Act, the Interception of Information Rules, and the Monitoring of Traffic Data Rules**

Procedures for issuing directions:

1. The interception of messages should not be undertaken if there are other reasonable methods to seek such information.

2. All directions for interception of any message should be issued by the Secretary to the Government of India in the Ministry of Home Affairs or the Secretary to a state government who is in charge of the Home Department of that state. These roles may be further delegated in unavoidable circumstances or in emergencies.

3. Directions are subject to approval from specified authorities and a review committee.

4. The directions to intercept, monitor, or decrypt information can remain valid for a period of up to 180 days.

Designated officers of intermediaries or persons who are in charge of computer resources should provide all information to the authorities that seek the interception and cooperate in this regard.

**The SPDI Rules**

Authorized government agencies may require companies to share sensitive personal data without obtaining the consent of the data subject but are required to refrain from publishing or sharing this information.

***H. Are there legal remedies for data subjects?***

Any restriction on the right to privacy, as established by the Supreme Court in a judgment that affirmed the right as a fundamental right in 2017, has to be justified on the following three grounds:

- there should be a law;
- the law should aim to achieve a public purpose; and
- the public purpose should be proportionate to the infringement of privacy.

Separately, if data subjects suspect surveillance through an illegal order in contravention of existing law, they may invoke the courts' writ jurisdiction to quash the illegal surveillance order.

Under the DPDP, data subjects have the right to have readily available means of grievance redressal, and data subjects have the right to approach the Board, after exhausting the opportunity of redressing the grievance pursuant to the DPDP.

***I. Can an organization refuse to comply with a request and what remedies are available to them?***

There are no 'ordinary' grounds on which an organization can refuse to comply with the request made by a public authority. Any organization is entitled to invoke the 'extraordinary' supervisory jurisdiction of the High Courts to challenge any such request.

***J. Do the above provisions apply to both residents/citizens of the jurisdiction and to foreign data subjects? If not, what are the differences?***

The rights to equality, life and personal liberty, and privacy apply to all persons regardless of citizenship, while the right to freedom applies to only Indian citizens.

The Telegraph Act applies to both citizens and foreign nationals within the Indian territory.

The IT Act applies to both citizens and foreign nationals within the Indian territory. It also applies to any offence committed outside India if the offence involves a computer resource or network located in India.

The DPDP applies to the processing of digital personal data: (a) within the territory of India where the personal data is collected, (i) in digital form, or (ii) in non-digital form and digitised subsequently, and (b) outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to data subjects within the territory of India.

***K. Has the jurisdiction entered into international commitments, such as legally binding conventions or instruments related to data protection? For example, Convention 108.***

India is not a party to any conventions or international instruments related to data protection. Although, it is a party to the ICCPR, which generally references a right to privacy.

***L. Is there any further information that is relevant in regard to public authorities' access to personal data held by private organizations?***

Other legislation through which certain authorized persons or public authorities may have access to personal data held by private organizations are:

**The Code of Criminal Procedure**

Authorities may seek information or documents in connection with criminal investigations.

**The Companies Act**

Authorities under the Companies Act, 2013 have the power to conduct search and seizure of certain documents or properties that relate to a company.

**The Income Tax Act**

Authorities have the power to conduct search and seizure in respect of commissions of offences under the Income Tax Act, 1961.

**The Prevention of Corruption Act**

Police officers have the power to inspect any bankers' books that relate to the accounts of persons who are suspected to have committed an offence under the Prevention of Corruption Act, 1988, or of any other person who is suspected to hold money on behalf of such person.

**The Prevention of Money Laundering Act**

Designated officers are permitted to conduct a search of the premises of an organization and seize any record or property found as a result of the search under the Prevention of Money Laundering Act, 2002.

***M. Risk?***

This TIA concludes that there are indications that the laws of India, at present, do not provide an equivalent level of protection considering fundamental rights under EEA and UK law. This may lead to a level of risk posed by this data transfer on rights and freedom of data subjects.

Risk: Low; requires supplementary measures

Transfer can go ahead because supplementary measures are in place.

iManage has never received a request for data from any public authority (India or otherwise).

**vi. Japan**

This transfer benefits from an adequacy decision granted pursuant to Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information. Transfers subject to the UK GDPR benefit from the same adequacy decision position by virtue of Part 3, Schedule 21 of the Data Protection Act 2018.

Risk: adequacy decisions can be revoked and invalidated.

iManage will regularly monitor the status of the adequacy decision and carry out an additional TIA in the event of any change.

## vii. Singapore

### A. *Are there laws which establish the rule of law, and which protect human rights and fundamental freedoms?*

There is no express right to privacy in the Singapore Constitution. While Part IV of the Singapore Constitution protects certain fundamental liberties (e.g., right to life and personal liberty; equal protection of the law; freedom of speech, assembly, and association; freedom of religion), these rights are not absolute and are generally subject to certain exceptions or restrictions.

Nonetheless, there is a broad framework of common law and statutory torts in Singapore which indirectly protect privacy-related interests (e.g., nuisance, trespass to the person, defamation, and law of confidence). Moreover, the Protection from Harassment Act (Cap. 256A) enshrines in statute the tort of harassment, and provides a range of remedies against harassment and false statements of facts.

### B. *Is there a comprehensive data protection / privacy law?*

The primary data protection legislation is the Personal Data Protection Act 2012 (No. 26 of 2012) ("'**PDPA**") which sets out a baseline standard of protection for personal data across organizations. The PDPA operates concurrently with other sector-specific regulations and other laws which may also address issues relating to privacy and data protection.

### C. *What are the laws that enable public authorities or law enforcement to access personal data held by private organizations?*

There is no general legislation in Singapore which specifically relates to the surveillance conducted by public authorities of personal data held by private organizations. However, please see our answers below for a discussion on the general powers according to Singapore public authorities to access and seize data (which may include personal data) held by private organizations.

For completeness of understanding, Singapore public agencies are not subject to the data protection provisions under the PDPA as they have their own set of data protection rules which all public officers must comply with. Public agencies are defined in the PDPA to include the Government of Singapore ('the Government'); any ministry, department, agency, or organ of State; any tribunal appointed under any written law; or any specified statutory body. That said, this exemption does not extend to organizations working on behalf of government agencies.

***D. What legal bases/purposes are there for public authorities to access personal data held by private organizations? Are these bases/purposes exhaustive or do public authorities have general discretion?***

There is no overarching legislation which specifically relates to the surveillance conducted by public authorities of personal data held by private organizations. Notwithstanding, there are certain laws in Singapore which empower the Singapore authorities to access and seize data stored in Singapore (which may include personal data), whether for domestic purposes, or at the request of a foreign country. Depending on the laws in question, there are certain requirements and safeguards put in place in relation to the exercise of such power, for example, the requirement to obtain a court order.

Some of these statutory provisions which allow Singapore authorities to do so are as follows:

**Criminal Procedure Code**

Part IV of the Criminal Procedure Code (Cap. 68) ("**CPC**") gives authorities broad powers to seize relevant property, inspect computers (defined broadly to include, e.g. any data processing device) and access and decrypt data. For instance, Section 35(1) of the CPC allows a police officer to 'seize, or prohibit the disposal of or dealing in, any property: (i) in respect of which an offence is suspected to have been committed; (ii) which is suspected to have been used or intended to be used to commit an offence; or (iii) which is suspected to constitute evidence of an offence'.

We also highlight that under section 40 of the CPC, the Public Prosecutor may authorize a police officer to, for the purposes of investigating an arrestable offence, *inter alia*, 'require any person whom he reasonably suspects to be in possession of any decryption information [in relation to encrypted data under investigation] to grant him access to such decryption information as may be necessary to decrypt any data required for the purposes of investigating the arrestable offence.'

**Telecommunications Act**

Under the Telecommunications Act (Cap. 323) ("**Singapore TA**") and other regulatory instruments, the Info-communications Media Development Authority ("**IMDA**") is empowered to, by order, require any person to produce to IMDA any document or information, which IMDA considers to be related to any matter relevant to an investigation or for discharging its functions under this Act (section 59 of the Singapore TA).

Furthermore, telecommunications licensees may also be required pursuant to the conditions of their licence to provide documents and information when requested by IMDA.

**Official Secrets Act**

Section 9 of the Official Secrets Act (Cap. 213) ("**OSA**") states that where it appears to the Minister that such a course is expedient in the public interest, he may, by warrant, require the owner or controller of any telecommunication system used for the sending or receipt of messages to or from any place out of Singapore, to produce such messages.

**Prevention of Corruption Act**

Section 22 of the Prevention of Corruption Act (Cap. 241) allows the Director of the Corrupt Practices Investigation Bureau or any Magistrate, by warrant directed to any special investigator or police officer, to enter that place by force if necessary and to seize and detain any document or property, where there is reasonable cause to believe that it relates to the commission of a relevant offence.

Singapore government authorities are granted wide discretion under the relevant provisions as set out above. The provisions are worded broadly, and Singapore authorities generally do not need to obtain court orders to require private organizations subject to such legal obligations to comply.

Nonetheless, under Singapore law, government authorities do not have unfettered discretion. Any such administrative action by a public authority may be subject to judicial review by the courts, provided that the relevant thresholds are met. The grounds by which the Singapore courts may invalidate the authority's actions include illegality, irrationality, and procedural impropriety.

Separately, under the Mutual Assistance in Criminal Matters Act (Cap. 190A) ("**MACMA**"), the Singapore authorities are also empowered to assist certain foreign countries to, among other things, obtain evidence (e.g., data that is stored in a data center in Singapore), provided that the request is in respect of criminal matters.

Where an appropriate authority of a prescribed foreign country makes a request for the production of a thing or description of a thing for the purposes of any criminal matter in that country, the Singapore Attorney-General may apply to the court for an order to (a) compel the production of the thing to an authorized officer for him to take away, or (b) give an authorized officer access to the thing (Section 22 of the MACMA).

### *E. Are there limitations and/or safeguards to the legal bases/purposes for public authorities to access personal data held by private organizations?*

As stated above, Singapore authorities generally do not need to obtain court orders to require private organizations subject to such legal obligations to comply. However, administrative action by a public authority may be subject to judicial review by the courts, provided that the relevant thresholds are met. While the data protection provisions of the PDPA do not apply to public agencies, we note that there are in place strict laws against the disclosure of official documents and information, which may contain personal data of individuals.

For example, under the OSA, criminal penalties are imposed on any person who wrongfully communicates confidential information that has been entrusted in confidence to him by government office holders, or who fails to take reasonable care of such information by endangering the safety or secrecy of such information or otherwise. In another example, the Public Sector (Governance) Act 2018 (No. 5 of 2018) sets out directions regarding data sharing in the public sector and imposes criminal penalties on public officers who recklessly or intentionally disclose data (which may include personal data) without authorization, misuse data for a gain or re-identify anonymized data. Furthermore, we note that the Government's data security policies are set out in certain non-legally binding documents such as the Government Instruction Manual Policy on Data Management, which prescribes specific measures to protect Government data (which may include personal data).

### *F. Has an independent supervisory authority been established which provides oversight for the protection of privacy, and what is its role?*

Generally, there is no independent supervisory authority which oversees the actions of public agencies in Singapore in relation to issues of privacy. Nonetheless, there usually exist various avenues to appeal decisions or determinations to the relevant Minister or the courts. Furthermore, as stated above, Singapore administrative law provides for a judicial review mechanism which allows for the review of executive actions by the independent judiciary.

Although there is no privacy supervisory authority over public agencies *per se*, we highlight that the Personal Data Protection Commission ("**PDPC**") has been set up and appointed to be the body which oversees the protection of personal data in Singapore. The PDPC administers and enforces the PDPA and is empowered to issue directions (including administrative financial penalties) to organizations that are in breach of the data protection provisions. As of 30 August 2023, the PDPC has published over two hundred grounds of decisions or summaries of grounds of decisions, with a significant majority of these cases relating to breaches of the 'protection obligation' (Section 24 of the PDPA) due to inadequate security measures being taken to safeguard the personal data of the individuals.

With effect from 1 October 2016, the PDPC was subsumed into IMDA, which is a statutory body under the Ministry of Communication and Information.

In some sectors, organizations are also subject to the regulatory oversight of the relevant sectoral regulator (e.g. IMDA for telecommunications licensees, and the Monetary Authority of Singapore for financial institutions), which may administer and enforce certain legal obligations or regulatory requirements relating to privacy and data protection.

***G. What are the oversight mechanisms for the approval and review of relevant actions by public authorities? Are there oversight mechanisms in place for when actions by public authorities are conducted in secret?***

As mentioned above, the data protection provisions of the PDPA do not apply to public agencies. Notwithstanding, public agencies are governed by their own separate set of laws and internal standards with regard to the protection of personal data and the preservation of confidentiality.

Generally speaking, there are a number of oversight mechanisms in place. Depending on the specific laws in question, these oversight mechanisms may include: (i) the requirement for authorized officers to obtain court orders prior to requesting the production of material related to an investigation; (ii) avenues of appeal to the Minister or designated appeal panel; and (iii) judicial review by the courts of administrative action or determinations by public bodies.

***H. Are there legal remedies for data subjects?***

The PDPA gives individuals the right to make access and correction requests. In summary, an organization must, upon request, allow an individual to access and/or correct his/her personal data in its possession or under its control. In addition, the organization is also obliged to provide the individual with information about the ways in which the personal data may have been used or disclosed during the past year (Sections 21 and 22 of the PDPA).

Moreover, individuals also have the right to withdraw their consent with respect to the collection, use or disclosure of their personal data (Section 16 of the PDPA).

Individuals may lodge a complaint to the PDPC in respect of a contravention of the data protection provisions by an organization. In this regard, the PDPC has a broad range of enforcement powers which include powers to review refusal to provide access of personal data requested by the complainant, and the powers to issue directions requiring an organization to pay a financial penalty of not exceeding SGD 1 million (approx. €624,600).

As of 1 October 2022, certain changes to the financial penalty regime under the Personal Data Protection (Amendment) Act 2020 became effective. In particular, the PDPC became empowered to impose a financial penalty

on organizations in breach of the data protection provisions in the PDPA, of up to a maximum of 10% of the organization's annual turnover in Singapore (if its annual turnover in Singapore exceeds SGD 10 million (approx. €6.2 million)) or up to SGD 1 million (approx. €624,600) in any other case. An organization's annual turnover in Singapore will be ascertained from the most recent audited accounts of the organization that is available at the time the financial penalty is imposed.

With respect to avenues of appeal under the PDPA, organizations and individuals aggrieved by certain decisions or directions by the PDPC may, within a specified time period, either apply to the PDPC for reconsideration or appeal to the Chairman of the Data Protection Appeal Panel.

***I. Can an organization refuse to comply with a request and what remedies are available to them?***

With respect to requests from data subjects, we note that under the PDPA, there are specific exceptions with respect to access and correction requests, pursuant to which organizations may refuse to comply with such requests. For instance, an organization is not required to provide access to, or correct opinion data kept solely for an evaluative purpose, or a document related to a prosecution if all proceedings related to the prosecution have not been completed.

However, if such exceptions do not apply and the organization has wrongfully refused to comply with an individual's requests, this may constitute a contravention of the relevant data protection provision under the PDPA.

See above in regard to remedies relating to public authorities' actions.

***J. Do the above provisions apply to both residents/citizens of the jurisdiction and to foreign data subjects? If not, what are the differences?***

The PDPA does not make a distinction as to the nationality of data subjects. Furthermore, the PDPA applies to all private sector organizations, whether or not formed or recognized under Singapore law, or resident or having an office or place of business in Singapore.

***K. Has the jurisdiction entered into international commitments, such as legally binding conventions or instruments related to data protection? For example, Convention 108.***

Singapore has not signed or ratified any of the major international human rights treaties which uphold the right to privacy or data protection as a human right, such as the ICCPR.

Nonetheless, Singapore has entered into some non-legally binding international commitments relating to privacy and data protection, for instance, the Asia Pacific Economic Cooperation ("**APEC**") Privacy Framework, which was developed in light of the 1980 Organisation for Economic Co-operation and Development ('OECD') Guidelines, and applies to all APEC member economies, including Singapore. The APEC Privacy Framework sets out principles and implementation guidance for public and private sectors which control the collection, holding, processing, use, transfer, or disclosure of personal data.

Singapore is also a participant of the APEC Cross-Border Privacy Rules ("**CBPR**") and the APEC Privacy Recognition for Processors ("**PRP**") system. In June 2020, the Personal Data Protection Regulations 2014 was amended to recognize the APEC CBPR and PRP System certifications for overseas transfers of personal data under the PDPA.

***L. Risk?***

This TIA concludes that there are indications that the laws of Singapore, at present, do not provide an equivalent level of protection considering fundamental rights under EEA and UK law. This may lead to a level of risk posed by this data transfer on rights and freedom of data subjects.

Risk: Low; requires supplementary measures

Transfer can go ahead because supplementary measures are in place.

iManage has never received a request for data from any public authority (Singapore or otherwise).

**viii. UAE**

***A. Are there laws which establish the rule of law, and which protect human rights and fundamental freedoms?***

The Constitution of the United Arab Emirates 2011 (as amended) (the "**UAE Constitution**") provides for a broad range of human rights. In particular, some of the key Articles outlining the rights and freedoms of individuals in the UAE are set out in Chapter Two ('Basic Social and Economic Pillars of the UAE') and Chapter Three ('Freedoms, Rights and Public Duties'). Amongst the rights and freedoms provided for in the UAE Constitution is the freedom of opinion and expression (Article 30), the right to privacy (Articles 31 and 36), and the right to private property (Articles 21 and 39).

There are also a number of other UAE federal laws that protect and uphold human rights and freedoms, including:

- the Federal Decree Law No. (31) of 2021 promulgating the Crimes and Penal Code (only available in Arabic here) (the "**Penal Code**"): The Penal Code provides that all persons shall be presumed innocent

until proven guilty (Article 2). Articles 431, 432, 433, and 434 of the Penal Code also impose an obligation on individuals to respect the privacy of others;

- the Federal Decree Law No. (38) of 2022 issuing the Code of Criminal Procedure (only available in Arabic here) (the "**Criminal Procedure Law**"): Article 2 of the Criminal Procedure Law provides that no person may be arrested, searched, detained, or imprisoned except as provided for under the law and, pursuant to Chapter IV, law enforcement authorities are not permitted to enter into a person's place of residence unless in certain prescribed circumstances; and
- the Personal Status Law (Federal Law No. 28 of 2005 on Personal Affairs, as amended): Various rights pertaining to personal affairs (e.g., marriage and separation) are provided for in the Personal Status Law.

In addition, the UAE has ratified a number of international conventions in the realm of human rights, and they are in full force and effect in the UAE, including:

- the International Convention on the Elimination of all Forms of Racial Discrimination;
- the Convention on the Rights of the Child;
- the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment; and
- the Arab Charter on Human Rights.

Further, there are a number of laws that relate directly to the right to privacy, in addition to the provisions of the UAE Constitution and the Penal Code mentioned above, such as:

- the Cybercrimes Law (Federal Law No. 34 of 2021) (the "**Cybercrimes Law**"), which prohibits various acts that would infringe the privacy of individuals and provide for sanctions (such as imprisonment and/or fines) under certain circumstances set out therein. For example, Article 13 of the Cybercrimes Law provides that whoever uses information technology to collect, save, or process personal data and information pertaining to nationals and residents of the UAE in violation of the legislation in force in the UAE shall be punished with imprisonment and/or a fine in accordance with the provisions of the Cybercrimes Law; and
- the Federal Law No. 3 of 2003 Regarding the Organization of the Telecommunications Sector (as amended) (the "**Telecommunications Law**"), which outlines the laws applicable to the telecommunications sector in the UAE and specifically to telecommunication service providers. For

example, pursuant to Article 72 of the Telecommunications Law, it is prohibited for any person to copy or disclose, without a right to do so, the content of any communication, telephone message, or any telecommunication services.

***B. Is there a comprehensive data protection / privacy law?***

On November 27, 2021, the UAE Council of Ministers (the "**Cabinet**") announced the issuance of Federal Decree Law No. 45 of 2021 regarding personal data protection (available in English here and Arabic here) (the "**UAE Personal Data Protection Law**" or "**UAE PDPL**"), which serves as the UAE's comprehensive federal data protection law regulating the collection and processing of personal data, in the UAE. The UAE PDPL entered into effect on January 2, 2022. The UAE PDPL applies to the processing of personal data, which is defined as any data relating to an identified natural person or a natural person that may be identified, directly or indirectly, through the linking of data by reference to an identifier. Personal data expressly includes, among other things, an individual's name, voice, picture, identification number, and geographical location, as well as sensitive personal data (as defined under the UAE PDPL) and biometric data.

Executive regulations supplementing the UAE PDPL ("**UAE Executive Regulations**") were due to be issued by the UAE Cabinet within six months following the date of issuance of the UAE PDPL. Thereafter, 'data controllers' (defined as the establishment or natural person who determines the means, method, standards, and purposes of processing of personal data) and 'processors' (defined as the establishment or natural person processing personal data on behalf of the controller and under such controller's supervision and instruction) have a period of six months from the date of issuance of the UAE Executive Regulations to comply with the UAE PDPL However, the UAE Cabinet may extend this period.

As of 15 April 2024, the UAE Executive Regulations have not been issued. Once issued, companies will have 6 months to achieve compliance with the UAE PDPL (unless this compliance deadline is otherwise extended).

It should be noted that the UAE PDPL does includes some exclusions. These include (but are not limited to) excluding applicability to Government entities, as well as security and judicial authorities processing of personal data and/or Government Data. Furthermore, companies and entities located in free zones that have special laws regarding personal data protection (e.g. Dubai International Financial Center (DIFC) and Abu Dhabi Global Markets (ADGM)) are also excluded from applicability.

**Free Zones / Offshore Locations**

The UAE is comprised of a number of free zones (also referred to as offshore locations). Of those, two have more mature personal data protection laws that apply to entities incorporated or otherwise doing business within such locations.

1) **DIFC**: Data Protection Law No.5 of 2020 ("**DIFC DPL**") governs the processing of personal data within the DIFC. The DIFC DPL, based largely upon the EU GDPR, sets out key data protection principles, legal bases for processing personal data, special protections for sensitive personal data, data subject rights, requirements for appointing a Data Protection Officer, data breach notification obligations, rules for cross-border data transfers, and penalties for non-compliance. The Commissioner of Data Protection is responsible for enforcing the law, which is largely aligned with international data protection standards.
2) **ADGM**: the ADGM Data Protection Regulations 2021 ("**ADGM DPR**"), which govern the processing of personal data within the jurisdiction of the ADGM. The ADGM DPR set out key data protection principles, legal bases for processing personal data, special protections for sensitive personal data, data subject rights, requirements for appointing a Data Protection Officer, data breach notification obligations, rules for cross-border data transfers, and penalties for non-compliance. The Office of Data Protection is responsible for enforcing the ADGM DPR, which are largely aligned with the EU GDPR.

**Sectoral Requirements**

In addition to the UAE PDPL and data privacy and protection laws that exist within freezones across the UAE, there are also sectoral requirements (particularly within healthcare and financial services) that provide protection to patients / customers over how their data may be used. By way of example:

1) **Financial Services / Banking**: Licensed Financial Institutions are required by the Article 120 of the Decretal Federal Law No. (14) 2018 to protect Consumers' Data and ensure their confidentiality ("**UAE Central Bank Law**"). This is further clarified by the UAE Central Bank Consumer Protection Regulations and related Consumer Protection Standards. This has Federal scope applying across the UAE (expect in free zones).
2) **Healthcare**: Federal Law No.2 of 2019 concerning the use of information and communications technology in health fields ("**UAE ICT Law**") regulated the use of ICT in the healthcare sector across the UAE (including across free zones) with the aim of improving use of ICT in health care, ensuring the security and safety of health data and information, and enabling the Ministry of Health and Prevention to collect, analyse and maintain health information at the country level. On 22 April 2020, the Federal Cabinet issued Cabinet Resolution No. 32 of

2020 concerning the Regulations Concerning the Use of the Information and Communications Technology in the Areas of Health ("**ICT in Health Fields Regulation**s"). The regulations provide further details, including on permission controls to access and use the central system, and on the storage and exchange of information on the central system.

It is therefore important to consider the jurisdictional complexity of the UAE as the laws may differ depending upon whether there is a federal (onshore) dimension, freezone (offshore) nexus, and/or sectoral consideration (which may or may not be overridden by or override federal UAE law).

C. ***What are the laws that enable public authorities or law enforcement to access personal data held by private organizations?***

The National Electronic Security Authority, now known as the Signals Intelligence Agency (the "**Agency**"), was established by Federal Law No. 3 of 2012 on the Establishment of the National Electronic Security Authority (as amended by Federal Law No. 9 of 2015) (the "**Agency Law**"). Broadly, the Agency is responsible for the advancement of cyber security, cyber education, and the protection of the communications networks and information systems in the UAE. The Agency Law sets out the provisions governing the Agency's access to personal data held by private organizations.

In addition to the Agency Law, Federal Law No. 20 of 2019 on the Establishment of the Monitoring and Control Centre (the "**Monitoring and Control Law**") established the Monitoring and Control Centre (the "**Centre**") and regulates the Centre's access to and surveillance of personal data held by private organizations.

It is important to note that across sectors (e.g. banking, healthcare etc), there are laws and regulations that also grant authority for public authorities to access personal data. For the purpose of this analysis, we have limited our review to federal requirements that apply across the UAE, key freezones (DIFC and ADGM), and two core sectors (healthcare and banking).

**Access to banking information**

The UAE Central Bank Law provides that all data and information relating to customers' accounts and deposits are considered confidential in nature and cannot be directly or indirectly disclosed to any third party without the written permission of the owner of the account or deposit (or their legal attorney or authorized agent). Pursuant to Article 120(5), the Central Bank of the United Arab Emirates (the "**Central Bank**") also has the power to establish additional rules and conditions relating to the exchange of banking and credit information in its capacity as the competent

regulatory authority in the UAE in this regard. Article 26 of the UAE Central Bank Law outlines additional confidentiality obligations (together with any exemptions) in respect of banking and credit information held by financial institutions (and other related parties) in the UAE. Confidential information may be disclosed in certain circumstances, such as where disclosure is 'permitted, legally enforced, or addressed to authorities and agencies within the State or in other jurisdictions' or with the prior written consent of the account owner.

**Access to Health Information**

As noted above, **the UAE ICT Law** regulates the use of ICT in the healthcare sector across the UAE. This includes enabling the **Ministry of Health and Prevention** to collect, analyse and maintain health information at the country level. In particular, Art. 5 of the UAE ICT Law provides that the Ministry shall establish the central system to keep, exchange and collect the health data and information.

**Government Entity Exclusion from the UAE PDPL**

As noted above, the UAE PDPL specifically excludes its applicability to Government entities, as well as security and judicial authorities processing of personal data and/or Government Data.

***D. What legal bases/purposes are there for public authorities to access personal data held by private organizations? Are these bases/purposes exhaustive or do public authorities have general discretion?***

**Agency Law**

Article 5 of the Agency Law prescribes the Agency's competencies, and the Agency has broad powers to carry out its objectives, which could potentially include the power to access personal data held by private organizations. Pursuant to Article 13, the Agency is permitted to take 'all necessary measures' to verify the UAE's communication network and information systems are not exposed to any illegal access or to discover areas in the network or systems that have malfunctioned in order to avoid any contravention of the Agency Law. Likewise, the Agency is permitted to establish the 'necessary controls' to prevent any attempt to hinder or otherwise damage the communications network or information systems and may carry out any act necessary to avoid the occurrence of such instances, both from within and outside the UAE (Article 14 of the Agency Law).

In certain circumstances, the Agency may monitor, penetrate, process, eliminate, jam, or otherwise block communications networks, information systems, and communication and email devices belonging to any person or entity where it appears to the Agency that such an entity or person has participated in any act that may affect the

UAE's 'security, doctrine, heritage, civilization, public system, social peace, international and regional relations, or vital utilities […] or that may affect the life or funds of any person' in the UAE. The conditions in which such monitoring may take place are broadly as follows (Article 14 of the Agency Law):

- in matters of urgency;
- after consultation with the National Security Advisor; and
- 'provided that the competent public prosecution is informed of the measure taken by the Agency within one week so that it can conduct its affairs in respect of such measures.'

**Monitoring and Control Law**

In addition to the Agency Law, pursuant to Article 4 of the Monitoring and Control Law, the Centre aims to manage and regulate the use of 'Monitoring and Control Devices' (defined in Article 1 of the Monitoring and Control Law as the process of using and directing a monitoring and control device towards a person, group of persons, utilities, facilities, vehicles or others) in vital places and utilities, as well as in any public and private facilities, and also supervise monitoring and control related systems. Public facilities are those owned by Governmental Entities (as defined in the Monitoring and Control Law) and allocated for the management of public utilities and the provision of government services, whilst private facilities are those not owned by a Governmental Entity that carry out a commercial or industrial activity (Article 1 of the Monitoring and Control Law).

It should be noted that the Centre is subject to all the laws and regulations which are applicable to the Supreme Council for National Security (Article 21 of the Monitoring and Control Law). The competencies of the Centre are set out in Article 5 of the Monitoring and Control Law, which outlines nine powers and competencies that the Centre may perform in order to achieve its objectives. Broadly, among the Centre's powers is the ability to set conditions and procedures for the practice of implementing and installing Monitoring and Control Devices and to establish a database for all monitoring and control-related information to serve the objectives and competencies of the Centre.

***E. Are there limitations and/or safeguards to the legal bases/purposes for public authorities to access personal data held by private organizations?***

The limits on the actions of public authorities are as set out in the relevant legislative provisions above.

*F. Has an independent supervisory authority been established which provides oversight for the protection of privacy, and what is its role?*

**Federal Supervisory Authority**

Pursuant to Federal Decree Law No. 44 of 2021 on the establishment of the UAE Data Office (the "**Data Office Law**"), the Data Office shall be established and affiliated with the UAE Cabinet. Under Article 3 of the Data Office Law, the Data Office has broad competencies, including implementing control over the application of the UAE Data Protection Law and conducting the necessary investigations to ensure compliance with the UAE Data Protection Law.

In accordance with Article 2 of the Data Office Law, the Data Office shall enjoy legal personality, financial and administrative independence, and legal capacity to undertake the activities necessary to implement its competencies.

Article 6 of the Data Office Law confirms that the Data Office shall have an annual budget and financial resources, as set out in the Data Office Law. Moreover, under Article 24 of the UAE PDPL, a data subject may lodge a complaint with the Data Office if the data subject has reason to believe that a contravention of the UAE PDPL has been committed. According to Article 24(3) of the UAE PDPL, the Data Office may impose administrative sanctions in the event of a contravention by the data controller or processor of the provisions of the UAE PDPL.

As of 15 April 2024, it is unclear as to the exact status of the establishment of the UAE Data Office. It is likely the UAE Data Office will be formalised ahead of the issuance of the UAE Executive Regulations.

**Free zone Authorities**

**DIFC's Commissioner of Data Protection**: As noted above, the DIFC's DPL is regulated by the Commissioner of Data Protection who is responsible for enforcing the law. The DIFC Commissioner's office is very active and engages globally with regulators including the UK's Information Commissioner's Office. The UK has identified six "top priority" destinations for adequacy and the DIFC is the only such destination in the Middle East. The decision to include the DIFC as a "top priority" destination is a strong endorsement of the DIFC's legislative, administrative, and executive efforts around the promotion and enablement of modern innovative businesses in a manner with due regard to personal data.

**ADGM's Office of Data Protection**: The Office of Data Protection is responsible for enforcing the ADGM DPR.

**Sectoral Authorities**

Banking / Financial Services – as noted above, the UAE Central Bank govern and regulate federal financial services, including the consumer protection regulations and standards.

Healthcare – as noted above, the UAE Ministry of Health & Protection governs and regulates healthcare data.

***G. What are the oversight mechanisms for the approval and review of relevant actions by public authorities? Are there oversight mechanisms in place for when actions by public authorities are conducted in secret?***

Article 41 of the UAE Constitution provides that a person has the right to file a complaint with a competent authority, including a judicial entity, against the violation of the rights and freedoms stated in Part III of the UAE Constitution.

The primary oversight mechanism for the review of public authority action is through the UAE Courts.

With regard to the Agency Law, where the Agency acts, it is required to consult with the National Security Advisor. In the event that action is subsequently taken, the Agency's Board of Directors (established by the Supreme Council for National Security, pursuant to Article 6 of the Agency Law) is the 'supreme authority' concerned with the Agency's affairs and is liable before the Supreme Council for National Security (or such other body as specified by the Head of the Supreme Council for National Security) (Article 7 of the Agency Law). The Supreme Council for National Security thereby serves as an additional mechanism through which the Agency's actions may be reviewed. There are no provisions in the Agency Law which concern actions conducted in secret by the Agency.

In addition, in April 2017, the UAE Government issued a Guide to Access Government Information (the "**Guide**") in which it confirmed that certain 'Government Information' (as defined therein) can be provided to the public under certain circumstances. Accordingly, the ability to request details as to the personal information held by a government entity may therefore serve as a mechanism through which individuals can review the access to personal data by public authorities. The Guide explains in Section 7 that there is certain Government Information that cannot be provided to the public, including information that may be harmful to the public interest or the government entity, in the event that it is disclosed.

### *H. Are there legal remedies for data subjects?*

**Federal Law**

When enforced, Article 24 of the UAE PDPL provides the ability for a data subject to lodge a complaint with the Data Office if the data subject has reason to believe there has been a contravention of the UAE PDPL or that the data controller or processor is processing personal data in relation to the data subject in violation of the provisions of the UAE PDPL. Pursuant to Article 24(3) of the UAE PDPL, the Data Office may impose administrative sanctions in the event of any contravention by the data controller or processor of the provisions of the UAE Data Protection Law.

Specific legislation provides the relevant right to privacy relied upon to determine the remedies available. Breaches of the relevant UAE legislative provisions can result in criminal and/or civil liability, fines, and/or imprisonment (as set out above), although the extent to which such penalties may be levied against public authorities is uncertain. For example, where a breach of the Penal Code is at issue, a data subject can file a criminal complaint through the public prosecutor, and the relevant criminal court can hand down the penalty set out in the provision that has been violated. The existence of criminal penalties under UAE law for breaches of privacy rights is notable in highlighting the seriousness of data protection in the UAE.

Where a provision of the Monitoring and Crime Law has been breached, an administrative fine may be issued for each violation (Article 9 of the Monitoring and Crime Law), or the Centre may issue warnings and suspension of a license or authorization (Article 10 of the Monitoring and Crime Law). However, where a person against whom a penalty is imposed objects, such person may file a grievance before the Grievance Committee of the Centre and retain the right to appeal the issued decision before the competent court (Article 11 of the Monitoring and Crime Law).

**Free zones**

**DIFC**: Art. 60 of the DIFC DPL provides that a "…Data Subject who contends that there has been a contravention of the Law or an alleged breach of his rights under the Law may lodge a complaint with the Commissioner".

**ADGM**: Art. 57 of the ADGM DPR provides that a "…Data Subject has the right to lodge a complaint with the Commissioner of Data Protection if the Data Subject considers that the Processing of Personal Data relating to him or her contravenes these Regulations".

*I. Can an organization refuse to comply with a request and what remedies are available to them?*

In the context of the UAE PDPL (when enforced), a controller must comply with the requests received from data subjects (e.g. pursuant to Articles 13 to 18) unless the controller can rely upon an exception or is otherwise permitted to refuse adhering to such a request as set out in the PDPL.

In addition, according to Article 3 of the Data Office Law, the Data Office shall be responsible for preparing a system for complaints and grievances in relation to personal data, in coordination with the competent authorities, receiving and verifying complaints and grievances related to personal data, and issuing guidelines and instructions in respect of the implementation of the UAE PDPL.

Outside of the context of the PDPL, the primary means through which an organization can seek to challenge a request is through court proceedings.

*J. Do the above provisions apply to both residents/citizens of the jurisdiction and to foreign data subjects? If not, what are the differences?*

**UAE PDPL**

The UAE PDPL applies to UAE residents. Pursuant to Article 2(1) of the UAE PDPL, the UAE PDPL applies to the processing of personal data (as such terms are defined in the UAE PDPL), either in whole or in part, through electronic automated means, or other than by such means, by:

- data subjects who reside or have their place of business in the UAE;
- any controller or processor established in the UAE that is processing the personal data of data subjects inside or outside the UAE; and
- any controller or processor established outside the UAE that is processing the personal data of data subjects within the UAE.

Article 2(2) of the UAE Data Protection Law sets out those circumstances and types of data to which the UAE Data Protection Law does not apply. The Agency Law provides that in urgent cases, following consultation with the National Security Advisor and where there is a threat to national security, the Agency is permitted to monitor, penetrate, process, eliminate, jam, or block the communications networks, information systems, communications, and email devices belonging to 'any person or entity.'

The requirement to provide data and information required by the Centre to carry out its functions under the Monitoring and Control Law applies solely to UAE Government Entities (as defined in the Monitoring and Control Law) (Article 7 of the Agency Law). However, the Centre is permitted to carry out any tasks and competencies assigned to it by virtue of a law or decision issued by the National Security Advisor and thus may have extra-territorial scope.

The UAE Constitution applies solely to UAE citizens. However, Article 40 of the UAE Constitution proclaims that foreigners within the UAE shall enjoy the rights and freedoms stipulated in international charters that are in force, as well as the treaties and agreements to which the UAE is a party. Therefore, the privacy rights of foreigners, as enshrined in the treaties and agreements to which the UAE is a party (and set out in the section on 'Rules of law, human rights, and data protection/privacy regime' above), are generally protected.

***K. Has the jurisdiction entered into international commitments, such as legally binding conventions or instruments related to data protection? For example, Convention 108.***

While the UAE is not a signatory to Convention 108, the UAE is a party to the League of Arab States Arab Convention on Combating Information Technology Offences of 2010 (the "**Arab Convention**") (only available in Arabic here), which is binding on all 22 Arab States. The primary aim of the Arab Convention is to enhance and strengthen cooperation between the Arab States (in the area of combating information technology offenses) and to protect the security interests of their communities and individuals. The Arab Convention contains specific provisions regarding data protection; for example, Article 8 provides for the offense of deliberately and unlawfully destructing, obliterating, obstructing, modifying, or concealing information technology data.

***L. Risk?***

This TIA concludes that there are indications that the laws of the UAE, at present, do not provide an equivalent level of protection considering fundamental rights under EEA and UK law. This may lead to a level of risk posed by this data transfer on rights and freedom of data subjects.

However, it should be noted that the DIFC is being assessed independently of the wider UAE. The UK government is considering an adequacy decision for the DIFC, but this would not apply to the entire country. This provides an indication that in the context of transfers of personal data to the DIFC only (and not storage, transfer or access to personal data from onshore / wider UAE) may pose materially lower risks of harm to data subjects and therefore if this is the case, further analysis should be conducted into the dataflows in question.

Risk: Low; requires supplementary measures

Transfer can go ahead because supplementary measures are in place.

iManage has never received a request for data from any public authority (the UAE or otherwise).

**ix. United Kingdom**

This transfer benefits from an adequacy decision granted pursuant to the Commission Implementing Decision of 28.06.2021 pursuant to Regulation (EU) 2016/679.

Risk: adequacy decisions can be revoked and invalidated, and this adequacy decision will only apply for a period of four years.

The adequacy decision for the United Kingdom is due to be reviewed in 2024 and will expire on 27 June 2025 unless renewed. iManage will regularly monitor the status of the adequacy decision and carry out an additional TIA in the event of any change.

**x. United States of America**

***A. Overview of US surveillance laws***

For information on US laws, including the Foreign Intelligence Surveillance Act 1978 (FISA) section 702, please review the Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II White Paper that the US Department of Commerce, Department of Justice, and the Office of the Director of National Intelligence jointly issued in September 2020, detailing the limits and safeguards pertaining to their access to data in response to the Schrems II ruling (the "**US White Paper**"). The key points of the US White Paper are as follows:

- Most U.S. companies do not deal in data that is of any interest to U.S. intelligence agencies and have no grounds to believe they do. They are not engaged in data transfers that present the type of risks to privacy that appear to have concerned the CJEU in Schrems II.

- The US White Paper directly states: "The theoretical possibility that a U.S. intelligence agency could unilaterally access data being transferred from the EU without the company's knowledge is no different than the theoretical possibility that other governments' intelligence agencies, including those of EU Member States, or a private entity acting illicitly, might access the data. Moreover, this theoretical possibility exists with respect to data held anywhere in the world, so the transfer of data from the EU to the United States in particular does not increase the risk of such unilateral access to EU citizens' data. In

summary, as a practical matter, companies that fall in this category have no reason to believe their data transfers present the type of data protection risks that concerned the ECJ in Schrems II."

- There is individual redress, including for EU citizens, for violations of FISA section 702 through measures not addressed by the court in the Schrems II ruling, including FISA provisions allowing private actions for compensatory and punitive damages.

- The U.S. government frequently shares intelligence information with EU Member States, including data disclosed by companies in response to FISA 702 orders, to counter threats such as terrorism, weapons proliferation, and hostile foreign cyber activity. Sharing of FISA 702 information undoubtedly serves important EU public interests by protecting the governments and people of the Member States.

- There is a wealth of public information about privacy protections in U.S. law concerning government access to data for national security purposes, including information not recorded in Decision 2016/1250, new developments that have occurred since 2016, and information the CJEU neither considered nor addressed.

**Clarifying Lawful Overseas Use of Data Act (Cloud Act) – enacted March 2018**

The following is a summary of iManage's position related to the Cloud Act.

- Governmental and regulatory bodies need to follow the applicable legal process to obtain valid and binding orders (whether that be under the CLOUD Act, the UK Crime Act or other applicable act), and iManage will review all such orders and challenge as appropriate, such as not a US person (under the CLOUD Act), or if there is a risk of violating the laws of the country where the data is stored (e.g., the Netherlands).

- As a general rule, iManage does not provide any governmental or regulatory body with unfettered access to Customer Data (nor does the CLOUD Act require it).

- iManage gives prior notice to customers of any third-party requests for their data, except if prohibited by law. Except in the most limited circumstances, iManage believes governments can obtain information directly from a customer, without jeopardizing its investigation or risking harm to individuals, just as they did before such customer moved to the iManage cloud. With that in mind, iManage believes that customers can, except in the most exceptional circumstances, be notified about government requests for their data. The US Department of Justice appears to agree with this position as it published recommended

practices to prosecutors, advising prosecutors to seek data directly from the enterprise, rather than the cloud services provider (if doing so will not compromise the investigation) (https://www.justice.gov/criminal-ccips/file/1017511/download).

- iManage does not give access to platform encryption keys. iManage does not provide any government with encryption keys or the ability to break the iManage encryption. The CLOUD Act does not require companies to break their own encryption. It is also important to point out that all data stored on the iManage cloud is encrypted, and iManage provides customers with the option to manage their own encryption keys.

- The United States has a CLOUD Act Agreement with the United Kingdom which makes it easier for American and British law enforcement agencies, with appropriate authorization, to obtain electronic data regarding serious crime, including terrorism, child sexual abuse, and cybercrime, directly from communication providers / technology companies based in the other country.

**EU-US Data Privacy Framework**

On July 10, 2023, the European Commission adopted its adequacy decision for the EU-US Data Privacy Framework ("**DPF**"). The DPF is a self-certification programme, building on the prior EU-US Privacy Shield. US companies can certify their participation in the DPF by committing to comply with a detailed set of privacy obligations. This could include, for example, privacy principles such as purpose limitation, data minimisation and data retention, as well as specific obligations concerning data security and the sharing of data with third parties. As of 12 October 2023, organizations operating in the UK may also rely on the DPF from transfers from the UK to the US, relying on the UK Extension to the DPF.

The European Commission and UK Government's decisions means that personal data can be transferred from the UK and / or EU to companies which self-certify under the DPF without any other data transfer mechanisms (similar to Standard Contractual Clauses or Binding Corporate Rules). Further, organizations transferring personal data to importers who participate in the DPF will not need to carry out transfer risk assessments, because the DPF benefits from an adequacy decision.

In the light of the adequacy decisions, data exporters should confidently be able to conclude that US law as it pertains to organizations certified under the DPF, meets UK and EU requirements in this regard.

Enforcement of the DPF itself continues to be by the Federal Trade Commission (FTC) and the Department of Transportation (DoT). The European Commission and UK Government will monitor the DPF through periodic checks and ensure compliance by US authorities. If the US does not meet its commitments, the DPF could be suspended by the UK or EU.

The US Government has implemented a two-tier mechanism to address complaints from individuals in the UK or EU where data has been transferred to the US, in respect of access by US intelligence agencies. Individuals can submit complaints to their national data protection authority, which are then passed to the US via the European Data Protection Board. The initial investigation of complaints is performed by the US intelligence community's 'Civil Liberties Protection Officer'. If needed, individuals can appeal a complaint to the newly established Data Protection Review Court ("**DPRC**"), an independent entity comprised of individuals who are not part of the US Government. The DPRC can enact binding decisions, including the ability to order the deletion of improperly collected data. Throughout the investigation, the court appoints a special advocate to represent the complainant's interests. Once the investigation concludes, the complainant is informed that either no violation of US law was identified, or that a violation was found and remedied. A reasoned decision of the court can be released later once and if confidentiality requirements have concluded.

***B. Risk?***

This transfer benefits from an adequacy decision based on the DPF.

Risk: adequacy decisions can be revoked and invalidated, and this adequacy decision is subject to periodic review.

iManage is certified to the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the commitments they entail. iManage agrees to notify customers if it decides that it can no longer meet its obligation to provide the same level of protection as is required by the principles of the Data Privacy Framework program.

iManage will regularly monitor the status of the adequacy decision and carry out an additional TIA in the event of any change.

This TIA concludes that, outside of organizations certified under the DPF (like iManage), there are indications that the laws of the United States of America, at present, do not provide an equivalent level of protection considering fundamental rights under EEA and UK law. This may lead to a level of risk posed by this data transfer on rights and freedom of data subjects. However, as set forth above, the DOJ regulations and the DPF aim to address the two failings

the CJEU cited in invalidating the Privacy Shield: lack of necessity and proportionality limits on US surveillance programs and insufficient redress rights to challenge unlawful government surveillance. Both the substance and legal structure of these components matter under the CJEU's essential equivalence test.

Risk: Low; requires supplementary measures

Transfer can go ahead because supplementary measures are in place.

iManage has never received a request for data from any public authority (USA or otherwise).

**d.** Step 4: If the laws or practices of the third countries mean that the use of the transfer tool alone would not provide an essentially equivalent level of protection, identify the supplemental contractual, technical, or organizational measures that are necessary to bring the level of protection of the data transferred up to the EEA standard of essential equivalence[2]

The Recommendations identify a non-exhaustive list of supplementary measures (contractual, technical, or organizational) that may be effective to ensure an equivalent level of protection. iManage has adopted a number of such supplementary measures to mitigate the risks identified in this TIA. Where applicable, the supplementary measures are incorporated into the agreement between a customer and the relevant iManage entity which governs the provision of the iManage services (including, but not limited to, the CSA).

**i. Contractual measures**

iManage makes a number of contractual commitments related to the measures it takes to protect Personal Data. In short, iManage makes contractual commitments to:

- Implement certain technical measures intended to protect Personal Data;
- Cooperate with customers with regard to data subjects, supervisory authorities, and other obligations to ensure compliance with data protection legislation; and

[2] The supplemental contractual, technical, or organizational measures include the type of measures identified to supplement the appropriate transfer tools.

- Attempt to redirect any public authority requesting Personal Data to the applicable customer; if legally permitted to do so, notify the applicable customer about the request; assess the legitimacy of any public authority request; and, if there are grounds to do so, challenge such request.

**ii. Technical Measures**

iManage has implemented and will maintain the following security measures intended to protect Customer Data, Professional Services Data, and Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. iManage may adapt or replace such measures from time to time based on changes in applicable legal and regulatory requirements, best practices, and industry standards related to privacy and data security; provided that, iManage will not materially decrease the security measures.

| Security Measure | Practices |
|---|---|
| Organization of Information Security | **Security Ownership**. iManage has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.<br><br>**Operational Policy**. iManage maintains security documents describing its security measures and the relevant procedures and responsibilities of iManage Personnel with access to Customer Data, Professional Services Data, or Personal Data.<br><br>**Security Roles and Responsibilities**. iManage Personnel with access to Customer Data, Professional Services Data, and Personal Data are subject to confidentiality obligations. |
| Network Security | **Application Access**. Access to the Cloud Services is provided via a secure HTTPS connection. Industry-standard best practices are implemented to restrict access to backend components of the Cloud Services and ensure that public-facing web servers maintain the highest security ratings. These practices include, but are not limited to:<br>• Implementation of firewalls and proxies with monitoring to detect hostile activity;<br>• Internal segmentation utilizing standard application security methodology;<br>• Separation between production, development, and testing environments; and<br>• Full segregation between the Cloud Services and iManage corporate networks.<br><br>**System Network Access**. The Cloud Services are delivered on a dedicated, independent network isolated from all other networks, including those used for development, testing, and iManage internal IT networks. Access to the production network for each regional implementation uses a VPN connection and requires multi-factor authentication from an iManage-owned device with a valid digital certificate.<br><br>Access to the production Cloud Services network is restricted to individuals tasked with operating and deploying the production services. Authentication with a unique user ID is required, and all access to the production Cloud Services network is logged to our enterprise SIEM. Once authenticated, access to the Cloud Services is determined based on the user role and provided on a "need to know" basis.<br><br>**Software Information and Event Management (SIEM)**. The Cloud Services utilize a SIEM (e.g., Splunk Enterprise, etc.) for data and asset inventory, compliance monitoring and |

| Security Measure | Practices |
|---|---|
| | reporting, collection and analysis of security events, threat detection, and unified log management and analysis. Also included are machine analytics with host forensics. Logs are maintained for one year.<br><br>Host system event logs (e.g., system event logs, non-iManage application logs, and network logs) are ingested and analyzed to detect potential threats and an extensive range of early indicators of compromise, enabling rapid response and mitigation.<br><br>**Secure Activities within the SDLC**. iManage uses a secure software development lifecycle (SDLC) when developing new applications and creating new features in existing applications. The SDLC process provides a consistent risk-based approach to systems development that delivers quality solutions to meet business needs. Business needs such as confidentiality, integrity, and availability are implemented in all iManage applications by leveraging the following activities as early as possible in the SDLC process:<br><br>• Secure system architecture design and analysis;<br>• Static Application Security Testing (SAST);<br>• Software Composition Analysis (SCA);<br>• Dynamic Application Security Testing (DAST);<br>• Infrastructure as Code (IaC) Analysis;<br>• Container Analysis;<br>• Automated pen testing of hosted application;<br>• Manual Penetration Testing (MPT); and<br>• Manual pen testing of the hosted application<br><br>All alerts discovered in the SDLC are verified for risk and then prioritized and remediated per the risk calculation. iManage uses industry-leading application security tools and processes to assess the SDLC. |
| Encryption | **At Rest**. Customer Data at rest within the Cloud Services is encrypted using ciphers at least as strong as 256-bit advanced encryption standard (AES). At rest, encryption is mandatory for all document storage, including storage volumes supporting operating systems, backup, and recovery systems. In addition, the encryption is validated to Federal Information Processing Standards (FIPS) 140-2 level 2.<br><br>Additionally, Customer Data stored in the Cloud Service known as iManage Work provides higher levels of encryption, ensuring that (i) every version of every file stored in iManage Work is individually encrypted at rest with a randomly generated encryption key, and (ii) each encryption key is securely wrapped with a higher-level key, thereby providing a highly granular encryption model for added data security.<br><br>**In Transit**. Customer Data is protected in transit using the TLS v1.2 (or higher) protocol for authenticated and encrypted communication and is strictly enforced. The encrypted communications utilize an RSA-2048 key exchange.<br><br>**CMEK**. Certain Cloud Services also provide an add-on option where a customer may use a Customer Managed Encryption Key ("**CMEK**") to assume ownership of the primary encryption key ("**PEK**") used to encrypt Customer Data. This add-on option also allows the customer to revoke a CMEK, ensuring that Customer Data encrypted with the PEK cannot be decrypted. With a CMEK, the customer has exclusive control of the PEK. In a third-party key management service, the customer sets up the CMEK. iManage never receives or |

| Security Measure | Practices |
|---|---|
| | stores a copy of the CMEK. The customer will configure its Cloud Services environment to connect to the third-party key management service using the customer's company-specific private credentials. If the customer elects to utilize a CMEK, the customer assumes all risks and liabilities associated with such utilization. |
| Data Segregation | The Cloud Services are delivered by a shared infrastructure, but various access controls and validation mechanisms logically separate Customer Data:<br>• Implementation of zero-trust network architecture principles;<br>• Logical segregation of Customer Data stored in the Cloud Service known as iManage Work via unique per-customer encryption key hierarchy in accordance with NIST best practices;<br>• Logical metadata segregation by customer ID for metadata storage;<br>• Independent tenant administrative functions; and<br>• Containment Security Model that includes, subject to being included in the customer's subscription:<br>  ○ Highly granular security model with independent security access down to the document version level;<br>  ○ Ability to require the filing of documents and emails to a container;<br>  ○ Refiling service to ensure document and email access aligns to the container where required;<br>  ○ Users outside of the schema/library with access to content are easily recognized and can be blocked;<br>  ○ Integration with iManage Security Policy Manager to govern access by client or matter/engagement by policy; and<br>  ○ Integration with iManage Share to provide a clear distinction between content shared with external collaborators and that which is visible to internal collaborators. |
| Identification and Authorization | **Access Policy**. An access control policy (physical, technical, and administrative) based on least privileges principles is enforced to control access to Customer Data, Professional Services Data, and Personal Data.<br>**Access Authorization**.<br>• An authorization management system is maintained and designed to ensure that only authorized iManage Personnel (technical and non-technical) are granted access to systems containing Customer Data, Professional Services Data, or Personal Data.<br>• iManage Personnel accessing systems containing Customer Data, Professional Services Data, or Personal Data have a separate, unique username.<br>• Access to Customer Data, Professional Services Data, and Personal Data is restricted solely to iManage Personnel who have a need to access such Customer Data, Professional Services Data, or Personal Data in connection with the services or as otherwise required by applicable law.<br>**Authentication**. |

| Security Measure | Practices |
|---|---|
| | • Industry standard practices, including strong authentication, are utilized to identify and authenticate all iManage Personnel who attempt to access the iManage network or information systems.<br>• iManage ensures that access rights are revoked for all iManage Personnel upon the termination of their employment, or their contractual or other relationship with iManage.<br><br>**System Logs**. Access to system and network logs is provided on a need-to-know basis for operating and supporting the Cloud Services. Only iManage Personnel who deliver the Cloud Services can access the production network where the logs reside. In addition, access is restricted based on job function (e.g., DBA has access to database logs, web administrator to web server logs, system administrator to system event logs, etc.). |
| Human Resources Security | **Security Training**. All iManage Personnel with access to Customer Data, Professional Services Data, or Personal Data receive annual security training. iManage Personnel are informed about relevant security procedures and their respective roles. iManage also informs iManage Personnel of possible consequences of breaching the security rules and procedures. Additionally, all iManage Personnel that are developers or engineering managers are required to participate in annual secure software development training.<br><br>**Background Checks**. All iManage Personnel are subject to industry-standard background checks. |
| Physical Security | **Security Safeguards**. Physical security safeguards are maintained at any facilities where iManage stores Customer Data, Professional Services Data, or Personal Data. Physical access to such facilities is only granted following a formal authorization procedure and access rights are reviewed periodically.<br><br>**Facilities**. Such facilities for storing Customer Data are rated as Tier 3 data centers or greater. Such facilities use a variety of industry standard systems to protect against loss of Customer Data due to power supply failure, fire, and other natural hazards. |
| Business Continuity and Disaster Recovery | iManage performs annual business continuity testing and validation of high availability. The primary focus for iManage is to ensure the reliability and availability of the Cloud Services. However, there may be incidents and events outside iManage's control, and iManage has invested in the resources and defined processes to ensure business continuity and timely recovery of the Cloud Services in the event of a disaster.<br><br>Disaster recovery capability is included within the Cloud Services. The Cloud Services disaster recovery services include replicating Customer Data in encrypted form to a secondary location maintained in the event of a disaster. Secondary locations are located far enough away from the primary location to avoid the impact of a large-scale regional catastrophe. In addition, a global network of iManage support and operations resources ensures that in the event of a disaster, communications are maintained, and the technical resources required to recover are available.<br><br>iManage maintains a business continuity program compliant with and certified against the ISO 22301 standard to guide the development, implementation, and management of business continuity in the event of a disaster impacting iManage business operations. The iManage Business Continuity Management System (BCMS) is documented and part of the |

| Security Measure | Practices |
|---|---|
| | iManage Information Security Management System. The BCMS is reviewed, at minimum, annually. In addition, iManage Personnel involved in implementing the BCMS are trained by participating in tabletop exercises and reviewing the appropriate procedure and process documentation.<br><br>**Journaling**. Each time a document/object is modified in the Cloud Services, a copy of the original is written to a journal – this provides a complete history of every revision to a document. Any authorized user with access rights to the document can view and recover one of the prior entries maintained in the journal. In addition, documents written to the journal are retained indefinitely, or until explicitly purged, to allow a customer to recover replaced or overwritten documents.<br><br>**Backups**. iManage maintains the ability to recover all modified or deleted data objects for up to 90 days. This capability is intended for system recovery purposes only. If a customer requires recovery of individual documents, such customer should use the journal as described above. |
| Certification of Processes | **Standards**. iManage adheres, and at all times will adhere, to information security practices that comply with the requirements set forth in ISO 27001 and ISO 27017 (or substantially equivalent or replacement standards) or other generally accepted authoritative standards (e.g., SSAE 16, SOC2). iManage may add industry or government standards at any time. iManage will not eliminate ISO 27001 or any standard or framework maintained, unless it is no longer used in the industry, and it is replaced with a successor (if any).<br><br>**Independent Assessments**. On an annual basis, iManage has an independent third-party organization conduct an independent assessment of security standards. A business continuity plan is maintained that is compliant with ISO 22301. Upon a customer's request (not more than one time per calendar year), and subject to the confidentiality and non-disclosure obligations set forth in the Agreement, iManage shall make available to such customer information regarding iManage's compliance with the obligations set forth in the Agreement in the form of iManage's ISO 27001 certification and/or SOC 2 or SOC 3 reports. |
| Regularly Testing, Assessing and Evaluating the Effectiveness of the Measures | **Vulnerability Testing**. iManage conducts vulnerability testing of the Cloud Services on a monthly basis. iManage also utilizes third-party assessment services that scan iManage's external network.<br><br>**Penetration Testing**. On an annual basis, iManage undergoes penetration testing of the Cloud Services, and the cloud and corporate networks, such tests are conducted by an independent third-party organization. Testing is based on NIST SP 800-115 and NIST 800-53 standards. An executive summary of the scope and the testing results can be provided on request.<br><br>**Security Updates**. iManage uses commercially reasonable efforts to ensure that the Cloud Services operating systems and applications that are associated with Customer Data are patched and otherwise secured to mitigate the likelihood and impact of security vulnerabilities in accordance with iManage's patch management processes and within a reasonable time after iManage has actual or constructive knowledge of any critical or high-risk security vulnerabilities. |

| Security Measure | Practices |
|---|---|
| Data Minimization / Data Quality | **Data Minimization**. iManage shall make reasonable efforts to use the minimum necessary Customer Data, Professional Services Data, and Personal Data to provide the services.<br><br>**Data Quality**. At all times during a customer's subscription, such customer shall have the ability to amend and delete Customer Data to assist the customer with its data minimization and data quality obligations. |
| Data Retention | **Professional Services Data and Personal Data**. Subject to the Customer Data paragraph below, iManage shall delete or return Professional Services Data and Personal Data in accordance with the mutual agreement of the parties save to the extent that iManage is required by any applicable law to retain some or all of such data. In such event, iManage shall extend the protections of the Agreement and the DPA to such retained data and limit any further Processing of such data only to those limited purposes for which, and only for so long as, such retention is required by applicable law.<br><br>**Customer Data**. iManage will retain Customer Data for 90 days after expiration or termination of the customer's subscription so that the customer may extract Customer Data. After said 90-day period ends, iManage will disable the customer's account and delete all Customer Data (within 30 days) and, where required by law, shall certify to the customer that it has done so, save to the extent that iManage is required by any applicable law to retain some or all of such Customer Data. iManage has no obligation to return Customer Data to a customer. |
| Accountability | **Accountability**. iManage defines accountability as holding individuals accountable for their internal control responsibilities.<br><br>**Control Activities**. Specific control activities that iManage has implemented in this area are described below.<br><br>• An employee sanction procedure is in place and documented to communicate that an employee may be terminated for noncompliance with a policy or procedure, and<br>• A performance review of employees is conducted annually to evaluate the performance of employees against expected levels of performance and conduct and hold them accountable for their internal control responsibilities. |
| Portability and Erasure | **Portability**. At all times during a customer's subscription, such customer shall be able to access, extract, and delete Customer Data.<br><br>**Erasure**. iManage uses industry standard processes to destroy, delete, or otherwise make irrecoverable Customer Data, Professional Services Data, and Personal Data when it is no longer needed. |

### iii. Organizational Measures

The Recommendations state that organizational measures may consist of internal policies, organizational methods, and standards. iManage has a number of organizational measures related to the measures it takes to protect Personal Data. In short, iManage has the following organizational measures in place:

- Intragroup policies/agreements related to the transfer of Personal Data;
- Internal processes to deal with governmental requests for data, including transparency and accountability measures; and
- Adoption of strict data security and data privacy practices (e.g., ISO 27001, ISO 27017, ISO 27018, ISO 27701, CSA STAR Level 2 certification, etc.).

**Transparency and Accountability**

As stated above, iManage shall inform the applicable customer about access orders received from authorities concerning Personal Data, such information to consist at least of the number of orders, the nature of data demanded, the legal basis for such orders, and the identity of the ordering bodies, unless such information proves impossible for iManage to provide, or the disclosure of such information is otherwise legally prohibited.

To date, iManage has not received any such requests for access to any data (Personal Data or otherwise).

**e.** Step 5: Take procedural steps that may be required for adoption of supplementary measures

At this stage, no further procedural requirements have been identified, in light of the lawful transfer mechanisms adopted and described above.

**f.** Step 6: Re-evaluate

iManage shall review this TIA periodically. iManage shall also review and update this TIA in the event: (i) a new processing location is used to process Personal Data; or (ii) it becomes aware of a change in local applicable law in an existing processing location which may impact the conclusions drawn in this TIA.

This TIA was last updated on 15 April 2024, updating the versions from 1 December 2022 and 30 August 2022.