

## Data Transfer Assessment



Please indicate the **name of the data transfer assessed** (e.g. making reference to the relevant service/contract to which the data transfer relates to)

ServiceNow ticket administration system

## Step 1. Identify specific circumstances of the proposed data transfer

In this Step, we will confirm the specific circumstances of the data transfer, which will feed into later stages in the methodology

## 1.1 Countries - Jurisdictions involved in the processing

Please select the number of countries/jurisdictions in which the **data exporter** is located from the drop down list

1

Please select the countries / jurisdictions in which the **data exporter** is located from the drop down list, and, where relevant, indicate the specific Region/State

Country	State/Region
Denmark	

Please select the number of countries/jurisdictions in which the **data importer** is located from the drop down list

5

Please select the countries / jurisdictions in which the **data importer** is located from the drop down list, and, where relevant, indicate the specific Region/State. Please only take into consideration countries outside of the EEA and for which no adequacy decision pursuant to Art. 45 GDPR has been issued.

Business name (e.g. in case of subsidiary/affiliate of the data importer)	Country	State/Region	To be included in step 2?
ServiceNow Inc.	United States of America (USA)		Yes
ServiceNow UK Ltd.	United Kingdom (UK)		No
ServiceNow Australia Pty Ltd	Australia		Yes
ServiceNow Software Development India Private Limited	India		Yes
ServiceNow Japan G.K	Japan		No

Please add any further comments in the box  
→

The data exporter decides which personal data to upload into the ServiceNow solutions instance and the purpose for which it uses ServiceNow's services. The personal data is accessed remotely by non-EU ServiceNow Affiliates for the delivery of the ServiceNow offering, namely supporting a ticket handling system utilized by the data exporter.

## 1.2 Information on data exporter

Please answer the questions below, filling the corresponding cells with the required information

A) What is the **full business name of the data exporter**?

Kamstrup A/S

B) In which **economic sector** does the data exporter operate? (e.g. public vs. private, adtech, telecommunication, financial, etc.)

Manufacturer of system solutions for smart energy and water metering

C) In what **privacy role** is the data exporter acting (e.g. data controller, data processor, sub-processor)?

Data Processor to its customers

## 1.3 Information on data importer

Please answer the questions below filling the corresponding cells with the required information

A) What is the **full business name of the data importer**?

ServiceNow Group entities

B) In which **economic sector** does the data importer operate? (e.g. public vs. private, adtech, telecommunication, financial, etc.)

Delivery of business-to-business digital workflow solutions.

C) In what **privacy role** is the data importer acting (e.g. data controller, data processor, sub-processor)?

Sub-processor

D) What is the **relationship between the data importer and data exporter** (e.g. affiliate of data exporter, service provider, other)?

The data importer is a market leading service provider.

E) Is there a **contractual relationship directly between the data exporter and the data importer**? If the answer is no, please provide the details of the contractual counterparty in section 1.3.1 below

Yes

## 1.4 Information on onward transfers

Please answer the questions below, selecting the adequate options from the drop down list and filling the corresponding cells with the required information. Please only take into consideration countries/jurisdictions outside of the EEA and for which no adequacy decision pursuant to Art. 45 GDPR has been issued.

A) Will the data importer perform any onward transfers (i.e. to third parties / other countries)?

No

## 1.5 Nature of personal data

## Categories of personal data

<input type="checkbox"/> Identification data (name, address, telephone, ...)	<input type="checkbox"/> Work records	<input type="checkbox"/> Financial characteristics (bank account, credit card details, ...)	<input type="checkbox"/> Leisure activities and interests
<input type="checkbox"/> Personal characteristics (age, gender, civil status, ...)	<input type="checkbox"/> Medical records	<input type="checkbox"/> Electronic identification data (e-mail, IP addresses, cookies, ...)	<input type="checkbox"/> Professional interests
<input type="checkbox"/> Physical data (height, weight, ...)	<input type="checkbox"/> Health records	<input type="checkbox"/> Electronic location data (GPS position, ...)	<input type="checkbox"/> Consumption habits
<input type="checkbox"/> Racial or ethnic data	<input type="checkbox"/> Biometric identification data (fingerprints, iris scans, ...)	<input type="checkbox"/> Web history and logs	<input type="checkbox"/> Housing characteristics (house type, ...)
<input type="checkbox"/> Family & household (spouse, children, ...)	<input type="checkbox"/> Genetic data	<input type="checkbox"/> Appointments, Schedules, Calendar Entries	
<input type="checkbox"/> Education and training	<input type="checkbox"/> Data concerning sexual life	<input type="checkbox"/> Pictures & video (e.g. in directories, on websites, ...)	
<input type="checkbox"/> Profession and job	<input type="checkbox"/> Religious or philosophical convictions	<input type="checkbox"/> Images (CCTV, etc.)	
<input type="checkbox"/> National register number / social security identification number	<input type="checkbox"/> Political opinions	<input type="checkbox"/> Sound recordings (call recordings, ...)	<input type="checkbox"/> Other (please specify in the comment box below)
<input type="checkbox"/> Criminal convictions and offences	<input type="checkbox"/> Trade union membership	<input type="checkbox"/> Employees performance	
	<input type="checkbox"/> Memberships (sport clubs, ...)	<input type="checkbox"/> Psychological data (personality, character, ...)	

Please add any further comments in the box  
→

The ServiceNow solution offer a free-text solution and the data exporter may decide to submit personal data at its own discretion as needed to fulfill the purpose of the contract.

## 1.6 Nature of data subjects

Please select the categories of data subjects whose personal data is involved in the processing

Please insert in the cell below any additional category of data subjects

## Categories of data subjects

<input type="checkbox"/> Employees and collaborators	<input type="checkbox"/> Internet Website users	<input type="checkbox"/> Minors
<input type="checkbox"/> Clients	<input type="checkbox"/> Job applicants	<input type="checkbox"/> Sales Representatives (BDs)
<input type="checkbox"/> Prospects	<input type="checkbox"/> Providers	<input type="checkbox"/> Other (please specify in the box ->)

The personal data transferred will primarily relate to the end-users of the Kamstrup meters (the customers of the data controller). Personal data on employees within the data exporters organisation may be transferred.

## 1.7 Purposes of the intended processing

Please answer the questions below filling the corresponding cells with the required information

A) What are the **purposes for which the data importer intends to process the data**?

The personal data is transferred to the data importer in order to utilize the workflow solutions offered and will be accessed remotely by non-EU ServiceNow Affiliates for the delivery of the ServiceNow offering, namely supporting a ticket handling system.

## 1.8 Data storage and limitation of access to data

Please answer the questions below, filling the corresponding cell with the required information

A) Please describe the **steps taken to ensure the limitation of access to data** (e.g., whether restricted access is possible or full access to whole datasets is necessary) **and the transfer is adequate, relevant and limited to what is necessary**, e.g., whether the data will be stored in the third countries or only remote access to data stored within the EEA/UK will be possible including **details on the storage locations of data transferred and transmission channels used**, where available

The data importer will access the personal from the jurisdictions specified in section 1.1. Personal data will be stored at the ServiceNow datacentres in Amsterdam (EU/EEA-region) and the non-EU ServiceNow entities will access the personal data in order to provide the agreed services.

The data importer will have wide access to the IT systems of the data exporter for the purpose of its tasks. The data importer will, however, be restricted access to IT systems not necessary for its tasks.

## 1.9 Data format

Please answer the questions below, filling the corresponding cell with the required information

A) Please indicate the **level of protection ensured by the format in which the data are transferred**, in transit and at rest. (e.g. plain text, pseudonymised or encrypted)

Data will be remotely accessed by non-EU ServiceNow Affiliates.

## 1.10 Envisaged transfer tool

Please answer the questions below filling the corresponding cells with the required information

A) What is the **proposed legal basis for transferring the data** under Art. 46 GDPR, e.g. EU standard contractual clauses (SCCs), Binding Corporate Rules (BCRs)? Please select a choice from the drop down list.

EU SCCs Controller to Controller (Commission Decision (EC) 2004/915) or Controller to Processor SCCs (Commission Decision (EC) 2010/67)

## 1.11 Applicable laws and practices specific to the transfer

Please answer the questions below, filling the corresponding cells with the required information

A) Please include **details on the application of laws and practices of the third country** requiring the disclosure of personal data to public authorities or granting public authorities access to personal data relevant **in light of the specific circumstances of the transfer**.

N/A

## Step 2. Consider the laws and practices in the destination country/countries

In this Step, assess the extent to which the pervasive legal framework and practices in each of the third countries to which the data is transferred (the 'destination country') provide legal protections for personal data that are essentially equivalent to the guarantees ('EDGs') offered within the EEA and consistent with the restrictions set out in the GDPR and guarantees provided for in the relevant transfer terms (e.g. EU SCCs of Commission Decision No. 2021/914). In case there are multiple destination countries, including with respect to onward transfers, please select an overall level of safeguards and indicate any peculiarities of each legal regime in the comment box below each section. This Step 2 will not assess the laws or practices specific to the circumstances of the transfer, which will be assessed separately at Step 4.

This assessment will follow the principles set out in Article 45(2) GDPR (the test for adequacy of a third country), take into account the criteria set out in the EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures of 10 November 2020 (the 'EDPB European Essential Guarantees Recommendations') (which are however mere recommendations and, as such, not binding), and consider the following key factors as applicable to the specific transfer:

## 2.1 Regulation on the processing of personal data

4

The extent to which **local laws** offer legal clear, precise and accessible safeguards to the processing of personal data equivalent to the protections offered in the EEA/UK. This will include an analysis of the local laws, practices, and data protection law framework, including constitutional rights to privacy and how those laws apply both to the data importer but also third parties (e.g. requiring to disclose data to law enforcement/public authorities or authorising access by such authorities) who may seek to secure access to the data following transfer, as well as the applicable limitations and safeguards.

In this context, note the EEA / UK has a developed law that specifically recognises legal rights to protection of 'personal data' consistent with the principles of data protection set out in OECD Convention 106.

- ☐ 1 - high level of safeguards in place, essentially equivalent to the level available in the EU
- ☐ 2 - high level of safeguards in place, but below the level of those available in the EU
- ☐ 3 - some safeguards in place, but materially below the level of those available in the EU
- ☒ 4 - very limited safeguards in place, significantly below the level of those available in the EU
- ☐ 5 - no safeguards in place

Complete  
Country  
Analysis 2.1

Hide Analysis

Country Analysis		Score
Please add any further comments in the box →	UNITED STATES OF AMERICA (USA) : In general, while many privacy laws exist, the balance of federal and state law is focused on data security, meaning that many businesses focus on the protection of personal data from breach events. Where privacy laws do exist, they do not offer data subject rights in a manner comparable with EEA/UK law. The US at the federal level lacks generally applicable data protection laws. Many states have laws that cover privacy and security issues in particular. Moreover, California has imposed both privacy and security laws that are general in nature, applying to controllers doing business in California and potentially imposing significant penalties.	4
	AUSTRALIA : The Federal Privacy Act does have areas of overlap with the GDPR, including in relation to its data protection principles, and its definition of personal information. However, the majority of the Privacy Act is closer to the previous Directive 95/46/EC than GDPR. Whilst the breadth of application of the Act is not as wide (for example, the turnover based limit on application to private sector entities), this is compensated in part by additional sector and state specific laws. There are also subject specific laws in areas that mirror equivalent laws in the EU (e.g. on electronic marketing). Whilst the Privacy Act does create some data subject rights, these are not as comprehensive as those under the GDPR. Further, there is no fundamental or constitutional right to privacy or data protection (equivalent to rights under the EU Charter and the European Convention on Human Rights).	3
	INDIA : Although the PDP Bill has been introduced, it has been delayed due to Covid-19 and has not come into law yet. As such, there is no equivalent legislative instrument governing data protection, (other than what is contained in the Privacy Rules), and there is no specific regulatory authority in charge of enforcement. However, the right to privacy is recognized by the Indian constitution, offering some alignment with the 'constitutional rights to privacy and data protection under the Charter and the ECHR.	4

## 2.2 Regulation of public authority access to private data

4

The extent to which the **level of access legally permitted and conducted in practice by public authorities to personal data** (e.g., to secure disclosure of, or conduct surveillance on, private information for national security purposes or other reasons) is subject to safeguards equivalent to that within the EEA/UK. This will consider specifically whether the right of public authorities to access data is:

- (i) underpinned by a legal framework that is publicly available and sufficiently clear (conducted 'in accordance with law'),
- (ii) carried out in pursuit of legitimate aims which are necessary in a democratic society ('proportionate') (noting that proportionality involves balancing any interference with fundamental privacy rights with what are necessary and important public interests), and
- (iii) subject to adequate and effective oversight from courts or other independent authorities

The assessment will consider both **pervasive surveillance activity** (across the destination country as a whole) and whether access can in practice be exercised by public authorities in light of legislation, legal powers, technical, financial and human resources at their disposal and of reported precedents.

- ☐ 1 - high level of safeguards in place, essentially equivalent to the level available in the EU
- ☐ 2 - high level of safeguards in place, but below the level of those available in the EU
- ☐ 3 - some safeguards in place, but materially below the level of those available in the EU
- ☒ 4 - very limited safeguards in place, significantly below the level of those available in the EU
- ☐ 5 - no safeguards in place

Complete  
Country  
Analysis 2.2

Hide Analysis

Please add any further comments in the box →	Country Analysis	Score
	UNITED STATES OF AMERICA (USA) : Some areas of US surveillance law have an identifiable and clearly constrained basis in law (e.g., the regimes that operate within the US under FISA, since Section 702 is limited to electronic communication service providers, and a Section 215 search is conducted on tangible things and ordered by a judge on the basis of specific 'selection terms'). However, this is not universally the case (e.g., the broad executive authority to intercept information in transit to the US under EO 12.333).	5
	AUSTRALIA : The Encryption Act is problematic for a few reasons. First, the notices issued under the Act (TCNs, TANs, TARs) are vague in terms of scope, and may therefore present challenges in terms of the 'quality of law' requirement for surveillance powers. Second, there is the possibility that notices could be used in a way that would directly undermine security an increase the likelihood of government access to transferred data (e.g. the removal of encryption).  However, it is notable that the use of TANs or TCNs appears, in practice, to have been limited to date.  More broadly, the Telecommunications Act does create a legal framework for law enforcement and intelligence agency interception of communications and access to communications data. This framework includes privacy protective controls in a number of areas (for example, application of powers to limited defined agencies). However, these controls could be more robust in some areas (for example, certain powers under the Act are warrantless, creating a potential issue with the 'subject to judicial oversight' requirement).  It is notable that the Privacy Act regime extends (with exemptions / limitations) to law enforcement, in a manner which broadly parallels the Law Enforcement Directive approach in the EU.  However, along with the UK and the US, Australia participates in the 'five eyes' intelligence alliance, the details of which (as revealed in a number of public leaks), has created some degree of uncertainty about the proportionality of Australian surveillance activities	4
	INDIA : The IT Act provides various grounds for interception and surveillance in India, including for surveillance of metadata. The grounds are broad and include 'for the investigation of any offence'. Many official bodies (both central and state agencies) have been granted surveillance rights across a wide range of sectors.	4

## 2.3 Regulatory supervision

3

The extent to which courts, regulators and/or supervisory authorities enforce the rule of law and/or rights guaranteed in relation to the protection of data in an independent and effective manner, with evidence of meaningful resources and enforcement activity.

- ☐ 1 - high level of safeguards in place, essentially equivalent to the level available in the EU
- ☐ 2 - high level of safeguards in place, but below the level of those available in the EU
- ☒ 3 - some safeguards in place, but materially below the level of those available in the EU
- ☐ 4 - very limited safeguards in place, significantly below the level of those available in the EU
- ☐ 5 - no safeguards in place

Complete  
Country  
Analysis 2.3

Show Description +

Please add any further comments in the box →	Country Analysis	Score
	UNITED STATES OF AMERICA (USA) : In the limited areas where the US extends data privacy protections, there is evidence of active enforcement and often significant fines. In the surveillance context, judicial oversight (through the FISC) is applied to Section 702. However, the CJEU was critical of the high-level nature of this oversight, given that it operates at the level of approving an overall surveillance program (and not individual requests for communications data). There is no judicial oversight of the broad executive authority to intercept information in transit to the US under EO 12.333.	3
	AUSTRALIA : The Commissioner appears to be an independent regulator, with a broad range of powers essentially equivalent to those of an EU supervisory authority. The total extent of its powers (including in respect of its ability to penalize infringements via fines) may not be as robust as for an EU authority, although this is to some extent mitigated by the parallel activity of the ACCC. However, the Commissioner is relatively inactive and the value of fines issued to date are low.	3
	INDIA : There is not yet a specific supervisory authority in India which governs the enforcement of data protection laws, and this does not align with regulatory supervision in the EU. In relation to surveillance, individuals can approach the high courts if they suspect they have been subject to illegal surveillance.	4

## 2.4 Rights of redress

4

The extent to which individuals can easily and effectively enforce rights and seek redress by raising complaints, claims and / or appeal and enforce decisions in relation to both data protection infringements and public disclosure / surveillance activity through judicial and/or administrative processes (e.g. help from local data protection authorities) including whether redress mechanisms can be effectively applied in practice and are not thwarted by local laws and/or practices. This section will also consider whether data subjects can secure 'self-help remedies' – e.g. right to secure access to or require erasure of personal data files, and whether the breach of local laws can be effectively invoked and relied on by individuals.

- ☐ 1 - high level of safeguards in place, essentially equivalent to the level available in the EU
- ☐ 2 - high level of safeguards in place, but below the level of those available in the EU
- ☐ 3 - some safeguards in place, but materially below the level of those available in the EU
- ☒ 4 - very limited safeguards in place, significantly below the level of those available in the EU
- ☐ 5 - no safeguards in place

Complete  
Country  
Analysis

Show Description +

Please add any further comments in the box →	Country Analysis	Score
	UNITED STATES OF AMERICA (USA) : The US system generally does not include rights for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data. Accordingly, aside from specific sectors or state laws (such as CCPA), data protection laws equivalent to the GDPR or the Law Enforcement Directive do not exist in the US to give data subjects fundamental rights to access, erase or amend their data, and to have these rights enforced in court.  The rights to bring a claim that do exist are rights to file a civil suit in respect of actual harm suffered. There is a disparity here between the European understanding of effective rights and remedies for data protection infringements—which includes not just a right to compensation for material or non-material damage, but also must include effective rights to access, amend or erase data—and the US understanding of civil lawsuits, in which actual (i.e. material) harm must be established. Significantly, it is generally accepted that the protection of the Fourth Amendment (which guarantees a right of privacy which must be respected by the US government) can only be invoked by US citizens.	4
	AUSTRALIA : The individual right of complaint under the Privacy Act provides for a clear mechanism of redress, and (as in the EU) the Commissioner can take account of both material and non-material damage. However, as a mechanism of redress, the right of complaint is not as direct as the statutory right to compensation regime that exists under the GDPR. Ultimately a complaint may lead to compensation, but the route is not as direct and applications may be required to enforce a determination made by the Commissioner.  As noted above, whilst data subject rights exist under Australian law, these are limited and not as extensive as in the EU.	3
	INDIA : Individuals in India do not have rights to pursue legal remedies in order to have access to personal data relating to them, or to obtain the rectification or erasure of such data. Currently, data protection laws equivalent to the GDPR or the Law Enforcement Directive do not exist in India to give data subjects rights to access, erase, amend etc. their data, and to have these rights enforced in court.  Therefore there are limited rights of redress compared to the standards afforded by the GDPR. Note however that individuals may enforce their fundamental rights against the state, however enforcing their rights (including the right to privacy) against a private entity may require judicial intervention.	4

## 2.5 International treaties

3

The extent to which the receiving countries have concluded international treaties and related commitments on handling of personal data to support the safeguarding of data—this will include consideration of the existence of both:

- (i) international treaties that relate to the protection of data generally consistent with principles enshrined in EEA/UK law, and
- (ii) any specific arrangements concluded to provide safeguards in relation to country to country transfers (e.g. UK/US Bilateral Data Access Agreement which brings into effect the 'quashing' provisions of 18 USC § 2703(h)(2))

- ☐ 1 - high level of safeguards in place, essentially equivalent to the level available in the EU
- ☐ 2 - high level of safeguards in place, but below the level of those available in the EU
- ☒ 3 - some safeguards in place, but materially below the level of those available in the EU
- ☐ 4 - very limited safeguards in place, significantly below the level of those available in the EU
- ☐ 5 - no safeguards in place

Complete  
Country  
Analysis 2.5

Show Description +

Country Analysis	Score
------------------	-------

Please add any further comments in the box  
→

UNITED STATES OF AMERICA (USA) : The US has limited commitments in this area and appears to clearly fall short of equivalence with the EEA.	4
AUSTRALIA : There are no international treaties comparable to Convention 108+ to note. However, the OAIC's participation in the APEC Privacy Framework and the Cross-border Privacy Enforcement Arrangement does provide for some degree of additional protection.	3
INDIA : There are no international treaties comparable to Convention 108+ to note. However, the ratification of the Universal Declaration of Human Rights does provide for some degree of additional protection.	3

### Step 3. Consider contractual, organizational or technical supplemental measures to safeguard the data

At this Step, assess the extent to which any additional safeguards adopted by the parties provide meaningful protection to the personal data and mitigate any of the risks exposed in Step 2. This stage will consider three criteria:

#### 3.1 Contractual

2

Whether the parties have agreed additional contractual commitments, including commitments contained within the data transfer tool in place (e.g. within the SCCs – whether legacy or new - or the BCRs), commitments in line with those contained in the EDPB Recommendations, which enhance (or in any way undermine) the guarantees offered in the SCCs and/or mitigate the risk posed by shortfalls within the destination country legal regime – examples may include:

(i) a process to be applied when there is a subpoena / legal process requiring the importer to challenge or demand individual review of an order to the extent possible;

(ii) an obligation to inform the exporter of the subpoena / legal process in a manner whereby the exporter can suspend the transfer / withdraw the data before a disclosure is made (to the extent not prohibited by law, e.g. an anti-tipping off law);

(iii) an obligation to routinely report to the exporter that there have been no disclosure requests made by authorities in the preceding period (warrant canary);

- ☐ additional safeguards in place which provide a high level of additional protections to the personal data
- ☒ additional safeguards in place which provide a limited level of additional protections to the personal data
- ☐ no additional safeguards in place
- ☐ measures adopted exacerbate the risk to personal data (eg contractual clauses which expressly permit standing disclosure to authorities)

(iv) requiring or requesting the requesting authority – to the extent permissible by law – to use a MLAT process;

(v) reinforcing the data exporter's right to conduct audits or inspections of the data processing facilities of the importer, on-site and/or remotely, to verify if data was disclosed to public authorities and under which conditions;

(vi) requiring the data importer to certify that: (1) it has not purposefully created backdoors or similar programming that could be used to access the systems used for the processing and/or any personal data; (2) it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems; and (3) that national law or government policy does not require the data importer to create or maintain backdoors or to facilitate access to personal data or systems or to be in possession or to hand over the encryption keys;

(vii) an obligation to provide compensation to data subjects for any material and non-material damage suffered in circumstances where the data importer disclosed personal data transferred in violation of the commitments contained under the chosen transfer tool.

Similarly where there are unhelpful contractual provisions, this would have a negative effect on the score.

Please add any further comments in the box  
→

**Implementation of transfer mechanisms:** Both the adequacy decisions and the SCCs are legal safeguards to ensure that International Transfers are afforded essentially equivalent protection, when personal data is transferred outside the EU/EEA.

The SCCs by their nature contractually obligate both the data exporter and the data importer to a range of onerous obligations, granting a number of rights and redress options for data subjects. As outlined above, ServiceNow relies on SCCs for its International Transfers – these are incorporated into the contractual arrangements.

**Jurisdiction Analysis:** The data importer continuously monitor the destination countries (where the Affiliates are located) for latest legislative changes, to assess the respect for data protection required by European law and the ServiceNow global standards for processing customer data. The data importer analyzes countries according to the level of safeguards in place and whether they are essentially equivalent to that of the EU.

The data importer's analysis of applicable laws with its Outside Counsel takes into account our current operational structure, the circumstances of the limited International Transfers, and numerous legal, technical and organizational safeguards. The data importer assesses the legal regime that applies to the data within the destination country to consider the extent to which: (1) legally enforceable protections are available in that jurisdiction to safeguard such data; (2) those protections are essentially equivalent to those offered within the EU; and (3) the guarantees provided for in the relevant transfer terms (SCCs) can be satisfied.

#### 3.2 Organisational measures

2

The extent to which:

- **organisational safeguards applied contribute to ensuring consistency in the protection of personal data** or which otherwise provide additional protective measures for data subjects, including those contained in the EDPB Recommendations on supplementary measures, for example:

- (i) adoption of internal policies with clear allocation of responsibilities for data transfers, reporting channels and standard operating procedures for cases of formal or informal requests;
- (ii) training procedures for personnel in charge of managing requests for access to personal data from public authorities;
- (iii) operating procedures to control public authority access requests to data, supported by a transparent disclosure request policy;
- (iv) access controls and confidentiality policies in place which are monitored with audits and enforced through disciplinary measures;
- (v) data security and data privacy policies, based on EU certification, self-regulatory schemes or codes of conduct or international standards such as ISO norms and best practices such as those published by ENISA

Note that where the safeguards act to facilitate disclosure (e.g. a policy to disclose without a court order, a policy to permit unfettered access to stored data, etc.) this would have a negative effect on the score.

- ☐ additional safeguards in place which provide a high level of additional protections to the personal data
- ☒ additional safeguards in place which provide a limited level of additional protections to the personal data
- ☐ no additional safeguards in place
- ☐ measures adopted exacerbate the risk to personal data (eg operating procedures which expressly permit standing disclosure to authorities)

Please add any further comments in the box  
→

**1. Third party requests:** ServiceNow respects the laws of the global jurisdictions in which it operates, as well as the privacy and security rights of its customers and the individuals whose data may be processed by our customers.

**2. Strong affiliate relationships:** The nature of the relationship between ServiceNow Affiliates means that there is a high level of communication and a cohesive approach to the protection of customer data. This is expressed, for example, through the ServiceNow Intra-Group Data Transfer and Processing Agreement (which incorporates the SCCs), which the ServiceNow Affiliates have concluded with each other.

**3. Data Agnostic:** ServiceNow processes customer data for the purpose of fulfilling the customer contract. The ultimate purpose of processing is determined by the customer. ServiceNow is data agnostic as to the data the customer uploads to the customer instance. Customers decide what, if any, personal data to upload to their instance.

**4. Binding Corporate Rules:** As of July 2021, ServiceNow is in the final stages of its application for Binding Corporate Rules (a mechanism for transferring data internationally within the ServiceNow group) with the relevant EU Supervisory Authorities, and expects the successful conclusion of that process in 2021.

**5. Third Parties:** ServiceNow does not outsource any service, operational, or management functions that would provide any third party with access to systems hosting customer data or to customer data itself. ServiceNow limits the infrastructure supporting its cloud's footprint to only those technologies, infrastructure, and components required to support the Now Platform.

#### 3.3 Technical measures

2

The extent to which:

- **privacy enhancing controls have been adopted** by the parties to mitigate risk, for example by seeking to anonymise or pseudonymise the personal data (e.g. where the sole means of re-identification are held only by the data exporter outside the destination country and outside the reach of the laws of the destination country), and / or otherwise preventing the importer from being able to disclose the personal data, such as encryption keys being kept only by the data exporter in another jurisdiction (bearing in mind that any form of root / admin access that may circumvent such measures / controls would likely render this variable as ineffective in terms of mitigation);

Similarly where the measures act to facilitate disclosure (e.g. a policy to disclose without a court order, a policy to permit unfettered access to stored data, etc.) this would have a negative effect on the score

- ☐ additional safeguards in place which provide a high level of additional protections to the personal data (e.g. encryption kept stored out of jurisdiction or (pseudonymisation in a manner where the sole means of re-identification are held only by the data exporter outside the destination country and outside the reach of the laws of the destination country)
- ☒ additional safeguards in place which provide a limited level of additional protections to the personal data
- ☐ no additional safeguards in place
- ☐ measures adopted exacerbate the risk to personal data (eg State-owned network infrastructure which can be exploited for investigation by authorities or policy implemented to automatically fulfil government information requests)

Please add any further comments in the box  
→

**1. Security:** ServiceNow's security framework is based on ISO/IEC 27002:2013. As an ISO/IEC 27001 certified organization there is a high level of integration between the ISO/IEC 27002:2013 code of practice and the ServiceNow Information Security Management System (ISMS). ServiceNow has been an ISO 27001 certified organization since 2012 and is also ISO/IEC 27017:2015 and 27018:2019 certified. ServiceNow is also ISO/IEC 27701:2019 Privacy Information Management System (PIMS) certified. ServiceNow's security program is expressed in its ISMS which is formally documented by means of an extensive library of standards, policies and procedures and other relevant documentation and guidance.

**2. Data Centres:** ServiceNow hosts its private cloud in colocation spaces within global data centres arranged in high-availability pairs which attained SSAE 18 Type 2 attestation or have ISO 27001 certifications (or equivalent). Data centres procured by ServiceNow are provided by specialist colocation data centre operators that deliver a secure and reliable space to operate in. The data centres are highly secure facilities with 24 hour, 7 days a week, 365 days a year security guards, CCTV, multiple levels of entry controls, and strict procedures for physically entering the facility.

**3. Encryption:** ServiceNow provides its customers with a variety of data encryption options that they can choose to deploy depending on the context of the data that they upload and their use of ServiceNow products:

a. Platform Encryption

b. Edge Encryption

c. Database Encryption

d. Full Disk Encryption

**4. Logical Architecture:** ServiceNow's Customers benefit from multiple layers of robust separation, rather than a single logical control point. The logical architecture of the ServiceNow application is a three-tier model as follows:

- Proxy Layer
- Application Layer
- Database Layer

ServiceNow's Logical Architecture is designed to ensure that data is protected at all times, even in the event of a security incident.



**3. Tenant Architecture:** ServiceNow (or the now platform) instances are delivered in a highly secure manner from the moment they are first provisioned; ServiceNow's architecture provides the template for the ServiceNow private cloud on which the Now Platform is deployed as a subscription service. This cloud is deployed on a highly standardized, redundant, and managed environment. From pre-built racks through to supporting services, such as networking and other logical infrastructure supporting a defence in-depth model, ServiceNow's cloud exclusively hosts instances of the Now Platform. Fundamentally each instance is dedicated to a single customer and accessible only by that customer. Additionally, the multi-instance single tenant architecture and ServiceNow cloud infrastructure means that there are several underlying security controls built into the foundations of all processes:

- Isolation
- Region Specific
- Layered Authentication
- Transport Authentication
- Standard Mitigations
- Managed Processes
- Monitoring
- Security by Design

Each ServiceNow instance records a unique compliance score as a percentage of completeness against a best practice set of configuration properties and other settings. This score is maintained on the Instance Security Dashboard (ISD), available free of charge on every ServiceNow instance. Customers can use the dashboard to obtain more information on these settings, or to make changes to them.

**6. Security by Default:** ServiceNow employs automation extensively when configuring new hardware, operating systems, and software, and in ensuring they remain in accordance with the relevant configuration and security baseline on an ongoing basis. This ensures a consistent and conformant global infrastructure and software services configuration footprint, aiding management, support and troubleshooting. The principle of least privilege is applied and systems are configured with the minimal capabilities necessary for them to function in accordance with their purpose, meaning that software services, physical and software ports and other elements are kept to only those that are absolutely required.

**7. Access to Customer Data:** ServiceNow only processes customer data in line with customer contracts. ServiceNow personnel do not process customer data within their ServiceNow instances except where necessary for the purposes of providing customer support and/or systems maintenance. Customer data may be accessed during customer support activity performed on their behalf – either directly, in the course of addressing an issue related to that data – or incidentally, whilst resolving an unrelated matter such as infrastructure configuration. This type of processing is done using ServiceNow's global network of positions, technology and employees to provide our services. When it comes to infrastructure level processing on the Now Platform, upgrades, patching, and restoration from backup are examples of tasks where automation is also extensively leveraged, with no human intervention, using our global network of Affiliates.

**8. Logical access to the infrastructure hosting:** The ServiceNow cloud and all hosted customer data access is provided on a per-role basis, in accordance with specific job functions and a least privilege model, and is reviewed regularly, in accordance with separation-of-duties good practice. ServiceNow personnel with physical access to data centres do not have logical access to data environments, and staff with logical access to data do not have physical access to data centres. The private cloud environment is both physically and logically isolated from ServiceNow's corporate environment. Access takes place from managed secured virtualized jump hosts from which employees cannot extract or copy data. Access occurs on a case-by-case basis and is strictly controlled, with activity being logged and monitored by a separate security team. Customer data accessed incidentally during support activities is not processed outside what is permitted contractually or under relevant statutory obligations, such as the General Data Protection Regulation.

**9. Access Control Plug In and the High Security Plug In:** These options can be used by Customers to limit or restrict ServiceNow access to customer data.

Please refer to the attached descriptions provided by ServiceNow defining the requirements and technical measures.

#### Step 4. Taking account of the specific circumstances of the transfer, consider the risk of harm to which a data subject may be exposed

In this Step we will consider the potential risk of harm that may be caused to a data subject as a consequence of their data being transferred to the destination country, **taking into account the circumstances of the transfer identified in Step 1, and the level of protection provided for in the safeguards as identified in Steps 2 and 3, and considering any potential shortfall thereof** and other real-life variables. This element of the assessment is important to help place context to the relative risks posed to the data subject given the particularities of the data transfer and whether (in practice) there is a meaningful risk to the safeguards provided to the data subject in the EEA / UK being undermined due to these transfers.

In order to perform this assessment please take into consideration any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred, if applicable.

This part of the assessment will consider two factors:

##### 4.1 Severity of harm

1

The **potential severity of harm that could occur to the data subject** taking into consideration relevant factors identified in Step 1, such as the nature of the data / data subject and the identified shortfalls in Steps 2 and 3, including the likely distress an individual might suffer due to the loss of privacy in the data, possible sanction faced as a result of processing, such as capital or corporal punishment, length and severity of custodial sentence, size of financial penalty, imposition of financial sanctions, etc., with a score assigned depending on the perceived severity of the risks.

- ☒ low severity of harm
- ☐ medium severity of harm
- ☐ high severity of harm

Please add any further comments in the box  
→

Taking into account the specific circumstances of the transfer such as the nature of the data transferred (pertaining to service tickets), the purpose of the processing, and considering the above mentioned technical and organizational safeguard measures applied to the processing, the magnitude of potential adverse effects, including material and non-material effects and impacts of data processing on the fundamental rights and freedoms, is decreased.

##### 4.2 Likelihood of harm

1

The **likelihood / probability of harm arising to the data subject**, given the circumstances in which the transfer is made and in light of the third country law and practices. This will take into consideration relevant factors identified in Step 1, such as the nature of the data / data subject and its interest to law enforcement / security establishment, and further elements such as:

- the **likelihood that law enforcement / security establishment would request the personal data** from the importer or a processor / sub-processor rather than from the exporter directly;
- **whether the data importer will (to the extent the law permits it) successfully exercise any rights it has to challenge the order for disclosure** issued by law enforcement / security establishment (by legal means or otherwise) causing such authorities to give up their requests for the data in plain text;
- the **probability that employees of the data importer, or subsequent recipients (subcontractors, affiliates/subsidiaries) technically have access to personal data in plain text** outside the envisaged scenarios (e.g. beyond maintenance purposes using admin privileges) or are able to obtain such access (e.g. by installing a backdoor or similar programming to access the system and/or personal data);
- **elements demonstrating that a third country authority will seek to access the data** with or without the data importer's knowledge, in light of reported precedents, legislation and practice; for example, in the U.S., requests for access to data under Section 702 of FISA are targeted at 'electronic communication service providers'. This term encompasses (i) telecommunications carriers; (ii) providers of electronic communication services (e.g. a provider of internet based messaging services); and (iii) providers of remote computing services (i.e. cloud computing providers). Accordingly, FISA does not apply to all recipients of personal data in the U.S.;
- **elements demonstrating that a third country authority will be able to access the data** – at rest, or in transit – through the data importer or through direct interception of the communication channel in light of reported precedents, legal powers, and technical, financial, and human resources at its disposal; and
- **elements demonstrating that the envisaged technical measures are effective** in the specific countries involved in the transfer (e.g. import of encrypted data is permitted in the data importer's country and state of the art encryption techniques are used which can be considered robust against cryptanalytic/active and passive attacks with resources known to be available to the public authorities).

- ☒ low probability of harm
- ☐ medium probability of harm
- ☐ high probability of harm

Please add any further comments in the box  
→

Taking into consideration the absence of available relevant practical experience up to the date of this assessment indicating the absence of prior instances of requests for disclosure from public authorities received by the data importer for the type of data transferred and considering the above mentioned technical and organizational safeguard measures applied to the processing, the threat occurrence probability is decreased, but still relevant.

Particularly taking into account that data is not stored (in rest) at the data importer's location and hence only at risk when in transit (or if someone gets access to the data importer's access credentials), the likelihood is deemed to be low.

#### Step 5. Final Decision

Summary of Step 1	
Data exporter location	Denmark,
Data importer location	ServiceNow Inc. - United States of America (USA), ServiceNow UK Ltd. - United Kingdom (UK), ServiceNow Australia Pty Ltd - Australia, ServiceNow Software Development India Private Limited - India, ServiceNow Japan G.K. - Japan
Full name of the data exporter	Kamstrup A/S
Sector in which the data exporter operates	Manufacturer of system solutions for smart energy and water metering
Privacy role of the data exporter	Data Processor to its customers
Full name of the data importer	ServiceNow Group entities
Sector in which the data importer operates	Delivery of business-to-business digital workflow solutions.
Privacy role of the data importer	Sub-processor
Relationship between the data exporter and data importer	The data importer is a market leading service provider.
Purposes for which the data importer intends to process the data	The personal data is transferred to the data importer in order to utilize the workflow solutions offered and will be accessed remotely by non-EU ServiceNow Affiliates for the delivery of the ServiceNow offering, namely supporting a ticket handling system
Categories of personal data involved in the transfer	Identification data (name, address, telephone, ...) - Electronic identification data (e-mail, IP-addresses, cookies, ...) - Personal characteristics (age, gender, civil status, ...) - Family & household (spouse, children, ...) - Electronic location data (GPS position, ...) - Consumption habits - The ServiceNow solution offer a free-text solution and the data exporter may decide to submit personal data at its own discretion as needed to fulfill the purpose of the contract. - Housing characteristics (house type, ...)

Categories of data subjects whose personal data are involved in the transfer	Clients - Employees and collaborators - The personal data transferred will primarily relate to the end-users of the Kamstrup meters (the customers of the data controller). Personal data on employees within the data exporters organisation may be transferred.
Data Format	Data will be remotely accessed by non-EU ServiceNow Affiliates.
Envisaged transfer tool	EU SCCs Controller to Controller (Commission Decision (EC) 2004/615) or Controller to Processor SCCs (Commission Decision (EC) 2010/87)
Applicable laws and practices specific to the transfer	N/A
Data storage and limitation of access	<p>The data importer will access the personal from the jurisdictions specified in section 1.1. Personal data will be stored at the ServiceNow datacentres in Amsterdam (EU/EEA-region) and the non-EU ServiceNow entities will access the personal data in order to provide the agreed services.</p> <p>The data importer will have wide access to the IT systems of the data exporter for the purpose of its tasks. The data importer will, however, be restricted access to IT systems not necessary for its tasks.</p>

## Summary of Steps 2, 3 and 4 risk score

Consider the adequacy of the legal regime in the destination country	18
Consider supplemental measures that may available to safeguard the data	0,38
Consider the risk of harm to which a data subject may be exposed	0,75

Total risk score	<b>5,18</b>	The residual risk is likely to be low. You may decide to proceed with the transfer given the safeguards that are in place, but ensure the supplementary measures which have been adopted are maintained at all times.
------------------	-------------	---

Final Risk Score analysis

# Data Encryption

Encryption technologies for  
data protection on the Now  
Platform



## Introduction

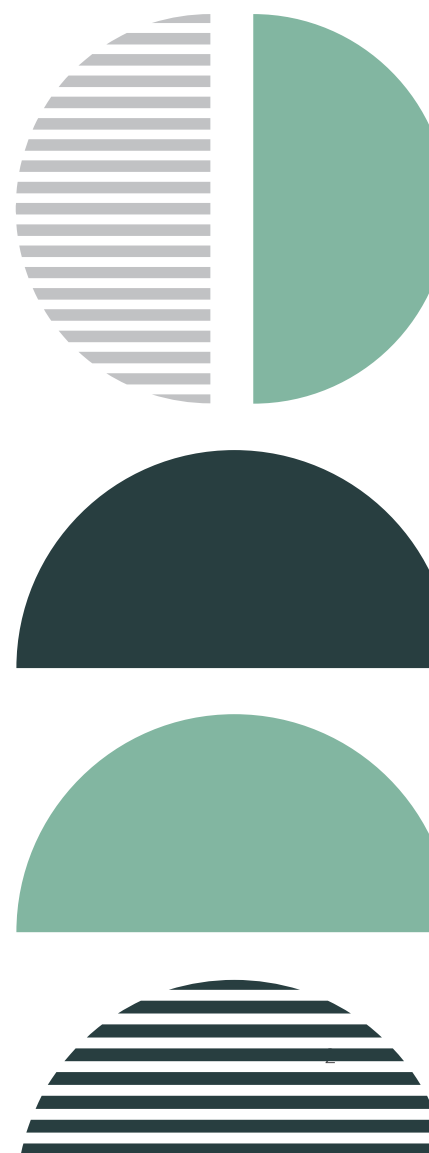
ServiceNow provides robust data security and privacy capabilities to protect its customers data. However, in today's environment there is no single encryption solution to address all data protection needs. Therefore, in order to meet the data security requirements of modern enterprises, ServiceNow provides customers with a suite of encryption options. These can be used individually or in conjunction with each other to address a variety of data confidentiality use cases:

- Column Level Encryption Enterprise is applied to data as it is added to an instance within the ServiceNow network
- Edge Encryption encrypts data before it leaves your network, ensuring that neither ServiceNow personnel nor an attacker would be able to read your data
- Database Encryption encrypts data directly in the database accessed by applications running on a ServiceNow instance
- Full Disk Encryption works at the hardware tier and ensures data is encrypted at rest, protecting against a storage attack

While each approach is different in terms of implementation, benefits, and functionality, you are not limited in choosing one approach over another; you can choose a combination based on your security needs.

This document explains these solutions and provides the information you need to choose the correct ones. For an overview of the ServiceNow security program, please refer to the [Securing the Now Platform](#) eBook.

**Please note, all information in this eBook is related to the standard Now Platform commercial environment.** For information related to ServiceNow's in-country cloud offerings around the globe and how they may differ, please contact your ServiceNow account representative.



# Table of Contents

Introduction ..... 2

Managing encryption keys..... 4

Encryption key management overview ..... 4

**Encryption in transit..... 5**

Summary of ServiceNow encryption in transit features..... 5

Secure communication with the instance ..... 6

Email in-transit encryption ..... 6

File transfer encryption ..... 6

Direct database query ..... 6

Web services integration..... 6

Single sign-on integrations ..... 7

ServiceNow MID server..... 7

**Encryption at rest..... 8**

Column Level Encryption Enterprise..... 8

Edge Encryption ..... 10

Edge Encryption vs Column Level Encryption Enterprise..... 12

Database Encryption ..... 13

Full Disk Encryption..... 15

**Conclusion..... 15**

**Resources ..... 16**

Appendix A: Edge Encryption Options..... 17

Appendix B: Functionality and encryption implications for Edge Encryption..... 18

Appendix C: Comparison of encryption at rest solutions..... 21



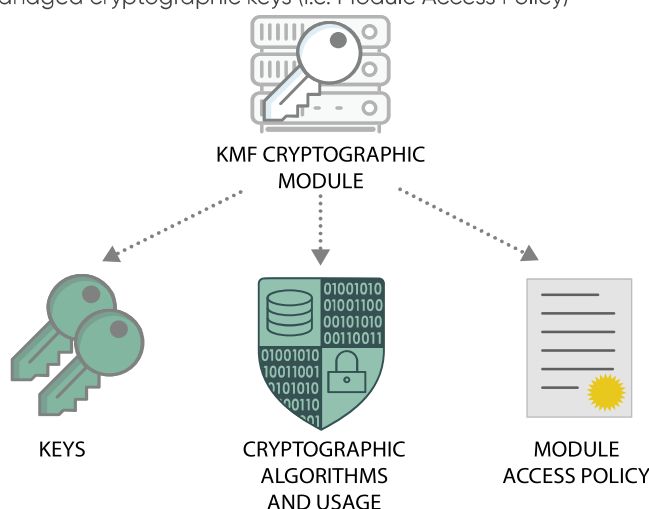
# Managing encryption keys

## Encryption key management overview

Backed by a hardware security module, the ServiceNow Key Management Framework (KMF) feature provides customers with the essential cryptographic tools to enable data security through confidentiality, integrity, and authentication.

At its core, KMF provides an interface for the following:

- Proper lifecycle management of cryptographic keys
- Configuration of the managed cryptographic keys to a specific cryptographic usage and algorithm (e.g. AES-GCM with 256-bit key for data encryption purposes)
- Access controls for the managed cryptographic keys (i.e. Module Access Policy)



KMF supports encryption on the Now Platform in the creation and management of cryptographic modules specific to each type of encryption. Encryption keys within the cryptographic modules can be created, rotated, revoked, and configured for automated lifecycle settings (e.g. automated deactivation or automated rotation).

Starting in the Quebec release, KMF is available out of the box on the Now Platform. In addition to the core functionality described above, KMF also supports other functionalities and features within the Now Platform.

## Column Level Encryption Enterprise

Encryption keys provided by customers for use with Column Level Encryption Enterprise (CLEE) are backed up within the database for the customer instance where they are used. Customers should also back up encryption keys prior to applying them to their instances. For CLEE, customer keys are re-encrypted using a wrapper key, commonly referred to as a key-encryption-key (KEK), which is stored and managed from a key management appliance.

## Edge Encryption and Database Encryption

Encryption keys for the Edge Encryption feature are managed entirely within a customer's network boundary. Encryption keys for Database Encryption are managed by ServiceNow using a three-level key hierarchy. The first two keys are customer-specific and are created by the database engine, while the third key is instance-specific.

## ServiceNow cloud infrastructure

Encryption keys used within ServiceNow's cloud infrastructure are managed by ServiceNow. Keys are stored in redundant secure key storage appliances. Dual controls are required for essential functions such as generating, deleting, or exporting keys. Key custodian forms are required as part of the generation of new keys. Cryptographic management is undertaken by a specific team within the security group, including appliances used to store the per customer instance wrapper key.

Standard operating procedures are used for the procurement, generation, and configuration of key appliances. Work instructions are used for configuration and backup with logs from these forwarded to the ServiceNow internal SIEM infrastructure.

# Encryption in transit

## Summary of ServiceNow encryption in transit features

Element	Encryption Method	Summary
Interactive end-user sessions	TLS 1.2*	Highest publicly available ratified encryption
Email	TLS 1.2* opportunistic TLS	Highest publicly available ratified encryption where mutually supported, with fallback to cleartext
File transfers	<ul style="list-style-type: none"><li>Inbound to instance via HTTPS only</li><li>Retrieved by instance, from external location: TLS 1.2* over FTPS (implicit or explicit), SFTP, SCP</li></ul>	Highest publicly available ratified encryption where mutually supported, with cleartext FTP option for legacy integration
Web services integration	TLS 1.2* supporting outbound certificate-based mutual authentication	Highest publicly available ratified encryption when initiated from ServiceNow instance, but does not currently support inbound mutual authentication
Single sign-on (SSO)	TLS 1.2*	Highest publicly available ratified encryption
MID server	TLS 1.2* plus additional application-level public key pair encryption between MID server and instance	Highest publicly available ratified encryption, with double encryption of credentials used for discovery and orchestration

\*References to TLS 1.2 include proposed TLS 1.3 suites, i.e. ECDHE-ECDSA (perfect forward secrecy)



## Secure communication with the instance

By their nature, customer instances of the Now Platform are designed to be accessible via the internet, providing maximum flexibility in how, when, and from where they are accessed. The internet, however, is a public network and therefore communications can potentially be intercepted and read if they are not encrypted or otherwise protected.

ServiceNow provides transport layer encryption as standard within its cloud infrastructure. The Now Platform enables customers to use its encryption in transit capabilities when integrating with own external systems, data sources, or services.

Customers access their instances via a web browser using Transport Layer Security (TLS) encryption using AES with 128-bit or 256-bit cipher suites. This is also true of any data transferred from the on-premises MID server to the Now Platform. All end-user access to a ServiceNow instance attempted over HTTP are redirected to HTTPS. Negotiated ciphers are subject to customer browser versions and may be influenced by customer internet proxy infrastructure. Customers can force specific cipher suites via their own browsers or proxies if desired.

For additional security, customers are also able to use IP range-based authentication to restrict the public networks that are used to access their instances of the Now Platform.

The standard contractual clauses are applicable as a data transfer mechanism, as per section 9 (international data transfers) of ServiceNow's [Data Processing Addendum](#).

## Email in-transit encryption

Customers commonly configure ServiceNow instances to generate emails in relation to service management tasks, for example, to request approval for a change or notify a user of the status of a service request. ServiceNow instances provide additional confidentiality in this respect by supporting opportunistic TLS for email sent or received. Now Platform instances will negotiate TLS 1.2 encryption during the SMTP handshake and will fall back to plaintext SMTP where a secure channel cannot be negotiated.

Additional related email security controls including Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) are also provided at no additional cost.

## File transfer encryption

Instances of the Now Platform support a variety of file transfer protocols, including FTPS, SFTP, and SCP. These are for instance- initiated communication out to external systems only and support TLS 1.2. There is no inbound file transfer facility beyond HTTPS/ web services uploads.

## Direct database query

Now Platform instances support direct Java Database Connectivity (JDBC) queries out to external systems. JDBC connections are not encrypted but can be securely proxied via a customer management, instrumentation, and discovery (MID) server. The communication to the MID server in the customer environment is secured, as described in the ServiceNow MID Server section below.

## Web services integration

ServiceNow supports web services using SOAP (Simple Object Access Protocol) and REST (Representational State Transfer) for integration, all traffic is encrypted using TLS.

“

Now Platform instances will negotiate TLS 1.2 encryption during the SMTP handshake and will fall back to plaintext SMTP where a secure channel cannot be negotiated



Web service security is enforced using the combination of basic authentication challenge/response and system-level access using contextual security. Additionally, there is a set of web service-specific roles that may be granted to the web service user.

For incoming SOAP requests, support for WS-Security 1.1 in the form of WSS X.509 token profile and WSS username token profile is available. In this context, "incoming" means requests targeting a web services resource in a customer ServiceNow instance.

ServiceNow instances support outbound-only web services mutual authentication by defining a protocol profile for connections that require mutual authentication. Protocol profiles allow you to associate a specific certificate record with a protocol, such as HTTPS. Requests made to an endpoint whose domain is defined in a profile are then mutually authenticated.

Mutual web services authentication is only possible for outbound HTTPS connections, such as SOAP, REST, or direct HTTPS calls. A ServiceNow instance does not support mutual authentication for inbound requests or for outbound requests sent through a MID Server.

Secure signing of SOAP requests for message integrity purposes is also available.

## Single sign-on integrations

Instances of the Now platform support single sign-on (SSO) via the multiple provider SSO or security assertion mark-up language (SAML) 2.0 plugins. These options allow integration with your own compliant SAML 2.0 identity providers (IDPs), and benefit from transport layer encryption. Additionally, customer-provided certificates are used to verify a SAML assertion is properly signed by the correct IDP.

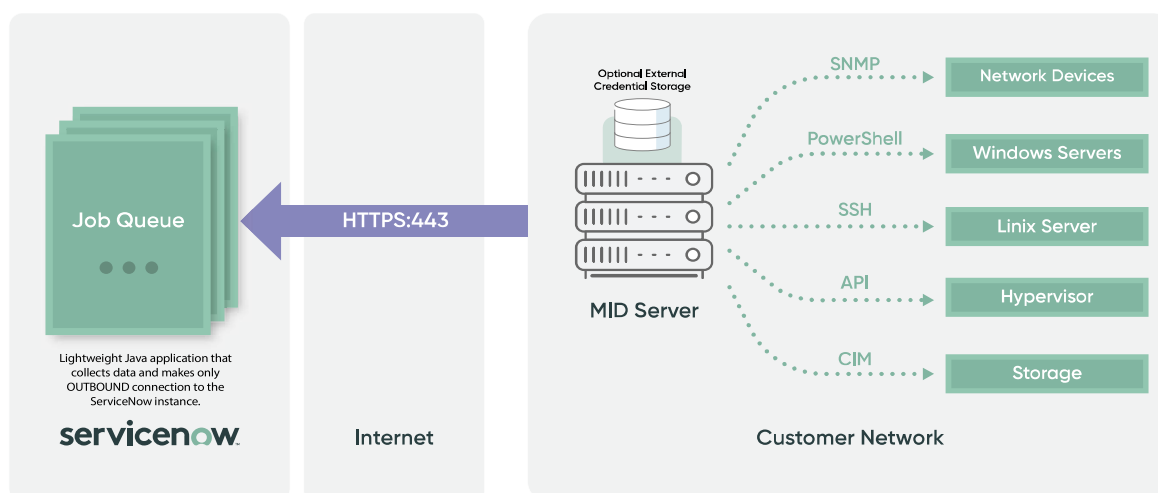
Instances of the Now Platform include LDAP client functionality and can access multiple LDAP v3 compliant directories according to customer configuration. Both standard and secure LDAP (LDAPS), which use TLS, are available.

## ServiceNow MID server

The ServiceNow management, instrumentation, and discovery (MID) Server is an optional, free ServiceNow component. It facilitates communication of data between the customer instances and external applications, data sources, and services. MID Servers are used by customers in conjunction with their instances for enterprise application and service monitoring, integration, orchestration, and discovery.

The MID Server is a Java application provided to customers via a download link within their instance. It may be installed by the customer on a suitable host system within their environment. The server can use Windows or Linux operating systems. MID Servers are cryptographically paired with an individual instance during installation and need to be approved by the customers ServiceNow administrators before they can be used.

At a customer defined interval, a MID server securely initiates an outbound session to a customer's instance over HTTPS using TLS 1.2, looking for activities to perform. The activity is retrieved and executed, and any output or resulting data is returned to the originating instance. This outbound, or 'pull' approach negates the need to permit inbound access through a customer's perimeter or firewalls directly to the Internet.



# Encryption at rest

## Column Level Encryption Enterprise

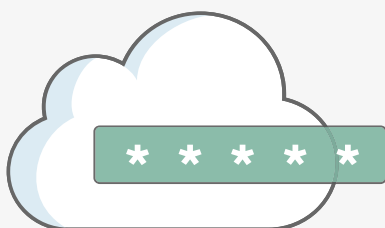
Column Level Encryption Enterprise (CLEE) provides field and attachment-based data encryption within instances of the Now Platform. With CLEE, users can configure which specific data to encrypt within a specific table. The data is then stored in encrypted form.

Encryption keys are stored and maintained within the ServiceNow instance and managed through the key management framework.

The main features of CLEE include:

- Encryption of supported field types of string, date/time, and URLs
- Can be used on file attachments
- Employs AES-CBC with 256-bit keys
- Offers both deterministic and non-deterministic encryption options
- Allows user with access to perform limited searching and filtering operations on data that has been encrypted
- Allows user to supply their own encryption keys (bring your own keys, BYOK) or have keys randomly generated on the Now Platform
- Offers several access controls based on role assignment and application scope

### Common use case



Mitigating the risk of exposing sensitive data as either the result of a direct attack or of compromised data stored in a cloud



Enabling customers to comply with governmental and industry certification requirements and regulations



Limiting access to sensitive data based on defined roles, defined script assignments, application scope and domain membership

### CLEE cryptographic module

CLEE encryption keys are managed via the key management framework (KMF), specifically through CLEE cryptographic modules, which are created by users assigned with the KMF cryptographic manager role. Once a PE cryptographic module is created, it can be associated to a field within a given table, thus enabling CLEE for the given field.

Whether generated by the ServiceNow instance or customer supplied (BYOK), the keys are stored in the same unique customer instance database where the data encrypted by them is stored. As part of the KMF, the encryption keys themselves are stored in encrypted form and are encrypted by the instance key-encryption key (IKEK), an instance-unique key generated by KeySecure. This mitigates direct access to the encryption key, either by an instance administrator or ServiceNow.

PE does not enable customers to store encryption keys in their own hardware security modules (HSM), key storage appliances, or services.

### CLEE access control

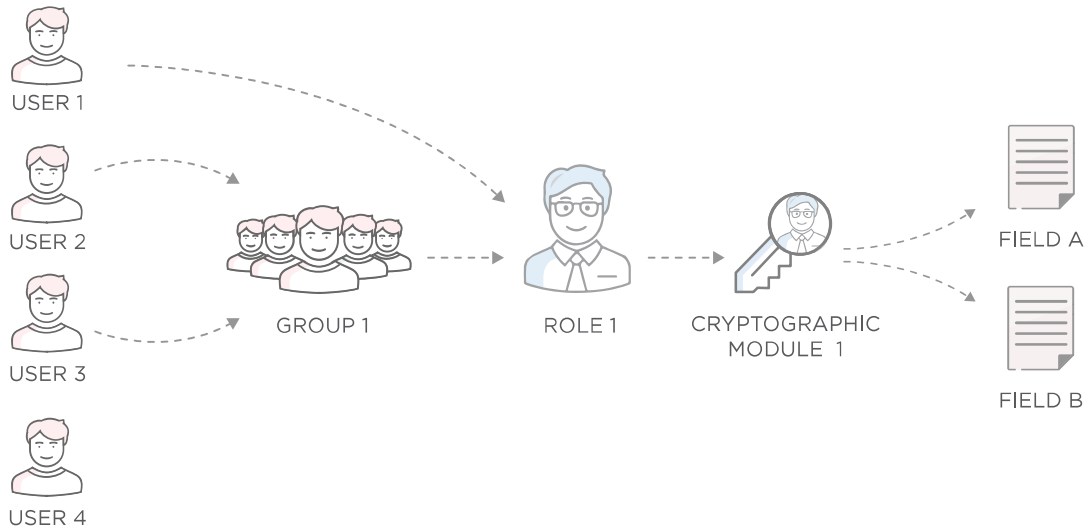
Within the CLEE cryptographic module, KMF cryptographic managers can grant access to the module based on:

- Role – access is based on the role for the user session.
- Application Scope – access is based on being in the targeted application scope.

These access controls are not mutually exclusive; multiple access controls can be configured for a CLEE cryptographic module to

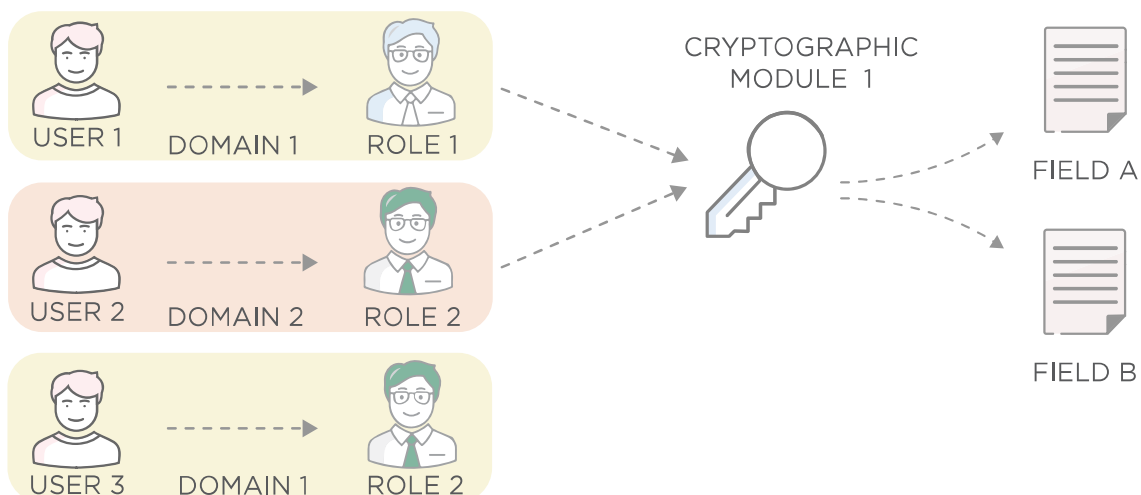
provide flexibility.

The access control example below illustrates single access control implemented (role-based):



- User 1 is a member of Role 1, which provides access to CLEE cryptographic module 1; this allows User 1 to see the contents of Field A and Field B.
- User 2 and User 3 are members of Group 1; Group 1 is a member of Role 1, which allows everyone in Group 1 access to cryptographic module 1 and allows User 2 and User 3 to see the contents of Field A and Field B.
- User 4 is not a member of any group or role and has no access to CLEE cryptographic module 1; not only does User 4 not have access to Field A or Field B, but User 4 will not even see that these fields exist.

Access control example 2 – Two access controls implemented (role-based + application scope):



- User 1 is a member of Role 1 and is currently in Domain 1. Access to CLEE Cryptographic Module 1 is granted due to an access control that allows access to Role 1. Thus, User 1 is able to see the contents of Field A and Field B. This demonstrates access based on role (similar to the previous example).
- User 2 is member of Role 2 (i.e. not a member of Role 1) and is currently in Domain 2. Access is allowed since an access control for Domain 2 exists for CLEE cryptographic module 1. As a result, User 2 is able to see the contents of Field A and Field B. This

demonstrates access based on domain membership.

- User 3 is neither a member of Role 1 nor in Domain 2. As a result, User 3 cannot see the contents of Field A and Field B. Furthermore, User 3 will not see that these fields exist.





### Usage and restrictions

Column Level Encryption Enterprise (CLEE) can be used to process specific sensitive data sets in the ServiceNow environment. The data is only decrypted by a user/script with authorized access to the associated CLEE cryptographic module. Controlling access to sensitive data often means limiting access in a controlled fashion or granting it on an as-needed basis.

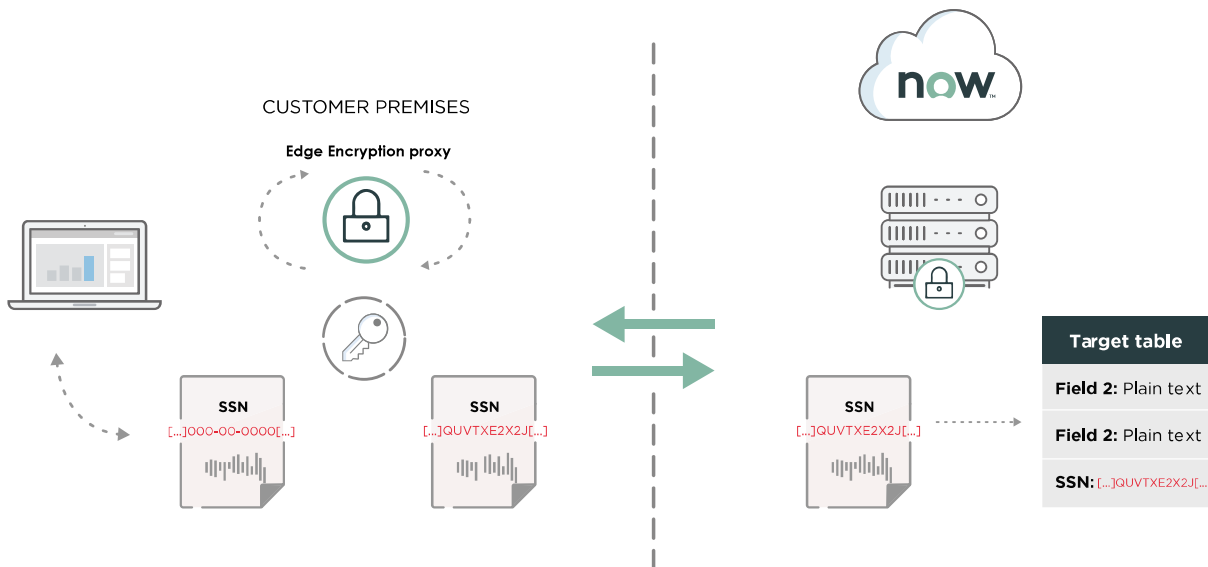
CLEE-encrypted data is maintained throughout the backup process.

## Edge Encryption

Edge Encryption provides customers the ability to control the end-to-end encryption of their data and key management. Edge Encryption uses a proxy application provided by ServiceNow and installed by customers within their own network. This tokenizes specified data patterns or encrypts string fields and attachment data before it is sent from a customers' environment to their instance. It also decrypts the same data again only within the customer's own network, using keys stored only within the customer's own network. Edge Encryption is also supported by ServiceNow.

Key features of Edge Encryption	Common use cases
<ul style="list-style-type: none"> <li>• <b>Customer-owned</b> Customer-retained encryption key administration</li> </ul>	 Requirements that prohibit encryption keys from being stored in a cloud service provider
<ul style="list-style-type: none"> <li>• <b>Flexibility</b> Flexible encryption options to balance security and user operation requirements</li> </ul>	 Mitigating the risk of exposing sensitive data as either the result of a direct attack or of compromised data stored in a cloud
<ul style="list-style-type: none"> <li>• <b>Tokenization</b> Provides pattern-specific protection for structured data, such as credit card or Social Security numbers</li> </ul>	 Customers who need to comply with governmental and industry certification requirements and regulations
<ul style="list-style-type: none"> <li>• <b>API Support</b> REST and SOAP APIs to support additional system integrations, web services, and customizations</li> </ul>	 Addressing the data sovereignty requirements for data that may be stored outside of a country's domain
<ul style="list-style-type: none"> <li>• <b>Easy administration</b> Easily administer and rotate encryption keys</li> </ul>	
<ul style="list-style-type: none"> <li>• <b>Native platform</b> Tight integration within the ServiceNow platform architecture to support ServiceNow applications and the ServiceNow portal interface</li> </ul>	
<ul style="list-style-type: none"> <li>• <b>Simple rule development</b> A native encryption rule development environment to provide integration support</li> </ul>	

The following diagram illustrates the Edge Encryption process – a field storing social security numbers (SSN) being encrypted within a customer's network by an Edge proxy. As shown below, the data in the SSN field is converted from plain text to ciphertext.



In addition to the Edge proxy configuration and management of rules, customers are responsible for the usual requirements of operating a server within their environment (including hosting, routing, backup, DNS configuration) to enable and support their Edge proxies.

Edge Encryption is rule-based; specific fields are identified for encryption or tokenization based on a customer's business requirements. Data in fields encrypted by the Edge proxy will be accessible to any end user whose roles or other access rights allow them to read or write to that field.

Access to Edge-encrypted data must always be made through the proxy application, which functions as a web application with a unique customer-defined URL. Attempting to access Edge-encrypted data directly from an Edge-enabled instance without first passing through the relevant proxy will result in only the encrypted version of the data being visible. Edge proxies are hosted by customers at their own preferred URL, such as `edgeproxy.customerdomain.com`.

The following example shows an incident record which has Edge Encryption applied to the Short Description field. This illustrates how it would appear to an appropriately credentialed user accessing that record via the customer's Edge proxy (i.e. in plain text).

≡ Number ▲	≡ Opened	≡ Short description
<u>INC0000001</u>	2018-05-07 16:09:51	Can't read email

Below is the same record and field when it is accessed directly at the customer's instance. Because this form of access bypasses the customer's Edge proxy, the data is inaccessible to any user, including administrators.

≡ Number ▲	≡ Opened	≡ Short description
<u>INC0000001</u>	2018-05-07 16:09:51	05klmji00/0vqp4ic2k00CAIQABgA00100900QUVTXzE2X2J5dGVzX2I2Xw

The relevant encryption keys and configuration exist only on the Edge proxy within the customer's network and are not visible to ServiceNow. The data is encrypted from the moment it leaves the customer environment and is only decrypted upon retrieval. At no point is the data accessible in clear text by ServiceNow systems or personnel.

### Types of encryption

Edge Encryption provides three options that support the advanced encryption standard (AES) for key lengths of 128 and 256 bits you can apply to data fields within an instance: standard, equality-preserving, and order-preserving encryption. For a side-by-side comparison of these encryption options, see [Appendix A](#).

## Tokenization

Another layer of data protection that Edge Encryption provides is tokenization. During this process, Edge Encryption uses a randomly generated token to mask a predefined pattern of characters within a data field when the pattern is matched.

The examples below illustrate tokenization from the user experience perspective.

In the first example, the patterns for a credit card and Social Security number were configured for tokenization. When the user connects through the Edge Encryption proxy, the content for those two values are displayed in plain text but are actually tokenized in the instance.

≡ Number ▼	≡ Opened	≡ Short description	≡ Caller	≡ Priority	≡ State
<a href="#">INC0010005</a>	2016-10-05 07:57:08	Please help Joe Smith (SSN: 123-45-6789) with his tax software installation.	<a href="#">ITIL User</a>	5 - Planning	New
<a href="#">INC0010004</a>	2016-10-05 07:55:31	Purchase order 89-23456 should be charged against Visa 4916 8699 9572 5861, not AMEX 377660611382710.	<a href="#">ITIL User</a>	5 - Planning	New

However, if the user were to bypass the Edge Encryption proxy and access the same incidents directly, the corresponding values within the short description field would be represented as a token as shown below.

≡ Number ▼	≡ Opened	≡ Short description	≡ Caller	≡ Priority	≡ State
<a href="#">INC0010005</a>	2016-10-05 07:57:08	Please help Joe Smith (SSN: xfu8bcng05x) with his tax software installation.	<a href="#">ITIL User</a>	5 - Planning	New
<a href="#">INC0010004</a>	2016-10-05 07:55:31	Purchase order 89-23456 should be charged against Visa x05barhg2gqq587sggx, not AMEX xzye8757w69p5vx.	<a href="#">ITIL User</a>	5 - Planning	New

## Implementation considerations

While encrypting specific fields or tokenizing embedded strings of data is beneficial from a data security perspective, having ciphertext in place of actual data can lead to potential functional or operational challenges within an instance of the Now Platform. To avoid these challenges, follow the implementation considerations and suggested capability and configuration approaches provided in detail in [Appendix B](#).

## Edge Encryption vs Column Level Encryption Enterprise

This section serves as a guide to help determine when to opt for Edge Encryption or Column Level Encryption Enterprise (CLEE).

At a high level, if an enterprise wants maximum control over the encryption of its data, Edge Encryption is the choice over CLEE. With Edge Encryption the customer owns and controls the encryption key outside of their ServiceNow instance. However, depending on your requirements, using Edge Encryption could result in reduced functionality.

CLEE can decrypt an encrypted column used in a server-side business rule when that rule is executed by a logged-in end-user assigned the appropriate encryption context. However, Edge Encryption would not have this capability since the data needs to be decrypted on the instance to run the business rule.

The table below shows a side-by-side comparison of the differences between Edge Encryption and CLEE functionality.

Functionality	Edge Encryption	Column Level Encryption Enterprise
Encryption key controlled and owned by customer	YES	NO <sup>1</sup>



Functionality	Edge Encryption	Column Level Encryption Enterprise
Multiple levels of functional encryption for equality, filtering, grouping, and sorting operations	YES	NO <sup>2</sup>
Data tokenization based on defined encryption pattern	YES	NO
Built-in encryption key rotation	YES	YES
Encryption of standard out-of-the-box fields	YES	YES
REST/SOAP API encryption support	YES	NO
Built-in mass encryption/decryption support	YES	YES <sup>3</sup>
Automatic attachment encryption	YES	NO <sup>4</sup>
Customer maintains additional infrastructure in their network to control encryption keys and encryption processing	YES	NO
Decryption by server-side business rules	NO	YES <sup>5</sup>
Encryption/decryption based on user roles	NO	YES <sup>6</sup>

**Table 1: Edge Encryption versus Column Level Encryption Enterprise**

<sup>1</sup> CLEE supports BYOK

<sup>2</sup> CLEE supports only equality filtering

<sup>3</sup> CLEE supports mass encryption with a single CLEE cryptographic module, and mass decryption with a single CLEE cryptographic module or multi CLEE cryptographic modules

<sup>4</sup> Manual process per record attachment for CLEE

<sup>5</sup> Supported only when business rules are executed by an entity assigned the appropriate access to the CLEE cryptographic module context

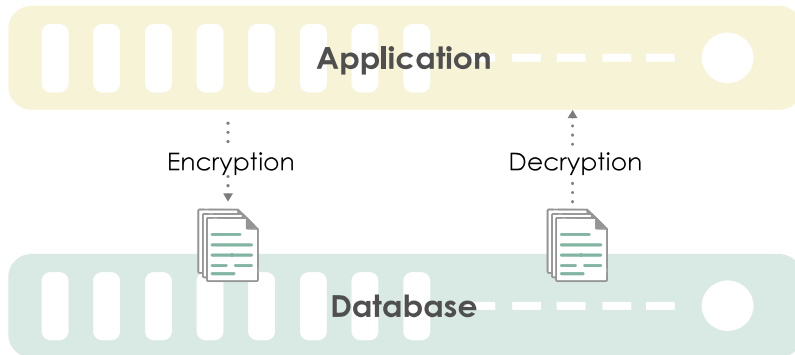
<sup>6</sup> CLEE supports access controls based on role, script, and application scope

## Database Encryption

Database Encryption enables all data to be protected with symmetric AES-256 encryption, whether the database is online or offline. It encrypts all customer data at rest in the database with no impact to functionality. Any new or changed data is encrypted as it is entered into a table – associated activity log files (e.g. bin, redo, undo, and error) are also encrypted.

When this feature is used, all related instances are encrypted – along with associated replication traffic and backups – and instance cloning is still possible. However, there is a minor performance impact for using Database Encryption of up to 5%. Both new and existing instances on supported releases of the Now Platform can take advantage of Database Encryption.

Database Encryption utilizes the native capabilities of the database engine to encrypt data as it is written to the database using industry standard AES-256 encryption and decrypt it in memory as it is read from the database. This technology (also known as Tablespace Encryption or Transparent Data Encryption) is fully transparent to the customer and to the application.



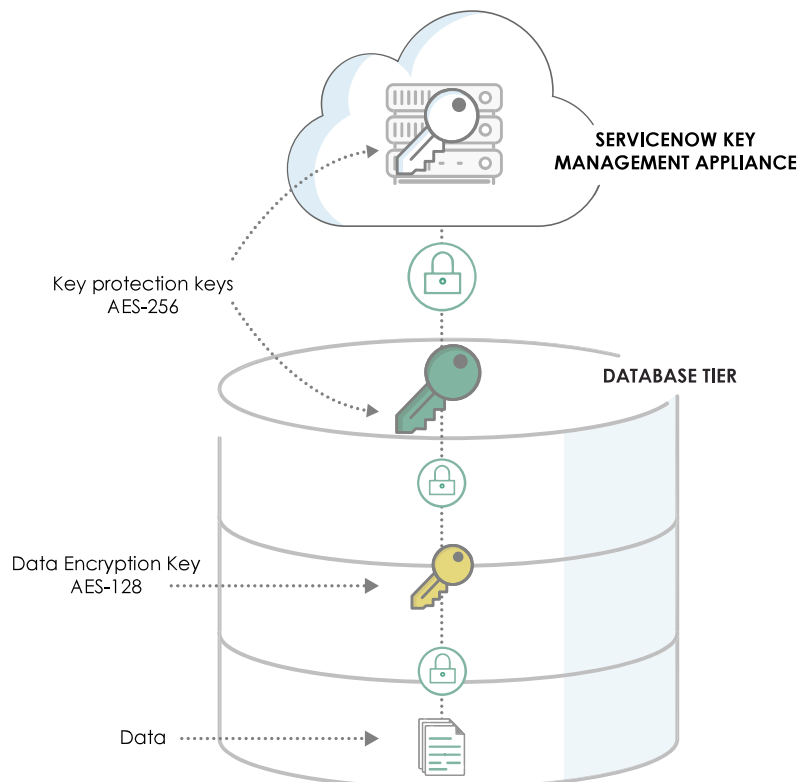
Both ServiceNow applications and custom applications can operate seamlessly without any changes because the application always has access to the data it needs, in the clear. When using Database Encryption, all data is encrypted, including attachments, logs, and backups.

#### Key Management: three-level hierarchy

Keys are stored and managed by ServiceNow using a three-level key hierarchy:

- 1st level: An AES-256 key is used to encrypt the data.
- 2nd level: Another AES-256 key is used to protect the 1st level key.
- 3rd level: An additional AES-256 key, used to protect the 2nd level key, is created by and stored within our FIPS 140-2 compliant key management appliances in the ServiceNow data centers

The first two keys are customer-specific and are created by the database engine. The third key is unique per customer instance.



“

Encrypting all data at rest provides a layer of security in cases where much of the data in your environment is considered sensitive or could potentially be considered sensitive in the future



## Common use cases

Encrypting all data at rest provides a layer of security in cases where much of the data in the customer environment is considered sensitive or could potentially be considered sensitive in the future, due to regulations or changes in the customer's business environment. Database Encryption is useful in cases where it is critical that functionality is not impacted, and application tier encryption is not necessary.

Database Encryption can be coupled with application tier encryption for a layered security approach. Highly sensitive fields that need to be encrypted at the application tier can be secured with Edge Encryption or CLEE. Layering encryption allows all data to be protected when not in use. It also allows highly sensitive fields, such as personally identifiable information (PII) and protected health information (PHI), to be protected from additional attack vectors.

## Full Disk Encryption

Full Disk Encryption (FDE) mitigates the risk of sensitive data being exposed in the event of the physical theft of a disk drive used in a cloud instance. FDE includes the entire disk, which can only be decrypted by the operating system. This encryption also does not impact the performance or functionality of the application.

Provided via self-encrypting hard drives with AES-256-bit encryption, FDE delivers at-rest protection only and is focused on preventing data exposure through the loss or theft of hard disks holding customer data. It does not provide application tier protection for data in transit or against unauthorized access while the drive is operational.

Measures in place by ServiceNow to mitigate loss or theft of storage devices may also be a factor when considering FDE.

## Usage and restrictions

FDE is a high-speed encryption method integrated into ServiceNow's Advanced High Availability (AHA) architecture that provides encryption of customer data at rest. FDE decrypts the data when actively being used or accessed by the server's operating system. The hard drive models used by ServiceNow comply with the Trusted Computing Group (TCG) enterprise specifications and are secured using a passphrase generated from a key stored in our SafeNet key management appliance.

## Conclusion

The available encryption options from ServiceNow are intended to address common additional data protection and privacy needs for its customers.

- **Column Level Encryption Enterprise** provides simple, secure encryption, but may not meet all customer requirements around key storage and management.
- **Edge Encryption** is a significant enhancement over Column Level Encryption Enterprise and allows customers to control where and how data is encrypted as well as the management and configuration of all keys. However, it requires significant planning on the part of the customers.
- **Database Encryption** allows all stored data to be encrypted in real-time, providing protection for data online and offline, with no loss of functionality.
- **Full Disk Encryption** protects offline data in case of disk loss or theft, and may be relevant to heavily regulated organizations, but can add significant cost to a customer's ServiceNow deployment.

Highly sensitive fields that need to be encrypted at the application tier can be secured with Edge Encryption or Column Level Encryption Enterprise.

With Edge Encryption, cleartext data never leaves your premises – only encrypted or tokenized data is sent to the instance. This can enable the Now Platform to be used in cases where external data storage may not otherwise be appropriate.

Full Disk Encryption can be coupled with both application tier encryption and database tier encryption for a layered security approach.

Layering encryption allows all data to be protected when not in use and highly sensitive fields, such as PII and PHI, to be protected from additional attack vectors.

## Resources

### Encryption-specific resources:

- [Product Documentation](#)
- [Column Level Encryption Enterprise technical implementation and configuration](#)
- [Edge Encryption technical implementation and configuration](#)

### Further reading resources:

- [Trust and Compliance Center](#)
- [CORE \(Compliance Operations Readiness Evidence\) platform](#)

## Appendix A:

### Edge Encryption options

Operations	Standard AES-128 or AES-256	Equality-preserving AES-128 or AES-256	Order-preserving* AES-128 or AES-256
Group by		X	X
Is empty		X	X
Is not empty		X	X
Equal		X	X
Not equal (excludes empty fields)		X	X
Is not		X	X
Sort by			X
Is greater than			X
Is greater than or equal			X
Is less than			X
Is less than or equal			X
Contains			
Starts with			
Ends with			
Operators that imply the right side of the clause is a field			
Text search			

\*MySQL is required for order-preserving encryption.

## Appendix B:

### Functionality and encryption implications for Edge Encryption

Functionality	Implication	Mitigation
Reporting	Reporting operates on column data values. Because the ServiceNow application must use the column's values to generate reports, there is the potential a report will not generate correctly because it does not have access to the plaintext. This is only an issue if the report being generated uses columns that have been encrypted using Edge Encryption.	Review the columns you need to include in the report that may benefit from equality-preserving or order-preserving encryption, and use those supported functions where necessary. Do not export reports that contain encrypted columns since the report is generated on your instance without access to the encryption key.
Buisness rules and logic	ServiceNow runs all business logic on the back end, so any business rule that needs to read from or write to an encrypted column may have trouble executing the rule.	Review the columns included in business rules that may benefit from equality-preserving or order-preserving encryption, and use those supported functions where necessary. If this is not possible, do not use the encrypted columns.
Encrypted text exceeding table column widths	Encryption algorithms often create ciphertext that is longer than the plaintext. For example, the name "King George III," which is 15 bytes long, might be encrypted to "#j&_xz[~K@6_69FExñ\$\$\$4n\{2*)c," which is 30 bytes long. If the column in the ServiceNow instance is limited to 20 characters, the full length of encrypted text will not be stored, causing it to become invalid and incapable of decryption.	Examine each column you plan to encrypt (either programmatically or by hand) and widen them to ensure each can store the longest possible encrypted value for that column.
Workflows	Similar to business rules, workflows often operate from a column's value. A workflow that depends on the ability to examine plaintext in a table column will fail to function because it only has access to encrypted versions of the text.	Review the columns from your workflows that may benefit from equality-preserving or order-preserving encryption, and use those supported functions where necessary. If this is not possible, do not use the encrypted columns.

Functionality	Implication	Mitigation
Searching	ServiceNow executes all searches on the back-end database, which means all searches use the data within the columns. If the search is being executed against columns with ciphertext values rather than plaintext values, a user may not receive the desired results. However, searches for exact matches will still work because the search term will be converted into ciphertext by Edge Encryption—this only applies to equality-preserving and order-preserving encryption. This enables the back-end search function within ServiceNow to effectively search for the desired term. “Contains” searches on free-form text fields are the most difficult to implement because the search text cannot be found in the body of the encrypted text.	Tokenization can make “contains” searches possible. For example, a word or character string can be tokenized individually so the encrypted search text finds a matching tokenized word in the body of the field. Equality-preserving and order-preserving encryption provide a technique that partially addresses the “contains” search with strong encryption.
Sorting	ServiceNow does all sorting on the back-end server. As an application, ServiceNow deals with large data sets and generally returns the Top N to the user based on some form of sorting. Because the application always sorts on the back end, and the application always sorts on the ciphertext values, when a user initiates the sorting of encrypted data, the results may appear incorrectly.	Apply order-preserving encryption to implement a technique that addresses this issue (while maintaining strong encryption) using a stored subset of plaintext table data as a token to prepend to the ciphertext for sorting purposes before it is sent to the instance.
Bulk import/export	ServiceNow does all export and import activities on the back-end servers. As such, any exported data—Excel, XML, CSV, PDF, or other— exports the ciphertext values of any encrypted columns. Likewise, because these data formats are not supported, any attempt to import data into an encrypted column will result in unencrypted values being written into the column, unless the process that is sending data to the instance is configured to proxy communications through the Edge Encryption proxy.	Some vendor solutions are capable of intercepting exported data files, such as XML or CSV, and decrypting them prior to being delivered to the user. Check with your vendors to ensure they can encrypt and decrypt the file types you need. If they can, a web service integration is necessary.
Mobile access	To see any data that has been encrypted using Edge Encryption, a mobile browser must access the ServiceNow instance through the Edge Encryption proxy. Actions allowed via mobile devices need the ability to see the plaintext data in order for the ServiceNow application to function correctly. This includes workflow approvals via mobile devices and other actions available to the user through the mobile interface.	Ensure that mobile access to the ServiceNow instance goes through the company's network so all access is granted via the Edge Encryption proxy. Be selective about which columns you encrypt. Modify any workflows that use encrypted columns if the workflow is visible or accessible using mobile devices.

Functionality	Implication	Mitigation
Inbound/ outbound email and SMS notifications	When ServiceNow triggers a notification, it could send an email or SMS that contains a mixture of hard-coded plaintext and encrypted field text. For example, an email template that looks like this: Dear \${name}, we have changed your shirt size from \${old_size} to \${new_size}. Will be rendered with field substitutions, so it looks like this if the corresponding columns are encrypted: Dear Bob Baker, we have changed your shirt size from 6^SD[&%T to H7asdh78.	Edge Encryption does not support inbound nor outbound email. Taking this into account, be selective about which columns you encrypt.  Modify any SMS text message that uses encrypted columns and remove them from the message. Provide a URL in the message that leads to a ServiceNow page that shows the contents of the message—this way, the Edge Encryption Proxy can decrypt the text.
Reference fields	Reference fields are not supported by Edge Encryption because the sysid that is being used to make the link between your form and the actual field needs to be in the clear.	Use a secondary field, encrypt it, and hide the reference from the form. The actual source field must be a string type and will need to be configured to be encrypted with one of the three available encryption types.
Web services integrations	ServiceNow can integrate with outside data sources using industry-standard web service protocols like REST and SOAP. A third-party integration, which is usually software running on a computer inside your network, can retrieve and insert data into ServiceNow automatically, but if that data is not properly encrypted, plaintext can be inserted into columns that are expected to be encrypted. As a result, the Edge Encryption proxy attempts to decrypt text that was not encrypted in the first place. This leads to data inconsistencies within the ServiceNow instance and could impact what the user sees.	Configure all automated processes to send or receive data from the ServiceNow instance using encryption rules so the Edge Encryption proxy can identify the columns in the payload with the encrypted instances.
Legacy data	ServiceNow customers may have amassed large amounts of data within their ServiceNow instances within various columns. The amount of data these customers need to encrypt could contain millions of records. Because encryption keys and algorithms cannot be held within ServiceNow, encrypting large amounts of data using Edge Encryption can take a long time.	You can run a mass encryption job on a per-column and attachment basis. Plan when you want to run this type of operation carefully so you can accommodate for the volume of columns and attachments you plan to encrypt.

## Appendix C:

### Comparison of encryption at rest solutions

	Database Encryption	Column Level Encryption Enterprise	Edge Encryption
Description	Encryption of data at rest when not being processed in the instance	Equality Preserving Encryption of data at rest within the database based on user role in the instance	Standard, Equality Preserving, and Order Preserving encryption of data at rest within the database and instance. Data sent to ServiceNow already encrypted by customer
Field types Supported for Encryption	All	<ul style="list-style-type: none"> <li>String Text</li> <li>Attachment</li> <li>URL</li> <li>Date</li> <li>Date/Time</li> </ul>	<ul style="list-style-type: none"> <li>String Text</li> <li>Attachments</li> <li>URL</li> <li>Journal</li> <li>Date</li> <li>Date/Time</li> </ul>
Encryption Types	AES-256	AES-128 and AES-256	AES-128 and AES-256
Tokenization	No	No	Yes, for pattern-matched data
Encryption Key Creation	ServiceNow	Managed by ServiceNow and the customer	Customer
Additional Requirements	None	None	<ul style="list-style-type: none"> <li>On-premises Encryption Proxy</li> <li>Encryption Key Store</li> <li>Optional on-premises MySQL Database for Tokenization and order Preserving encryption</li> </ul>

## STEP 2: ASSESSMENTS OF GENERAL LAWS AND PRACTICES IN THE DESTINATION COUNTRY

### UNITED STATES<sup>1</sup>

Score	Features
1	High level of safeguards in place, essentially equivalent to the level available in the EEA
2	High level of safeguards in place, but below the level of those available in the EEA
3	Some safeguards in place, but materially below the level of those available in the EEA
4	Very limited safeguards in place, significantly below the level of those available in the EEA
5	No safeguards in place (lowest level of equivalence)

<sup>1</sup> THIS BASELINE ANALYSIS PROVIDES A REVIEW OF US LAWS AND GENERAL PRACTICE. THIS ANALYSIS SHOULD BE COMPLETED IN STEP 4 TO TAKE ACCOUNT OF ACTUAL PRACTICE WITH REFERENCE TO RELEVANT, OBJECTIVE, RELIABLE, VERIFIABLE AND PUBLICLY AVAILABLE OR OTHERWISE ACCESSIBLE SOURCES SUPPORTING THE FINDINGS RELATING TO THE RISK IN PRACTICE.

For example, because 'foreign powers' or 'agents of foreign powers' is narrowly construed, it should be carefully considered for the purposes of scoring Step 4 of the transfer assessment whether the organization is likely to possess such information or (if not otherwise subject to Section 702), whether the organization will provide such information to any ECS or RCS. Examples of factors to be taken into account when considering the practical impact of Section 702 may include: the role of customer and employee due diligence programs that may be designed to screen out the sorts of entities and individuals likely to be of interest to US authorities; the types of goods or services provided by the organization; and/or the types of personal data processed (e.g., ordinary commercial information like employee, customer, and sales records). In addition, some of the qualifying activities that may lead to lawful surveillance are activities that would constitute (serious) criminal offences both in the US and the EEA/UK (such as sabotage, terrorism and the proliferation of weapons of mass destruction). Organizations whose EEA or UK operations involve ordinary commercial products or services and the related personal data are less likely to receive or generate such information in the course of business.



STEP 2 JURISDICTIONAL ANALYSIS FOR: UNITED STATES					
PREPARED BY: DLA Piper		Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>2</sup>	Comparative analysis	Score
Criteria					

---

<sup>2</sup> The assessment will be based first on legislation publicly available. Sources and information should be relevant, objective, reliable, verifiable and publicly available or otherwise accessible.

2.1 Regulation on the processing of personal data	<p>The extent to which <b>local laws</b> offer clear, precise and accessible legal safeguards to the processing of personal data equivalent to the protections offered in the EEA /UK. This will include an analysis of the local laws and practices, including constitutional rights to privacy and how those laws apply both to the data importer but also third parties (e.g., law enforcement) who may seek to secure access to the data following transfer.</p> <p>In this context, note the EEA / UK has a developed law that specifically recognises legal rights to protection of “personal data” consistent with the principles of data protection set out in OECD Convention 108+.</p> <p>In particular, the assessment will consider:</p> <ul style="list-style-type: none"> <li>(i) whether there are any relevant local laws laying down requirements to disclose personal data to public authorities or granting such public authorities powers of access to personal data;</li> <li>(ii) where relevant local laws formally meet EEA /UK standards on fundamental rights and freedoms and the necessity and proportionality of</li> </ul>	<p>The US privacy regime is not uniform. At the federal level it is fragmented by sector, and states can vary their laws; accordingly, the regime does not have the comprehensive nature of the GDPR, at least directly. The regime offers some protections, often that are significant, and many of the state laws are similar. The federal laws include HIPAA (privacy and security requirements for certain health data), GLBA (privacy and security requirements for financial services), FISA (limits on foreign intelligence surveillance), FCRA (privacy of credit reporting), Section 5 of the Federal Trade Commission (FTC) Act (prohibiting unfair and deceptive trade practices; this is the principal basis for FTC enforcement of privacy rights), TCPA (consent requirements for phone and text marketing), state UDAP (unfair or deceptive acts or practice) laws (the state equivalent of the FTC Act), the CCPA (California’s privacy law), state data breach reporting laws, state data security laws, state genetic privacy laws, state wiretap laws, state constitutions, as well as others. These laws typically apply based upon an analysis of the residency of data subject, and to some degree the location of the company, though this is often a lesser criterion for application.</p> <p>Consequently, while the US regime is markedly different from the EEA/UK regime in terms of structure, overall the privacy and security laws create a multitude of requirements for businesses using personal information, and these pose significant risks in terms of litigation and regulatory enforcement (see below).</p> <p>From a security perspective, federal and/or state laws create for most US businesses</p>	<p>In general, while many privacy laws exist, the balance of federal and state law is focused on data security, meaning that many businesses focus on the protection of personal data from breach events. Where privacy laws do exist, they do not offer data subject rights in a manner comparable with EEA/UK law.</p> <p>The US at the federal level lacks generally applicable data protection laws.</p> <p>Many states have laws that cover privacy, and security issues in particular.</p> <p>Moreover, California has imposed both privacy and security laws that are general in nature, applying to controllers doing business in California and potentially imposing significant penalties.</p>	4
--	--	---	--	---

	<p>restrictions, whether the practices of public authorities clearly indicate that they do not normally apply/comply with the legislation that governs, in principle, their activities; and</p> <p>(iii) where relevant local law may be lacking, are there any indications of practices in force that are incompatible with EEA/UK law.</p>	<p>requirements to take reasonable technical, physical and organizational measures to protect the security of sensitive personal information (e.g., health or financial information, telecommunications usage information, biometric data, national social security numbers (SNN), data that can be exploited for identity theft or other information that would require security breach notification). In addition, many states require that reasonable security exist for personal information, though the laws tend to focus on information such as credit card data, SSN, and not personal information in as broad a sense as GDPR. For example, Massachusetts has enacted regulations that apply to any company that collects or maintains sensitive personal information (e.g., name in combination with Social Security number, driver's license, passport number, or credit card or financial account number) regarding Massachusetts residents. California has a law that has similar requirements, and there are now statutory penalties for the failure to maintain reasonable security. Moreover, most state Attorneys General have the ability to enforce these laws. Regarding sectoral data security and privacy laws and regulations that impose specific security requirements on regulated, and unregulated, entities (principally the financial, insurance and health sectors) federal laws coexist with state laws. California notably requires any company operating a website to have an online privacy policy, and companies typically do not limit their privacy policy to just California residents. State wiretap, financial services, medical</p>	
--	--	--	--

		<p>privacy, genetic and insurance privacy laws also exist.</p> <p>The GLBA and implementing regulations require financial institutions to implement reasonable security measures, and also place limitations on use of non-public personal information as well as create transparency obligations. Federal financial regulators impose extensive security requirements on the financial services sector, including requirements for security audits of all service providers who receive data from financial institutions.</p> <p>At the state level, the New York Department of Financial Services (NYDFS) regulations impose extensive cybersecurity and data security requirements on licensees of the NYDFS, which includes financial services and insurance companies.</p>		
2.2 Regulation of public authority access to private data	<p>The extent to which the <b>level of access legally permitted and conducted in practice</b> by public authorities to personal data (e.g. to secure disclosure of, or conduct surveillance on, private information for national security purposes or other reasons) can be regarded as a justifiable interference and is subject to safeguards equivalent to that within the EU, in light of legislation, practice and reported precedents. This will consider</p>	<p>Foreign intelligence surveillance — i.e. the collection of intelligence information about non-US persons — is primarily conducted through a handful of legal frameworks that were considered by the CJEU in <i>Schrems II</i><sup>3</sup>. However, there are other surveillance regimes that the CJEU did not consider that may be subject to similar, or lesser, safeguards.</p> <p><u>Section 702 FISA</u></p> <p>Section 702 of the Foreign Intelligence Surveillance Act (FISA)<sup>4</sup> permits the US government to conduct targeted surveillance of non-US persons located outside the US to acquire 'foreign intelligence information.'</p>	<p>Some areas of US surveillance law have an identifiable and clearly constrained basis in law (e.g., the regimes that operate within the US under FISA, since Section 702 is limited to electronic communication service providers, and a Section 215 search is conducted on tangible things and ordered by a judge on the basis of specific 'selection terms'). However, this is not universally the case (e.g., the broad executive authority to intercept information in transit to the US under EO 12,333).</p>	5

<sup>3</sup> *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems and intervening parties* (Case C-311/18) ("**Schrems II**").

<sup>4</sup> 50 U.S.C. § 1881a.

	<p>specifically whether the right of public authorities to access data is:</p> <p>(i) underpinned by a legal framework that is publicly available and sufficiently clear;</p> <p>(ii) carried out in pursuit of legitimate aims which are necessary and proportionate in a democratic society to safeguard important objectives as also recognised in EU/UK law (noting that proportionality involves balancing any interference with fundamental privacy rights with what are necessary and important public interests); and</p> <p>(iii) subject to adequate and effective oversight from</p>	<p>'Foreign intelligence information' means:</p> <p>(1) Information that relates to, and if concerning a US person is necessary to, the ability of the US to protect against actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or</p> <p>(2) Information with respect to a foreign power or foreign territory that relates to, and if concerning a US person is necessary to, the national defense or the security of the US or the conduct of the foreign affairs of the US.<sup>5</sup></p> <p>Further, the target of the surveillance must be a "foreign power",<sup>6</sup> or an "agent of a foreign power".<sup>7</sup> According to the Office of the</p>	<p>Further, even where surveillance regimes have a basis in law, they may operate in a way that is not sufficiently targeted, and therefore proportionate, from an EEA perspective (i.e., Section 702). Further, judicial oversight is not present for EO 12,333 and, while it exists for Section 702, it operates at a broad level (i.e., to approve an overall program of surveillance, and not specific requests for access to communications data). As determined by the CJEU, this is not aligned with EEA standards.</p>	
--	---	---	--	--

<sup>5</sup> 50 U.S.C. § 1801(e).

<sup>6</sup> 'Foreign power' means: (A) A foreign government or any component thereof, whether or not recognized by the US; (B) A faction of a foreign nation or nations, not substantially composed of US persons; (C) An entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; (D) A group engaged in international terrorism or activities in preparation thereof; (E) A foreign-based political organization, not substantially composed of US persons; (F) An entity that is directed and controlled by a foreign government or governments; or (G) An entity not substantially composed of US persons that is engaged in the international proliferation of weapons of mass destruction. 50 USC § 1801(a).

<sup>7</sup> There are two definitions in FISA for 'agent of a foreign power', one that applies to non-US persons only and one that applies to all persons, including US persons. It is important to note that the first definition, which applies only to non-US persons, is broader and less tied to criminal violations of US law. With respect to non-US persons, 'agent of a foreign power' is defined as a person who: (A) Acts in the US as an officer or employee of a foreign power or a member of a foreign power, irrespective of whether the person is inside the US; (B) Acts for or on behalf of a foreign power that engages in clandestine intelligence activities in the US contrary to the interests of the US, when the circumstances indicate that such person may engage in such activities or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; (C) Engages in international terrorism or activities in preparation thereof; (D) Engages in the international proliferation of weapons of mass destruction or activities in preparation thereof; (E) Engages in the international proliferation

	<p>courts or other independent authorities.</p> <p>The assessment will consider <b>pervasive surveillance activity</b> (across the destination country as a whole) and whether access can in practice be exercised by public authorities in light of legislation, legal powers, technical, financial and human resources at their disposal and of reported precedents.</p>	<p>Director of National Intelligence, in 2016, the US government had approximately 106,469 targets authorized for collection under Section 702, which is approximately .004% of the world's internet users and .001% of the world's population.<sup>8</sup></p> <p>Moreover, although Section 702 surveillance does not require a warrant for each individual, it still receives oversight in the form of the of the Foreign Intelligence Surveillance Court (FISC). Before the US government may acquire data under Section 702, the FISC generally must approve a written certification submitted by the Attorney General and the Director of National Intelligence jointly authorizing the collection activities for up to one year.<sup>9</sup> These certifications include targeting procedures defining how the government determines which individuals' communications may be acquired and limit the purpose of the surveillance to a specified type of foreign intelligence information.<sup>10</sup></p> <p><u>Section 215 FISA</u></p> <p>Section 215 authorizes foreign intelligence related surveillance in respect of both US and non-US persons, and to activity both within</p>	
--	--	---	--

of weapons of mass destruction or activities in preparation therefore for or on behalf of a foreign power, or knowingly aids or abets any person in the conduct of such proliferation or activities in preparation therefor, or knowingly conspires with any person to engage in such proliferation or activities in preparation therefore.

For all persons, including US persons, 'agent of a foreign power' is defined to mean a person who: (A) Knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the US; (B) Pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the US; (C) Knowingly engages in sabotage or international terrorism or activities that are in preparation therefore for or on behalf of a foreign power; (D) Knowingly enters the US under a false or fraudulent identity for or on behalf of a foreign power or, while in the US, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; (E) Knowingly aids or abets any person in the conduct of activities described in Subparagraph (A), (B) or (C) or knowingly conspires with any person to engage in activities described in Subparagraph (A), (B), or (C). 50 USC § 1801(b).

<sup>8</sup> <https://www.dni.gov/files/icofr/Section702-Basics-Infographic.pdf>.

<sup>9</sup> 50 U.S.C. §§ 1881a(a),(g) 2018.

<sup>10</sup> Privacy and Civil Liberties Board FISA 702 Report at 6.

		<p>and outside US borders. The nature and type of information which may be collected is however different from Section 702 - this is not an electronically focused statute, but rather a law directed to the production of business records ("tangible things").</p> <p>Notably, Section 215 contains stricter safeguards than Section 702. Any request for the production of records under Section 215 must be made to a judge within the FISC and be presented in terms which set out the specific "selection terms" of tangible things that are to be ordered for production in terms that detail with precision what is required and when it must be produced – general requests must not be made and bulk data collection is not permitted.</p> <p><u>EO 12,333</u></p> <p>It is widely understood that surveillance activity undertaken to obtain foreign intelligence information outside the United States may be effectively authorized by the President on an almost unfettered basis. In this regard, Executive Order 12,333 governs collection of foreign intelligence information outside the United States. It was considered by the CJEU to be relevant to the issue of data transfers to the EU, on the basis that it is understood to be relied upon to intercept communications in transit to the United States (e.g. travelling through undersea Internet cables).</p> <p><u>PPD-28</u></p> <p>Presidential Policy Directive 28 ("PPD-28") applies to surveillance conducted under EO 12,333, and it attempts to introduce a degree of proportionality (i.e. a requirement that surveillance activities must be as tailored as</p>	



		feasible) that benefits non-US as well as US persons. While PPD-28 may not constitute a binding law, arguments have been advanced that, as an order from the President, there is no reason to suspect that it is not complied with in practice by the Executive branch.		
2.3 Regulatory supervision	The <b>extent to which courts, regulators and/or supervisory authorities enforce the rule of law</b> and/or rights guaranteed in relation to the protection of data in an independent and effective manner, with evidence of meaningful resources and enforcement activity.	Both at the federal and state level, where privacy laws exist, there is supervision and regulation of privacy. For example, the Federal Trade Commission (FTC) enforces compliance with the FTC Act; the Office of Civil rights enforces HIPAA privacy and security rules; the FTC enforces the GLBA Privacy Rule; and the Federal Communications Commission enforces TCPA. State Attorneys' General have a key role in enforcement of state security and privacy statutes (California settlement with Anthem Health for \$8.69 million; multi-state settlement with Equifax for approximately 600 million). Regarding supervision in the surveillance context, under Sections 702 and 215 there is supervision by the FISC, which is part of the independent judicial branch. However, under Section 702 the FISC approves an overall program of surveillance, it does not approve each individual request for surveillance data sent to an electronic communications provider under that program, nor each subsequent search / use of data received by the government in response to a request. Consequently, while there is judicial oversight under Section 702, it is necessarily high-level and does not extend to oversight of decisions to interfere with the communications of	In the limited areas where the US extends data privacy protections, there is evidence of active enforcement and often significant fines. In the surveillance context, judicial oversight (through the FISC) is applied to Section 702. However, the CJEU was critical of the high-level nature of this oversight, given that it operates at the level of approving an overall surveillance program (and not individual requests for communications data). There is no judicial oversight of the broad executive authority to intercept information in transit to the US under EO 12,333.	3



		individual persons within the context of an approved program. In terms of EO 12,333, PPD-28 requires that significant compliance issues (in relation to the surveillance procedures which agencies are required to maintain) involving a non-US person are reported to the Director of National Intelligence, and the DNI is required to consult with the US Secretary of State to determine whether to notify the relevant foreign government.		
2.4 Rights of redress	the extent to which individuals can easily and effectively <b>enforce rights</b> and <b>seek redress</b> by raising complaints, claims and / or appeal and enforce decisions in relation to both data protection infringements and public disclosure / surveillance activity through judicial and/or administrative processes (e.g., help from local data protection authorities) including whether redress mechanisms can be effectively applied in practice and are not thwarted by local laws and/or practices. This section will also consider whether data subjects can secure self-help remedies – e.g., right to secure access to or require erasure of personal data files, and whether the breach of local laws can be effectively invoked and relied on by individuals.	the extent to which individuals can easily and effectively <b>enforce rights</b> and <b>seek redress</b> by raising complaints, claims and / or appeal and enforce decisions in relation to both data protection infringements and public disclosure / surveillance activity through judicial and/or administrative processes (e.g., help from local data protection authorities) including whether redress mechanisms can be effectively applied in practice and are not thwarted by local laws and/or practices. This section will also consider whether data subjects can secure self-help remedies – e.g., right to secure access to or require erasure of personal data files, and whether the breach of local laws can be effectively invoked and relied on by individuals.	Some privacy laws (for example, credit reporting; marketing and electronic communications; call recording and cable communications privacy laws; the CCPA) may be enforced at least in part through private rights of action, either individual actions for actual damages, or class action lawsuits for significant statutory damages and attorney's fees. Moreover, private plaintiffs may also bring common law invasion of privacy claims, permitting state law actions against private companies. Injunctive relief is also permitted under these laws.  As noted in the <i>Schrems II</i> case, effective remedies with respect to claims against the US government for surveillance activities are complicated by constitutional issues (such as standing to bring a claim under Article III) well as a lack of cognizable damage in many cases for privacy violations. Claims may be brought with somewhat less difficulty under FISA in respect of surveillance performed without statutory or Presidential authorization, misuse of surveillance information, or unlawful disclosure of surveillance information by an individual officer); in many cases redress is granted in the form of a settlement. Further,	individual persons within the context of an approved program. In terms of EO 12,333, PPD-28 requires that significant compliance issues (in relation to the surveillance procedures which agencies are required to maintain) involving a non-US person are reported to the Director of National Intelligence, and the DNI is required to consult with the US Secretary of State to determine whether to notify the relevant foreign government.
			4	The US system generally does not include rights for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data. Accordingly, aside from specific sectors or state laws (such as CCPA), data protection laws equivalent to the GDPR or the Law Enforcement Directive do not exist in the US to give data subjects fundamental rights to access, erase or amend their data, and to have these rights enforced in court.  The rights to bring a claim that do exist are rights to file a civil suit in respect of actual harm suffered.  There is a disparity here between the European understanding of effective rights and remedies for data protection infringements – which includes not just a right to compensation for material or non-material damage, but also must include effective rights to access, amend or erase data – and the US

		self-help remedies are limited and in the surveillance context there are knowledge limitations that potentially impact remedies.	understanding of civil lawsuits, in which actual (i.e. material) harm must be established. Significantly, it is generally accepted that the protection of the Fourth Amendment (which guarantees a right of privacy which must be respected by the US government) can only be invoked by US citizens.	
2.5 International treaties	<p>The extent to which the country has concluded <b>international treaties</b> and related commitments on handling of personal data to support the safeguarding of data – this will include consideration both of the existence of:</p> <ul style="list-style-type: none"> <li>(i) international treaties that relate to the protection of data generally consistent with principles enshrined in EEA/UK law, and</li> <li>(ii) any specific arrangements concluded to provide safeguards in relation to country-to-country transfers (e.g., UK-U.S. Bilateral Data Access Agreement which brings into effect the 'quashing' provisions of 18 USC § 2703(h)(2))</li> </ul>	<p>There are a number of treaties, including Mutual Legal Assistance Treaties (MLATs) that can have an impact on the gathering of foreign nationals' data for use by US law enforcement. Moreover, there are certain arrangements to be considered on a country-by-country basis that may provide additional assurances (such as cooperation in the area of securities laws enforcement). However, data gathered in the US is likely not subject to treaty.</p> <p>The US is not subject to any data protection treaties that are of note, such as OECD Treaty 108, or other similar treaties.</p>	The US has limited commitments in this area and appears to clearly fall short of equivalence with the EEA.	4
<b>Total</b>				20

## STEP 2: ASSESSMENTS OF GENERAL LAWS AND PRACTICES IN THE DESTINATION COUNTRY

Score	Features
1	High level of safeguards in place, essentially equivalent to the level available in the EEA
2	High level of safeguards in place, but below the level of those available in the EEA
3	Some safeguards in place, but materially below the level of those available in the EEA
4	Very limited safeguards in place, significantly below the level of those available in the EEA
5	No safeguards in place (lowest level of equivalence)

STEP 2 JURISDICTIONAL ANALYSIS FOR: AUSTRALIA PREPARED BY: DLA Piper				
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis	Score
2.1 Regulation on the processing of personal data	<p>The extent to which <b>local laws</b> offer clear, precise and accessible legal safeguards to the processing of personal data equivalent to the protections offered in the EEA /UK. This will include an analysis of the local laws and practices, including constitutional rights to privacy and how those laws apply both to the data importer but also third parties (e.g. law enforcement) who may seek to secure access to the data following transfer.</p> <p>In this context, note the EEA / UK has a developed law that</p>	<p><b>Legal Framework</b></p> <p>Data privacy and protection is regulated in Australia by a combination of federal, state and territory laws.</p> <p>The <i>Privacy Act 1988</i> (Cth) (<b>Privacy Act</b>) which includes the Australian Privacy Principles (<b>APPs</b>) is the core privacy legislation in Australia.</p> <p>The Privacy Act applies to private sector entities (with an annual turnover of &gt;AU\$3m) and all Commonwealth Government (including ACT) agencies, as well other specific businesses not meeting the turnover thresholds, including private health service providers processing health information, credit-reporting bodies and businesses that sell or purchase personal information (<b>APP entities</b>).</p>	<p>The Privacy Act does have areas of overlap with the GDPR, including in relation to its data protection principles, and its definition of personal information. However, the majority of the Privacy Act is closer to the previous Directive 95/46/EC than GDPR. Whilst the breadth of application of the Privacy Act is not as wide (for example, the turnover based limit on application to private sector entities), this is compensated in part by additional sector and state</p>	3

<sup>1</sup> The assessment will be based first on legislation publicly available. Sources and information should be relevant, objective, reliable, verifiable and publicly available or otherwise accessible.

	<p>specifically recognises legal rights to protection of “personal data” consistent with the principles of data protection set out in OECD Convention 108+.</p> <p>In particular, the assessment will consider:</p> <p>(i) whether there are any relevant local laws laying down requirements to disclose personal data to public authorities or granting such public authorities powers of access to personal data;</p> <p>(ii) where relevant local laws formally meet EEA /UK standards on fundamental rights and freedoms and the necessity and proportionality of restrictions, whether the practices of public authorities clearly indicate that they do not normally apply/comply with the legislation that governs, in principle, their activities; and</p> <p>(iii) where relevant local law may be lacking, are there any indications of practices in force that are incompatible with EU/UK law.</p>	<p>Most states and territories also have their own (broadly aligned) privacy legislation which are applicable to state government agencies and private businesses that contract with them.</p> <p>In addition to the Privacy Act, APPs and state privacy laws, there is also specific sector-focused legislation that regulates privacy and information risk; for example, in the health sector and in the telecommunications sector. There is also other legislation at the Commonwealth and state level that is relevant to privacy and the use of personal information, including the <i>Spam Act 2003 (Cth)</i> (electronic marketing), the <i>Do Not Call Register Act 2006 (Cth)</i> (unsolicited commercial calls to listed phone numbers), criminal laws prohibiting unauthorised access to computer systems and various surveillance and listening-devices legislation (as further outlined in section 2 below). More recently, the <i>Treasury Laws Amendment (Consumer Data Right) Act 2019 (CDR)</i> introduces a consumer-directed data portability mechanism, applicable currently to the banking sector (see further below).</p> <p>Further, specific regulators have issued (non-statutory / non-mandatory) standards that instruct regulated entities with regard to specified data protection measures that should be put in place. For example, the Australian Prudential and Regulatory Authority (APRA) regulates financial services institutions and has introduced a number of ‘prudential’ standards on privacy and information risk, and the Australian Securities and Investment Commission (ASIC) regulates corporations generally.</p> <p>Finally, the Australian Consumer Law (ACL) prohibits applicable businesses (including digital platforms) carrying on businesses in Australia from engaging in certain forms of conduct in connection with the supply or acquisition of goods or services. This includes misleading or deceptive conduct, unconscionable conduct and unfair practices. Each of these prohibitions under the ACL have been recently cited by the Australian Competition and Consumer Commission (ACCC) (as regulator) as applicable to the privacy practices of an organisation, including representations and statements made as to how users’ data is collected and disclosed, including under privacy policies and terms of use. (See further below re ACCC’s recent case against Google for alleged breach of privacy practices).</p> <p><b>Scope of Privacy Act</b></p>	<p>specific laws. There are also subject specific laws in areas that mirror equivalent laws in the EU (e.g. on electronic marketing).</p> <p>Whilst the Privacy Act does create some data subject rights, these are not as comprehensive as those under the GDPR.</p> <p>Further, there is no fundamental or constitutional right to privacy or data protection (equivalent to rights under the EU Charter and the European Convention on Human Rights).</p>
--	---	--	--

STEP 2 JURISDICTIONAL ANALYSIS FOR: AUSTRALIA PREPARED BY: DLA Piper				
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis	Score
		<p>The Privacy Act regulates the handling of personal information, defined as information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether recorded in a material form or not.</p> <p>This definition has broad similarities with the definition of personal data under the EU GDPR, which applies to 'information relating to and identified or identifiable natural person', though at present it is unclear whether the Privacy Act definition includes metadata such as IP addresses, other location data, or other technical data – this is likely to be changed under the Government Privacy Act Review (<i>see further below</i>).</p> <p>The APPs set out standards, rights and obligations for the handling, including collection, use, disclosure, security, access and correction of personal information (including sensitive information), adopting a reasonableness approach in many cases.</p> <p>Broadly, the 13 principles require reasonable steps to be taken by APP entities to implement practices, procedures and systems to ensure compliance with the Privacy Act, including to:</p> <ul style="list-style-type: none"><li>• implement procedures that ensure open and transparent management of personal information, including to notify individuals, and to make available up-to-date privacy policies and collection statements;</li><li>• comply with certain restrictions when collecting personal data, including to obtain consent to the collection of sensitive personal information;</li><li>• subject to certain exceptions, to not use or disclose personal information for a secondary purpose without consent;</li><li>• ensure the quality of personal information, including that it is accurate, up to date and complete;</li><li>• destroy personal information or to ensure it is de-identified if no longer needed;</li><li>• secure and protect the personal data they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure; and</li></ul>		

STEP 2 JURISDICTIONAL ANALYSIS FOR: AUSTRALIA PREPARED BY: DLA Piper				
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis	Score
		<ul style="list-style-type: none"> <li>take reasonable steps to ensure that an overseas recipient does not breach the APPs when disclosing information cross-border, and subject to certain exceptions, the APP entity will generally remain liable for any breach of the APPs committed by the overseas recipient.</li> </ul> <p>Individuals are also granted some limited direct rights under the APPs, including a right of access to, and correction of their personal information in certain circumstances (<b>see below</b>).</p> <p>Further, under the <i>Privacy Amendment (Notifiable Data Breaches) Act 2017</i> (Cth) (<b>Notifiable Data Breach Regime</b>) which amends Part IIIC of the Privacy Act, obligations are imposed on APP entities who experience a data breach to conduct an assessment to determine whether a suspected breach is an 'eligible data breach'. An APP entity must notify the Australian Privacy and Information Commissioner (the <b>Commissioner</b>) and affected individuals in the event of an 'eligible data breach' or if the Commissioner directs the entity to do so. An eligible data breach is any unauthorised access to, or disclosure or loss of personal information where the breach is likely to result in serious harm to an individual and the prevention of the risk of serious harm through remedial action has not been successful).</p> <p><b>Law Enforcement</b></p> <p>Enforcement bodies (including law enforcement agencies, such as the Australian Federal Police) are granted certain exemptions to the collection, use and disclosure requirements of the Privacy Act and APPs (and under relevant state and territories legislation), including where the collection of such information is reasonably considered as necessary for 'law enforcement' purposes, including where such information is authorised or required under subpoena.</p> <p><b>Constitutional Right to Privacy?</b></p> <p>Currently, there is no constitutional right to privacy akin to that set out in the EU/UK under the OECD Convention 108+. There is also no common law tort of invasion of privacy in Australia, although there has</p>		



STEP 2 JURISDICTIONAL ANALYSIS FOR: AUSTRALIA PREPARED BY: DLA Piper				
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis	Score
		<p>been some suggestion recently that the Government, regulators and the courts may be open to such developments.</p> <p>In December 2019, the Commonwealth Government made commitments as part of its response to the final report of the ACCC's Digital Platforms' Inquiry (<b>Digital Platforms' Inquiry</b>), to introduce certain changes to the Privacy Act, and to carry out an overall review and reform of the regime (scheduled in 2020-2021) (<b>Privacy Act Review</b>), including to widen the definition of 'personal information,' expand notification requirements, amend consent requirements and pro-consumer defaults, as well as introduce new direct rights of action for individuals - which could operate in tandem with a new statutory tort of privacy, although this is not yet confirmed.</p> <p>It is expected that new legislation will be prepared in the coming years to (at least) increase civil penalties for breach (to align with existing consumer law regime) and to introduce a binding online privacy code for social media and other online platforms. To date, no new legislation has been prepared by the Government. The wider scheduled Privacy Act Review is likely to be postponed also following current Covid-19 priorities.</p>		
2.2 Regulation of public authority access to private data	<p>The extent to which the <b>level of access legally permitted and conducted in practice</b> by public authorities to personal data (e.g. to secure disclosure of, or conduct surveillance on, private information for national security purposes or other reasons) can be regarded as a justifiable interference and is subject to safeguards equivalent to that within the EU, in light of legislation, practice and reported precedents. This will consider specifically whether the right of</p>	<p>The regulation of public authority access to personal information is covered in a number of legislative acts as set out below. In general, there is limited information available in respect of the number of access requests and the types of requests made to private data given that it relates generally to surveillance and law enforcement.</p> <p><b>Encryption Act</b></p> <p>Under the recently enacted, <i>Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018</i> (Cth) (<b>'AA' or 'Encryption' Act</b>) (which amends the <i>Telecommunications Act 1997</i> (Cth), a number of obligations are imposed on Designated Communications Providers (DCPs) to provide assistance and access to Australia's intelligence and security organisations in connection with encrypted communications services provided by those DCPs.</p>	<p>The Encryption Act is problematic for a few reasons. First, the notices issued under the Act (TCNs, TANs, TARs) are vague in terms of scope, and may therefore present challenges in terms of the 'quality of law' requirement for surveillance powers. Second, there is the possibility that notices could be used in a way that would directly undermine security of government access to</p>	4

STEP 2 JURISDICTIONAL ANALYSIS FOR: AUSTRALIA PREPARED BY: DLA Piper				
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis	Score
	<p>public authorities to access data is:</p> <p>(i) underpinned by a legal framework that is publicly available and sufficiently clear;</p> <p>(ii) carried out in pursuit of legitimate aims which are necessary and proportionate in a democratic society to safeguard important objectives as also recognised in EU/UK law (noting that proportionality involves balancing any interference with fundamental privacy rights with what are necessary and important public interests); and</p> <p>(iii) subject to adequate and effective oversight from courts or other independent authorities.</p> <p>The assessment will consider <b>pervasive surveillance activity</b> (across the destination country as a whole) and whether access can in practice be exercised by public authorities in light of legislation, legal powers, technical, financial and human resources at their disposal and of reported precedents.</p>	<p>A DCP is defined broadly and appears to be intended to apply to the full range of participants in the global supply chain, from carriers to over-the-top messaging providers. It includes:</p> <ul style="list-style-type: none"> <li>carriers (i.e. owners of telecommunications network infrastructure in Australia);</li> <li>carriage service providers (i.e. entities that sell telecommunications services delivered over a carrier's network in Australia);</li> <li>entities that manufacture or supply customer equipment (e.g. device headsets) for use, or likely to be used, in Australia; and</li> <li>entities that supply electronic services to end-users in Australia (e.g. websites, chat services, secure messaging applications, hosting services such as cloud and web hosting services, peer-to-peer sharing platforms and email), as well as entities which that facilitate, or provide services ancillary or incidental to any of the above. Notably, as drafted – and confirmed by the Department of Home Affairs – a notice may be served on an individual if that individual is a sole-trader and their own corporate entity.</li> </ul> <p>The legislation was rushed through Parliament by the Commonwealth Government and there are ongoing criticisms and challenges to the broad scope of the news laws and the wide powers conferred on relevant authorities, which are heightened in particular by ambiguous drafting, lack of effective judicial oversight or authorisation in many cases under the regime, and uncertainty around its overall intended purpose.</p> <p><i>Key Scope</i></p> <p>Under the Encryption Act, a DCP must comply with:</p> <ul style="list-style-type: none"> <li>compulsory technical assistance notices (<b>TANs</b>) and technical capability notices (<b>TCNs</b>) issued either by the Director-General of Security or the head of an interception agency (in the case of TANs) or the Attorney General (in the case of TCNs); and</li> </ul>	<p>transferred data (e.g. the removal of encryption).</p> <p>However, it is notable that the use of TANs or TCNs appears, in practice, to have been limited to date.</p> <p>More broadly, the Telecommunications Act does create a legal framework for law enforcement and intelligence agency interception of communications and access to communications data. This framework includes privacy protective controls in a number of areas (for example, application of powers to limited defined agencies). However, these controls could be more robust in some areas (for example, certain powers under the Act are warrantless, creating a potential issue with the 'subject to judicial oversight' requirement).</p> <p>It is notable that the Privacy Act regime extends (with exemptions / limitations) to law enforcement, in a manner which broadly parallels the Law Enforcement Directive approach in the EU.</p>	



STEP 2 JURISDICTIONAL ANALYSIS FOR: AUSTRALIA PREPARED BY: DLA Piper				
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis	Score
		<ul style="list-style-type: none"> <li>voluntary technical assistance requests ('TARs') to certain designated agencies (including the ASIO, Australian Secret Intelligence Service and Australian Signals Directorate).</li> </ul> <p>The TAN and TCN notices require DCPs to provide assistance to, or do certain listed 'acts of things', with relevant law enforcement and interception agencies. The 'acts of things' are broad lists narrowed only to safeguarding national security or assisting the enforcement of serious criminal offences of Australia or a foreign country. In the case of TARs a request can be made for any assistance – not limited to 'listed acts or things'. Although these are voluntary requests, the only stated limitation is that the request must relate to a 'relevant objective' of the requesting agency (e.g. safeguarding national security or assisting the enforcement of serious criminal offences in Australia or a foreign country).</p> <p>The Act prescribes that such notices and requests must take into account the legitimate interests of the provider - although it is unclear how this would be applied in practice - national security interests, the interests of law enforcement, the expectations of the community with respect to privacy and cyber security and the availability of other means of achieving the intended outcome, among other considerations. They must also be reasonable, proportionate, practicable and technically feasible.</p> <p>In the case of TCNs, there are some additional oversight measures requiring the AG to consult with the affected provider prior to issuing a notice and to determine procedures and arrangements relating to requests for technical capability notices.</p> <p>Concerns have however been raised on these compulsory notices about the lack of judicial oversight and authorisation prior to issuance, security issues, whether compliance is actually technically possible, as well as, in the case of TCNs, the requirement on a provider to build new capabilities to enable assistance to a law enforcement agency</p>	<p>However, along with the UK and the US, Australia participates in the 'five eyes' intelligence alliance, the details of which (as revealed in a number of public leaks), has created some degree of uncertainty about the proportionality of Australian surveillance activities.</p>	

STEP 2 JURISDICTIONAL ANALYSIS FOR: AUSTRALIA PREPARED BY: DLA Piper			
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis
		<p>with a 'listed act or thing' (the latter being likely intended to be used in connection with a TAN).<sup>2</sup></p> <p>Although the Government has declared that TANs and TCNs will not require a DCP to implement or build 'systemic weaknesses' in forms of electronic protection (i.e. backdoors), nor can they prevent a DCP from fixing identified weaknesses or 'systematic vulnerability', despite such assurances, the definition of 'systemic weakness' and 'systemic vulnerability' in the Encryption Act are broadly and ambiguously defined (as rushed late inclusions), and the risk of such back-door capability appears to remain a key concern.</p> <p>The Act is currently undergoing challenge by the Federal opposition through Parliament in the form of the <i>Telecommunications Amendment (Repairing Assistance and Access) Bill 2019</i>. This Bill includes proposed changes to the definitions of 'systemic weakness' and 'systemic vulnerability' to remove relevant ambiguity; new bars to certain requests which could create 'systematic vulnerabilities' (or back-doors) in the future; removal of non-exhaustive type language and also seeks to impose a requirement for clear judicial oversight and authorisation of TANs and TCNs prior to issue. The Bill is currently before the Senate.</p> <p>That said, despite the wide ambit of the Encryption Act and the controversial powers conferred on enforcement agencies, in practice, there have been no reported cases of TANs or TCNs being required by authorities (at least as at August 2020).<sup>3</sup></p> <p><b>Telecommunications Sector - TIA Act</b></p> <p>Applicable specifically to telecommunications providers, the <i>Telecommunications (Interception and Access) Act 1979 (TIA Act)</i> permits national security and law enforcement agencies to</p>	

<sup>2</sup> <https://www.theguardian.com/australia-news/2020/jul/09/australias-world-first-anti-encryption-law-should-be-overhauled-independent-monitor-says> and [https://www.inslm.gov.au/sites/default/files/2020-07/INSLM\\_Review\\_TOLA\\_related\\_matters.pdf](https://www.inslm.gov.au/sites/default/files/2020-07/INSLM_Review_TOLA_related_matters.pdf)

<sup>3</sup> <https://www.smh.com.au/politics/federal/encryption-powers-not-used-by-asio-afp-as-tech-companies-volunteer-help-20200807-p55jhl.html>

STEP 2 JURISDICTIONAL ANALYSIS FOR: AUSTRALIA PREPARED BY: DLA Piper			
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis
		<p>access information held by communications providers in the investigation of serious crime, including to obtain warrants to intercept communications and access stored communications and authorise the disclosure of data.</p> <p>The TIA Act includes a requirement for carriers, carriage service providers and ISPs to retain certain metadata for a period of 2 (two) years from its collection. The information which is required to be retained under the TIA Act includes names and addresses, the dates, times and duration of communications and locations at the start and end of calls. Metadata is considered to be personal information for the purpose of the Privacy Act insofar as it relates to an individual and, under the TIA Act, stored metadata must be encrypted. It expressly excludes the contents and substance of a communication and information that was obtained by the service provider only as a result of providing the service (which is intended to refer to internet browsing histories).</p> <p>Access to metadata is limited to defined agencies. However, with the exception of access to a journalist's data for the purpose of identifying a source, no warrant is required for relevant agencies to access stored metadata.</p> <p><b>Surveillance Devices Act (Cth) &amp; State Legislation</b></p> <p>The <i>Surveillance Devices Act</i> (2004) (Cth) governs the use of surveillance devices by public sector agencies, pursuant to which an eligible agency can apply for a warrant to use a surveillance device to investigate a relevant offence. At the state and territory level, there is also a patchwork of additional laws that regulate monitoring and surveillance, including the <i>Crimes (Surveillance Devices) Act, 2010</i> (ACT), <i>Surveillance Devices Act (Vic)</i>, <i>Surveillance Devices Act, 2007</i> (NT and NSW) all of which restrict the installation, use and retrieval of surveillance devices, as well as the <i>Workplace Surveillance Act 2005</i> (NSW) to regulate the use of camera, audio, computer surveillance and geographical tracking.</p>	

STEP 2 JURISDICTIONAL ANALYSIS FOR: AUSTRALIA PREPARED BY: DLA Piper				
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis	Score
		<p>There is currently the <i>Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020</i> which is proposed to amend the <i>Surveillance Devices Act (2004)</i> in respect of particular crimes (ie, identity theft, child abuse etc) which will permit law enforcement to disrupt data, collect intelligence on networks and take over accounts of individuals.</p> <p>While each state differs, generally speaking, the use of surveillance and/or listening often requires individuals' consent and/or notification. However, exceptions may apply, including where the use of such a device is necessary to protect a party's lawful interests, for an enforcement-related purpose, or where it is in the public interest. Specific obligations may also be impacted by whether the person using the surveillance or listening device is a party to the activity or conversation and the location of the activity or conversation (e.g. in a private home or space).</p>		
2.3 Regulatory supervision	<p>The extent to which courts, regulators and/or supervisory authorities enforce the rule of law and/or rights guaranteed in relation to the protection of data in an independent and effective manner, with evidence of meaningful resources and enforcement activity.</p>	<p>The Commissioner is responsible for the enforcement of the Privacy Act and the APPs, which confer on the Commissioner and the Office of the Australian Information Commissioner (OAIC) a range of privacy regulatory powers.</p> <p>The Commissioner must act fairly, independently and in accordance with principles of natural justice (or procedural fairness) when investigating any alleged interference with privacy or other privacy breach either following a direct complaint, or on the Commissioner's own initiative through a Commissioner initiated investigation.</p> <p>Allegations of contravention are given individual consideration and have regard to all relevant circumstances. The OAIC must also act in accordance with the Legal Services Directions, 2005.</p> <p>Enforcement powers available to the Commissioner range from less serious to more serious regulatory action, including carrying out investigations, making determinations on a complaint, accepting enforceable undertakings, bringing proceedings to enforce determinations and enforceable undertakings, seeking injunctions and applying to the Courts for civil penalty orders for serious and repeated interferences with privacy. It is open to the Commissioner to use a combination of privacy regulatory powers to address a particular matter.</p>	<p>The Commissioner appears to be an independent regulator, with a broad range of powers essentially equivalent to those of an EU supervisory authority. The total extent of its powers (including in respect of its ability to penalize infringements via fines) may not be as robust as for an EU authority, although this is to some extent mitigated by the parallel activity of the ACCC. However, the Commissioner is relatively inactive and the value of fines issued to date are low.</p>	3

STEP 2 JURISDICTIONAL ANALYSIS FOR: AUSTRALIA PREPARED BY: DLA Piper				
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis	Score
		<p>After investigating a complaint, the Commissioner may attempt, by conciliation, to settle, or it may dismiss the complaint or find the complaint substantiated and make determinations including declarations that the organization rectify its conduct or that the organization redress any loss or damage suffered by the complainant (which can include non-pecuniary loss such as awards for stress and/or humiliation). If a determination is made, either of the Commission or an the individual can commence proceedings to enforce the determination</p> <p>Furthermore, fines of up to AU\$420,000 for an individual and AU\$2.1 million for corporations may be requested by the Commissioner and imposed by the Courts for serious or repeated interferences with the privacy of individuals. These penalties are regulatory fines and cannot be used to compensate individuals. As noted above, it is expected that the Privacy Act will be amended in coming years to (at least) increase civil penalties for breach (to align with existing consumer law regime) and give the Commissioner powers to impose fines of up to ~AU60,000 without the need for court proceedings.</p> <p>The Commissioner is relatively active in its pursuit of determinations<sup>4</sup> and enforceable undertakings<sup>5</sup> against Australian businesses, although its preferred approach is to work with entities to encourage and facilitate compliance with an entity's obligations under the Privacy Act before taking enforcement action. Further information on determinations and enforceable undertakings are available in footnotes 3 and 4 – the OAIC publishes recent determinations and enforceable undertakings on its website. The determinations and enforceable undertakings relate to breaches of the Privacy Act and with interfering with individual's privacy.</p> <p>For example, the Department of Health gave an enforceable undertaking to the OAIC after publishing details online that were reasonably identifiable that it would conduct an independent review</p>		

<sup>4</sup> <https://www.oaic.gov.au/privacy/privacy-decisions/privacy-determinations/>

<sup>5</sup> <https://www.oaic.gov.au/privacy/privacy-decisions/enforceable-undertakings/>

STEP 2 JURISDICTIONAL ANALYSIS FOR: AUSTRALIA PREPARED BY: DLA Piper				
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis	Score
		<p>into its handling of personal information and then implement any recommendations arising out of that review.</p> <p>Statistics on the number of determinations or average awards are not made public.</p> <p><b>Additional Regulator Action &amp; Courts</b></p> <p>Most recently, the Australian Competition and Consumer Commission (ACCC) has taken two separate Federal Court proceedings under Section 18 of the Australian Consumer Law (ACL) against Google LLC alleging that it had engaged in misleading and deceptive conduct in its collection of users' location data, and (as recently as last month) failing to disclose changes to its privacy policy about the way it collects and uses consumer personal information.<sup>6</sup> This is the first time a regulator, other than the OALC, has taken a direct action against an organisation for a breach of privacy practices. The relative significant of these cases, in addition to the high profile plaintiff, is having a more active and better resourced regulator in the ACCC and the increased penalties under the ACL that can be imposed for breach – the latter recently raised to the greater of AUD10 million, or 3 times the value of any benefit gained by the entity through misusing personal information, or 10% of the entity's annual domestic turnover. These suits against Google are expected to be the first in a multiple enforcement actions to be taken by the ACCC (in particular in the pursual of competition and consumer issues relating to digital platforms) on the handling and use of personal information and the privacy practices of Australian businesses.</p> <p>As part of its Privacy Act Review (cited above), the Commonwealth Government has also proposed to increase the penalties payable for serious or repeated interferences with privacy under the Privacy Act to align with the scope of penalties under ACL (as noted above). However, as yet no legislation has been introduced to implement this proposal.</p>		

<sup>6</sup> <https://www.accc.gov.au/media-release/google-misled-consumers-about-the-collection-and-use-of-location-data>



STEP 2 JURISDICTIONAL ANALYSIS FOR: AUSTRALIA PREPARED BY: DLA Piper				
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>7</sup>	Comparative analysis	Score
2.4 Rights of redress	The extent to which individuals can easily and effectively <b>enforce rights and seek redress</b> by raising complaints, claims and / or appeal and enforce decisions in relation to both data protection infringements and public disclosure / surveillance activity through judicial and/or administrative processes (e.g. help from local data protection authorities) including whether redress mechanisms can be effectively applied in practice and are not thwarted by local laws and/or practices. This section will also consider whether data subjects can secure self-help remedies – e.g. right to secure access to or require erasure of personal data files, and whether the breach of local laws can be effectively invoked and relied on by individuals.	<p>As noted above, an individual's right of recourse under the Privacy Act largely consists of a right to complain to the Commissioner about an act or practice that may interfere with their privacy, to apply for enforcement of a determination made by the Commissioner, or to seek an injunction in respect of conduct that breaches the Privacy Act. See further under footnotes 3 and 4 further information of recent determinations and enforcement actions undertaken by the OAIC. There are no current actions in relation to public disclosure / surveillance activity. These primarily relate to infringements due to breaches of the Privacy Act. For example, an enforceable undertaking was provided by Wilson Asset Management to the OAIC in respect of its collection of personal information which was not necessary for its functions and activities.<sup>7</sup></p> <p>In addition to rights of complaint to the Commissioner, individuals have rights under the Privacy Act to access their personal information – subject to certain exemptions, an APP entity must provide access within a reasonable period (usually 30 days). Individuals also have rights to request the correction of inaccurate information held about them, and to stop receiving unwanted direct marketing (<i>SPAM Act</i>). Under the <i>Freedom of Information Act</i> (1982), an individual can also request access to records (including personal information) held about them from applicable public sector agencies.</p> <p>Further, the Consumer Data Right Act provides for an additional consumer-directed data portability mechanism which allows individuals to access certain data held about, or related to, them by designated organisations, and direct that data to be transferred to relevant accredited third parties. This right enhances existing rights of access granted to individuals under APP 12 in the Privacy Act. The CDR applies to the banking sector currently only – but is intended to be rolled out to all sectors, with energy and telecoms next. It applies not only to personal information of individuals, but also to business consumers and related products and as such provides a mechanism for accredited (private sector) organisations in the relevant sectors to</p>	<p>The individual right of complaint under the Privacy Act provides for a clear mechanism of redress, and (as in the EU) the Commissioner can take account of both material and non-material damage. However, as a mechanism of redress, the right of complaint is not as direct as the statutory right to compensation regime that exists under the GDPR. Ultimately a complaint may lead to compensation, but the route is not as direct and applications may be required to enforce a determination made by the Commissioner.</p> <p>As noted above, whilst data subject rights exist under Australian law, these are limited and not as extensive as in the EU.</p>	3

<sup>7</sup> <https://www.oaic.gov.au/privacy/decisions/enforceable-undertakings/wilson-asset-management-enforceable-undertaking/>



STEP 2 JURISDICTIONAL ANALYSIS FOR: AUSTRALIA PREPARED BY: DLA Piper				
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis	Score
2.5 International treaties	<p>The extent to which the country has concluded <b>international treaties</b> and related commitments on handling of personal data to support the safeguarding of data – this will include consideration both of the existence of:</p> <p>(i) international treaties that relate to the protection of data generally consistent with principles enshrined in EU/UK law, and</p> <p>(ii) any specific arrangements concluded to provide safeguards in relation to country to country transfers (e.g. UK-U.S. Bilateral Data Access Agreement which brings into effect the 'quashing' provisions of 18 USC § 2703(h)(2))</p>	<p>access, with consent, a broader range of information within the designated sectors than is provided for by APP 12 .</p> <p>Rights of individual access to appeal under the Encryption Act (in the circumstances where notices are issued to individuals, e.g. as sole-traders) are generally limited to re-assessment or oversight by technical officers, or the Ombudsman, with limited judicial review.</p> <p>Australia has not as yet concluded international treaties of the kind noted, but the <i>Telecommunications Legislation Amendment (International Production Orders) Bill 2020</i> was released in March 2020, and is currently before the Federal Parliament for review.</p> <p>The Bill proposes to amend the TIA by establishing a framework to give effect to "future bilateral and multilateral agreements for reciprocal cross-border access to electronic information and communications data" .</p> <p>The Bill is a pre-condition to obtain (a first) proposed bilateral agreement with the USA in order to implement the <i>US CLOUD Act</i> (similar to the UK-US Bilateral Data Access Agreement executed in 2019).</p> <p>If legislated, the act would compel Australian 'designated communications providers' (as defined there) (<b>DCPs</b>) to hand over electronic information, including stored communications and telecommunications data to, for example, US authorities, and vice-versa, if presented with international production orders for interception (e.g. a warrant or subpoena) by Australian law enforcement agencies or the courts. It would also allow them to be able to respond to orders from the US for access to electronic information, although providers may not be obligated to respond to these requests. The direct nature of the proposed issue on DCPs bypasses existing mutual assistance access processes between Australia and other foreign governments (e.g. as established under the <i>Mutual Assistance in Criminal Matters Act, 1987</i>).</p> <p>The Bill is currently before the Parliamentary Joint Committee on Intelligence and Security for review, but has been delayed by Covid-19 priorities.</p>	<p>There are no international treaties comparable to Convention 108+ to note. However, the OAIC's participation in the APEC Privacy Framework and the Cross-border Privacy Enforcement Arrangement does provide for some degree of additional protection.</p>	3

STEP 2 JURISDICTIONAL ANALYSIS FOR: AUSTRALIA PREPARED BY: DLA Piper				
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis	Score
		<p>Separately, the OAIC is a member of a number of non-binding / enforceable collaboration frameworks and co-operation arrangements, including:</p> <ul style="list-style-type: none"> <li>• APEC Privacy Framework on information privacy protection across member economies;</li> <li>• Cross-border Privacy Enforcement Arrangement - a framework for privacy regulators to cooperate, and to seek information and advice from each other on cross-border enforcement matters;</li> <li>• Global Cross Border Enforcement Cooperation Arrangement since October 2015 to facilitate cooperation and collaboration in the enforcement activities of global privacy enforcement authorities.</li> </ul> <p>The OAIC and Commissioner also engage in certain global privacy networks, including the Asia Pacific Privacy Authorities Forum (APPA), the OECD Global Privacy Enforcement Network (GPEN) and the APEC Cross Border Privacy Enforcement Arrangement.</p>		
<b>Total</b>				16

## STEP 2: ASSESSMENTS OF GENERAL LAWS AND PRACTICES IN THE DESTINATION COUNTRY

## INDIA

Score	Features
1	High level of safeguards in place, essentially equivalent to the level available in the EEA/UK
2	High level of safeguards in place, but below the level of those available in the EEA/UK
3	Some safeguards in place, but materially below the level of those available in the EEA/UK
4	Very limited safeguards in place, significantly below the level of those available in the EEA/UK
5	No safeguards in place (lowest level of equivalence)

Current as of 22<sup>nd</sup> Sept. 2021

STEP 2 JURISDICTIONAL ANALYSIS FOR INDIA PREPARED BY: J. Sagar Associates (India) and DLA Piper				
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis	Score
2.1 Regulation on the processing of personal data	The extent to which local laws offer clear, precise and accessible legal safeguards to the processing of personal data equivalent to the protections offered in the EEA / UK. This will include an analysis of the local laws and practices, including constitutional rights to privacy and how those laws apply both to the data importer but also third parties (e.g. law enforcement) who may seek to	<b>Right to privacy is a constitutional right</b> The right to privacy is a recognized constitutional right in India. In 2017, the apex court, the Supreme Court of India, declared that right to privacy is a constitutional right and is part of Article 21 (Protection of life and personal liberty). Fundamental rights (including right to privacy) may only be enforced against the state or instrumentality of state. The term 'state' includes the Parliament, the executive and the Judiciary. As such, an act of parliament (for e.g. a law or direction) or executive (for e.g. investigating officer) which violates fundamental right may give the person right to approach the courts to strike down such law or executive action. <b>Legislative framework</b>	There are very limited safeguards in place to protect personal data. Although the PDP Bill has been introduced, it has been delayed due to Covid-19 and has not come into law yet. <sup>2</sup> As such, there is no equivalent legislative instrument governing data protection, (other than what is contained in the Privacy Rules), and there is no specific regulatory authority in charge of enforcement. However, the right	4

<sup>1</sup> The assessment will be based first on legislation publicly available. Sources and information should be relevant, objective, reliable, verifiable and publicly available or otherwise accessible.

<sup>2</sup> DLA Piper can also provide a jurisdictional analysis for India based on the passing of the PDP Bill in its current format.

STEP 2 JURISDICTIONAL ANALYSIS FOR INDIA PREPARED BY: J. Sagar Associates (India) and DLA Piper			
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis
	<p>secure access to the data following transfer.</p> <p>In this context, note the EEA / UK has a developed law that specifically recognises legal rights to protection of "personal data" consistent with the principles of data protection set out in OECD Convention 108+.</p> <p>In particular, the assessment will consider:</p> <p>(i) whether there are any relevant local laws laying down requirements to disclose personal data to public authorities or granting such public authorities powers of access to personal data;</p> <p>(ii) where relevant local laws formally meet EEA /UK standards on fundamental rights and freedoms and the necessity and proportionality of restrictions, whether the practices of public authorities clearly indicate that they do not normally apply/comply with the legislation that governs, in principle, their activities; and</p> <p>(iii) where relevant local law may be lacking, are there any indications of practices in force that are incompatible with EEA/UK law.</p>	<p>As of today's date, India has a very skeletal framework on privacy and data protection. The Information Technology Act, 2000 (<b>IT Act</b>), and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (<b>Privacy Rules</b>) issued under Section 43A of the IT Act that govern data protection in India.</p> <p>India does have on the anvil the Personal Data Protection Bill (<b>PDP Bill</b>), which will encapsulate the law on the subject. It is yet to be passed by the Indian Parliament. In anticipation of the PDP Bill being passed by Parliament, which may get further delayed due to the COVID-19 pandemic, the Indian Government is passing orders emphasizing the need for data sovereignty, guarding against 'data imperialism' by foreign technology players and ensuring that data generated by Indian citizens is utilised for their welfare.</p> <p><b>Subject matter of the law</b></p> <p>A body corporate or any person who on behalf of a body corporate collects, receives, possess, stores, deals or handles information of an information provider has to comply with the requirements set out under the IT Act and Privacy Rules. There are different sets of compliances which apply to entities engaging in personal information and sensitive personal data or information. By way of background, personal information means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person. Sensitive Personal Data or Information (SPDI) includes such personal information which consists of information relating to (i) password; (ii) financial information such as bank account or credit card or debit card details; (iii) health data; (iv) sexual orientation; (v) medical records and history; (vi) biometric information. For completeness we have set out below the compliance requirements in connection with both sets of data.</p> <p><b>Summary of key compliance requirements under the Privacy Rules</b></p> <p><b>Privacy Policy:</b> Every entity collecting, receiving, possessing, storing, dealing or handling data and information, is required to have a privacy policy for handling of, or dealing in, personal information, including SPDI and to ensure that the same is available to the providers of such information.</p> <p><b>Consent:</b> The entity collecting SPDI is required to obtain consent, in writing, from the provider of SPDI. The provider of information should have knowledge of the fact that the information is being collected, the purpose for which the information is being</p>	to privacy is recognized by the Indian constitution, offering some alignment with the 'constitutional' rights to privacy and data protection under the Charter and the ECHR.

STEP 2 JURISDICTIONAL ANALYSIS FOR INDIA PREPARED BY: J. Sagar Associates (India) and DLA Piper			
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis
		<p>collected, intended recipients of information, and name and address of the agency collecting the information and the agency that will retain the information.</p> <p><u>Review and Opt-out:</u> Providers of SPDI are entitled to (a) review the information they provide and ensure that any Personal Information or SPDI found to be inaccurate or deficient is corrected or amended as feasible; and/or (b) withdraw consent to use the information.</p> <p><u>Transfer and Disclosure:</u> SPDI may only be transferred by a relevant entity to any other entity in India, or located in any other country that ensures the same level of data protection that is adhered to by the relevant entity in India. Further, any disclosure of SPDI to a third party would require prior permission of the provider of SPDI, or be necessary for the performance of a lawful contract between the body corporate and the provider of SPDI. <b>(Data Transfer Obligations)</b></p> <p><u>Security Standards:</u> An entity collecting/ handling SPDI is required to comply with reasonable security practices and procedures in relation to SPDI, the minimum standard being the IS/ISO/IEC27001 standard on 'Information Technology – Security Techniques – Information Security Management System – Requirements'.</p> <p><u>Grievance Officer:</u> The Privacy Rules require each entity collecting/ handling SPDI to address any discrepancies and grievances of the provider of the information, in a time bound manner. For this purpose, the entity collecting SPDI must designate a 'grievance officer' and publish his name and contact details on its website.</p> <p>The Privacy Rules provide that an entity handling SPDI is exempted from obtaining the consent of the provider of information, if disclosed to a government authority pursuant to an order issued in writing. The government authority is required to state in such order that it will not be published or shared with anyone.</p> <p><b>Marketing</b></p> <p>Telemarketing by way of SMS and voice calls is a regulated activity. Only a telemarketer which is registered with access service providers under the Telecom Commercial Customer Preference Regulations, 2018 (2018 Regulations) may provide telemarketing services.</p> <p>The 2018 Regulations apply only to voice calls and SMS, and not to marketing communication by way of e-mail or direct messaging on social media.</p> <p>While there are laws which regulate unsolicited communication, do note that the enforcement is not as effective or structured. As a result of which, while some</p>	

STEP 2 JURISDICTIONAL ANALYSIS FOR INDIA PREPARED BY: J. Sagar Associates (India) and DLA Piper			
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis
		<p>telemarketers have been penalized in the past, the enforcement on these issues continues to be ineffective.</p> <p>No person may be subjected to unsolicited commercial communication without its consent.</p> <p>While the Privacy Rules do not deal directly with marketing practices, this may become relevant in the context of handling of personal information. The Privacy Rules regulate collection, dissemination, storage of personal information and SPDI. Personal Information has been defined to mean any information that relates to a natural person which, either directly or indirectly, in combination of information available or likely to be available with a body corporate, is capable of identifying such person. SPDI has been of a person has been defined as such Personal Information relating to, amongst other things, financial information such as bank account or credit card or debit card or other payment instrument details, as well as biometric information (including Aadhaar). Notably, the Privacy Rules applies to data of individuals and does not intend to cover data of corporates.</p> <p>For completeness please note that there are no specific laws governing online marketing in India, which may be applicable to private service providers. Having said that, courts in India, while acknowledging the lack of specific anti-spam legislation with respect to emails or electronic communications, have invoked traditional principles of tort, trespass and nuisance in cases involving unsolicited commercial emails. The said principles could be applied to any form of marketing practice. Hence, it is advisable to ensure that all recipients of such communications are provided the option to opt out or unsubscribe such communication.</p> <p><b>Data Retention</b></p> <p>Information which may be classified as SPDI may not be retained for a period longer than necessary for the purpose for which they are collected, or as required under applicable law.</p> <p>Generally, as a matter of practice, companies preserve other data for a period of 3 years after their 'relationship'.</p> <p>Payroll and tax related documents and records of employees/ex-employees may be maintained for a period of 8 years from the end of the 'employment relationship', which is the maximum period for which an income tax assessment may be re-opened.</p>	



STEP 2 JURISDICTIONAL ANALYSIS FOR INDIA PREPARED BY: J. Sagar Associates (India) and DLA Piper				
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis	Score
2.2 Regulation of public authority access to private data	<p>The extent to which the <b>level of access legally permitted and conducted in practice</b> by public authorities to personal data (e.g. to secure disclosure of, or conduct surveillance on, private information for national security purposes or other reasons) can be regarded as a justifiable interference and is subject to safeguards equivalent to that within the EEA / UK, in light of legislation, practice and reported precedents. This will consider specifically whether the right of public authorities to access data is:</p> <p>(i) underpinned by a legal framework that is publicly available and sufficiently clear;</p> <p>(ii) carried out in pursuit of legitimate aims which are necessary and proportionate in a democratic society to safeguard important objectives as also recognised in EU/UK law (noting that proportionality involves balancing any interference with fundamental privacy rights with what are necessary and important public interests); and</p>	<p>On the occurrence of any offence or for the purposes of investigation, Indian law enforcement entities may gain access to personal data, as illustrated below.</p> <p><b>Judicial</b></p> <p>If the courts in India believe that disclosure of information is necessary for greater public interest, or if the grounds specified under the empowering legislations are satisfied, they may order such disclosure, following due process prescribed under such legislation. These disclosure orders may emanate from an action brought against the company collecting the information and is involved in certain types of offences. Certain matters wherein the relief is dependent on disclosure of data, the courts may direct the parties to provide such information as may be required.</p> <p><b>CERT-IN</b></p> <p>Ministry of Electronics and Information Technology of the Government of India has constituted the Indian Computer Emergency Response Team (<b>CERT-IN</b>). CERT-IN is the agency responsible for dealing with cyber security attacks and similar activities. While the activism of CERT-IN is still at a nascent stage, the law does require the service providers to report cyber security incident to CERT-IN within reasonable time of occurrence to have scope for timely action. Follow on requisitions by CERT-IN may require disclosure of data in possession of the companies. Please note, CERT-IN does not have enforcement powers.</p> <p><b>Other Agencies</b></p> <p>Do note that there are several agencies which have investigative powers and may access records and information of an entity to probe a matter in relation to <b>money</b> laundering, tax evasion and financial fraud. For instance, (i) the Companies Act, 2013 empowers Serious Fraud Investigation Officer to investigate affairs of an Indian company in case of suspected fraud; and (ii) the Financial Intelligence Unit- India may also investigate and ask for information if the offence relates to money laundering. Specialized agencies/departments which may be investigating an issue pertaining to an offence may also have access to information. These agencies include:</p> <ul style="list-style-type: none"> <li>▪ Department of Telecommunications (DoT)</li> <li>▪ Ministry of Electronics and Information Technology (MeitY)</li> <li>▪ Research and Analysis Wing (RAW)</li> <li>▪ Intelligence Bureau</li> </ul>	<p>The IT Act provides various grounds for interception and surveillance in India, including for surveillance of metadata. The grounds are broad and include 'for the investigation of any offence'. Many official bodies (both central and state agencies) have been granted surveillance rights across a wide range of sectors.</p>	4



STEP 2 JURISDICTIONAL ANALYSIS FOR INDIA PREPARED BY: J. Sagar Associates (India) and DLA Piper			
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis
	<p>(iii) subject to adequate and effective oversight from courts or other independent authorities.</p> <p>The assessment will consider <b>pervasive surveillance activity</b> (across the destination country as a whole) and whether access can in practice be exercised by public authorities in light of legislation, legal powers, technical, financial and human resources at their disposal and of reported precedents.</p>	<ul style="list-style-type: none"> <li>▪ Narcotics Control Bureau</li> <li>▪ Directorate of Revenue Intelligence (DRI)</li> <li>▪ Central Economic Intelligence Bureau</li> <li>▪ Central Bureau of Health Intelligence</li> <li>▪ Defence Intelligence Agency</li> <li>▪ Joint Cipher Bureau</li> <li>▪ Directorate of Income Tax (Intelligence and Criminal Investigation)</li> <li>▪ Directorate General of Income Tax Investigation</li> </ul> <p>Additionally, certain legislation such as the IT Act, Indian Telegraph Act, 1872, Code of Criminal Procedure, 1973 and Code of Civil Procedure set out certain scenarios under which data may be accessed by authorities specifically empowered under these legislations, in accordance with procedure laid down thereunder.</p> <p><b>Regulatory</b></p> <p>If an entity is regulated by regulators such as Reserve Bank of India (RBI) or Securities Exchange Board of India (SEBI) or is servicing a regulated entity, they may be required to disclose data on account of a regulatory action. The aforesaid regulatory action refers to a regulator's (such as RBI or SEBI's) ability to retrieve information by conducting an audit or inspection. This may be done by invoking the audit right which is mandatorily required to be built in the outsourcing agreements.</p> <p><b>Proportionality</b></p> <p>Typically, judicial and executive actions are proportional in nature. Government will not seek unnecessary information which is not linked to the case or offence.</p> <p>As such, the courts may set aside the Government's request for information, if it believes that such an exercise is not necessary.</p> <p><b>Interception / Surveillance by Public Authorities</b></p> <p>The IT Act provides various grounds for interception and surveillance in India.</p> <p>Under Section 69 of the IT Act, Government (both central or state) may direct, by order, any agency of Government to intercept or monitor or decrypt any information through any computer resource, where it is necessary / expedient to do so and "in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for</p>	

STEP 2 JURISDICTIONAL ANALYSIS FOR INDIA PREPARED BY: J. Sagar Associates (India) and DLA Piper				
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis	Score
		<p><i>preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence</i>”;</p> <p>Whilst these grounds provide a purpose limitation, the scope is widely expanded by the inclusion of “<i>for the investigation of any offence</i>”.</p> <p>The subscriber or intermediary (any or person in charge of the computer resource) must extend <i>all</i> facilities and technical assistance to the competent authority (when called upon) to enable such actions to be undertaken. Failure to assist the competent authority is punishable by a fine and imprisonment of up to 7 years.</p> <p>Further, Section 69A of the IT Act empowers the Central Government or any of its officers to direct, by order, any agency of Government or intermediary to block public access to any information generated, transmitted, received, stored or hosted in any computer resource.</p> <p>In addition, Section 69B of the IT Act empowers the Central Government to authorise any government agency to monitor and collect traffic data or information through any computer resource for the purpose of cyber security and “<i>for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country</i>”.</p> <p>The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 (the <b>IT Interception Rules</b>) introduced safeguards for directions under Section 69 and specified:</p> <ul style="list-style-type: none"> <li>• who may issue a direction (i.e. the competent authority) and in what circumstances;</li> <li>• the duration of any direction;</li> <li>• to whom the data may be disclosed;</li> <li>• the bimonthly oversight by the Review Committee;</li> <li>• the confidentiality obligations of intermediaries (or persons in charge of the requested data); and</li> <li>• the destruction of records and directions for interception, monitoring and decryption of information within prescribed time periods.</li> </ul> <p>Further, a competent authority shall only issue any direction to intercept information only when alternative means of interception are not available.</p>		

STEP 2 JURISDICTIONAL ANALYSIS FOR INDIA PREPARED BY: J. Sagar Associates (India) and DLA Piper			
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis
		<p>The Information Technology (Procedure and safeguard for Monitoring and Collecting Traffic Data or Information) Rules 2009 laid down rules on the directions for monitoring and collection of traffic data. These rules contain similar safeguards and procedure to those set out above in the IT Interception Rules. In addition, a competent authority may issue a direction for monitoring for the following purposes related to cyber security:</p> <ul style="list-style-type: none"> <li>• forecasting of imminent cyber incidents;</li> <li>• monitoring network application with traffic data or information on computer resource</li> <li>• identification and determination of viruses or computer contaminant;</li> <li>• tracking cyber security breaches or cyber security incidents;</li> <li>• tracking computer resource breaching cyber security or spreading virus or computer contaminants;</li> <li>• identifying or tracking of any person who has breached, or is suspected of having breached or being likely to breach cyber security;</li> <li>• undertaking forensic of the concerned computer resource as a part of investigation or internal audit of information security practices in the computer resources;</li> <li>• accessing a stored information for enforcement of any provisions of the laws relating to cyber security for the time being in force; and</li> <li>• any other matter relating to cyber security.</li> </ul> <p>While seeking disclosure of data, the authorities would have to demonstrate and justify the necessity for seeking such data and follow the principles laid down by the Indian Supreme Court in the case of Justice K.S.Puttaswamy v. Union of India.</p> <p>In this case, the court held that any state action that infringes the right of privacy (which is protected as part of the right to life and personal liberty under the Indian Constitution) will only be lawful if that infringement is reasonable, legitimate and proportionate. This means that any measures taken by the authorities will only be lawful if they meet the following requirements:</p> <ul style="list-style-type: none"> <li>• the action should be authorized by law;</li> <li>• there should be a legitimate aim for taking such an action;</li> </ul>	

STEP 2 JURISDICTIONAL ANALYSIS FOR INDIA PREPARED BY: J. Sagar Associates (India) and DLA Piper				
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis	Score
		<ul style="list-style-type: none"> <li>the action should not be disproportionate and the need for such interference should be justifiable; and</li> <li>law enforcement and national security agencies must follow due process to ensure there is no abuse of power.</li> </ul> <p>There is very limited public information available regarding the activities of these authorities in relation to law enforcement / national security authorities' powers, which makes it difficult to provide a definitive response on the practices of public authorities with regard to access to private data. There is no database available in India that sets out any statistics or research, either by governmental authorities or issued by NGOs, academic institutions or public authorities relating to practices of public authorities with regard to access to private data. Companies such as Twitter, Google etc. publish transparency reports on a regular basis, detailing the total number of government data requests received and actions taken in India. However, these reports only reflect how many requests these organizations have received, and do not provide any specific details.<sup>3</sup> Please find below a few links to transparency reports from:</p> <p>India does not have central or dedicated databases relating to public authorities' access relating to personal data. However, experience from private organisations in relation to requests received for data relating to on-going investigations, indicates that most requests have been regarding non-personal data or where personal data has been a sub-set of a larger set of data. Generally on-going investigations are with respect to Indian citizens, unless there are graver offences such as those against national security that are being investigated and certain specific data is involved in such investigation.</p>		
2.3 Regulatory supervision	The extent to courts, regulators and/or supervisory authorities, enforce the rule of	<p><b>Overview of penalties</b></p> <p>Section 43A of the IT Act requires that a body corporate possessing, dealing, handling any SPDI in a computer resource, pays damages by way of compensation</p>	There is not yet a specific supervisory authority in India which governs the enforcement	4

3

Please find below a few links to transparency reports from:

Google: [https://transparencyreport.google.com/user-data/overview?dlr\\_requests=authority.IN;time:&lu=dlr\\_requests](https://transparencyreport.google.com/user-data/overview?dlr_requests=authority.IN;time:&lu=dlr_requests)Twitter - <https://transparency.twitter.com/en/reports/countries/in.html>Facebook - <https://transparency.fb.com/data/government-data-requests/country/IN/>

STEP 2 JURISDICTIONAL ANALYSIS FOR INDIA PREPARED BY: J. Sagar Associates (India) and DLA Piper				
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis	Score
	law and/or rights guaranteed in relation to the protection of data in an independent and effective manner, with evidence of meaningful resources and enforcement activity.	<p>to the affected person if there is a wrongful loss or wrongful gain to any person on account of negligence in implementing and maintaining reasonable security practise to protect information of affected person.</p> <p>Further, Section 72A of the IT Act states that any person who while providing services under the terms of a lawful contract, has secured access to any material containing personal information about another person, with the intent of causing or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.</p> <p><b>Enforcement</b></p> <p>Strictly speaking, an issue in connection with IT Act cannot be adjudicated by any civil court. The IT Act empowers the Adjudicating Officer to decide on matters in relation to IT Act up to a certain threshold. Once the claim crosses this threshold, the complainant may approach a civil court. That said, in India, the High Courts and the Supreme Court have writ jurisdictions and aggrieved parties may approach the courts for violation of 'right to privacy'.</p> <p><b>Enforcement trend</b></p> <p>For completeness, do note that it may be a challenge to enforce the liability even if there is an actual violation. Risk of enforcement/liability is low due to two major reasons. First, there is no data protection authority or enforcement mechanisms under the IT Rules 2011, therefore any liability would begin with a claim by one of the aggrieved data subjects. Second, if a company had presence in India, it would be relatively easy for the data subjects to initiate proceedings against a company located locally. In our experience, the chances of such a company which has presence in India has a higher risk of getting sued.</p> <p>India does not have currently a data protection authority or a similar supervisory authority given the rudimentary data protection framework.</p>	of data protection laws, and this does not align with regulatory supervision in the EEA / UK. In relation to surveillance, individuals can approach the high courts if they suspect they have been subject to illegal surveillance.	
2.4 Rights of redress	The extent to which individuals can easily and <b>effectively enforce rights</b> and seek redress by raising complaints, claims and / or appeal and enforce decisions in relation to both data	<p><b>Overview of rights</b></p> <p>The extant law provides for certain rights to the data subject.</p> <p>Body corporates collecting SPDI should keep the data subject informed about: (i) the fact that the information is being collected; (ii) purpose of such collection; (iii) intended recipients; and (iv) the name and address of agencies collecting and</p>	Individuals in India do not have rights to pursue legal remedies in order to have access to personal data relating to them, or to obtain the rectification or erasure of such data. Currently, data	4



STEP 2 JURISDICTIONAL ANALYSIS FOR INDIA PREPARED BY: J. Sagar Associates (India) and DLA Piper				
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis	Score
	<p>protection infringements and public disclosure / surveillance activity through judicial and/or administrative processes (e.g., help from local data protection authorities) including whether redress mechanisms can be effectively applied in practice and are not thwarted by local laws and/or practices. This section will also consider whether data subjects can secure self-help remedies – e.g., right to secure access to or require erasure of personal data files, and whether the breach of local laws can be effectively invoked and relied on by individuals.</p>	<p>retaining such information. Further, a provider of such information may access information provided by it upon request.</p> <p>Other rights such as right to be forgotten are explicitly set out under the IT Act and enforceable against the government but not private bodies. However, there have been cases wherein the courts have recognized this right. However, these rights were examined mostly from a context of offences against women.</p> <p><b>Enforcement</b></p> <p>Body corporates are required to designate a grievance officer. This grievance officer shall address discrepancies that the providers of information may have. The body corporates are required to publish name and contact details of the grievance officer on its website. Typically grievance officers are the first points of contact when an individual wants to enforce their rights or seek redressal.</p> <p><b>Judicial Intervention</b></p> <p>A data subject may initiate judicial review proceedings in a constitutional court (High Court or Supreme Court) should it believe that the data disclosure is illegal, disproportionate, unwarranted, or is done in a procedurally improper manner.</p> <p>To elaborate, data subjects may apply to the constitutional courts to enforce their privacy rights under either Article 32 or Article 226 of the Indian Constitution. Article 32 and 226 of the Constitution (generally provides individuals the right to constitutional remedy against violation of constitutional rights) gives the Supreme Court and high courts extensive original jurisdiction to take enforcement action to protect an individual's fundamental rights, including his/her right to privacy.</p> <p>Separately, companies may challenge orders or injunctions—including a criminal order to disclose data—by approaching constitutional courts and invoking their extraordinary jurisdiction. Companies may invoke the writ jurisdiction of High Courts under Article 226 of the Constitution to challenge such orders.</p> <p>For instance, in the 2019 case of <i>Vinit Kumar v. Central Bureau of Investigations (CBI) and Ors.</i><sup>4</sup> the Bombay High Court ruled that the interception of a businessman's telephone calls by the CBI went beyond the legal authority to do so granted under Section 5(2) of the Telegraph Act, on the basis that there was no public emergency, nor was there any objective threat to public safety that justified the interception of the complainant's phone calls (even though he was</p>	<p>protection laws equivalent to the GDPR or the Law Enforcement Directive do not exist in India to give data subjects rights to access, erase, amend etc. their data, and to have these rights enforced in court.</p> <p>Therefore there are very limited rights of redress compared to the standards afforded by the GDPR. Note however that individuals may enforce their fundamental rights against the state, however enforcing their rights (including the right to privacy) against a private entity may require judicial intervention.</p>	

<sup>4</sup> Writ petition No. 2367 of 2019.

STEP 2 JURISDICTIONAL ANALYSIS FOR INDIA PREPARED BY: J. Sagar Associates (India) and DLA Piper				
Criteria	Assessment to carry out	Laws and practices in the destination country (please include sources of information) <sup>1</sup>	Comparative analysis	Score
2.5 International treaties	<p>The extent to which the country has concluded <b>international treaties</b> and related commitments on handling of personal data to support the safeguarding of data – this will include consideration both of the existence of:</p> <p>(i) international treaties that relate to the protection of data generally consistent with principles enshrined in EEA / UK law, and</p> <p>(ii) any specific arrangements concluded to provide safeguards in relation to country to country transfers (e.g. UK-U.S. Bilateral Data Access Agreement which brings into effect the 'quashing' provisions of 18 USC § 2703(h)(2))</p>	<p>suspected of bribing public servants). As a result, the court found that the interception did not have the "sanction of law," nor was the interception order issued for a legitimate aim (following the test in the Puttaswamy Case). Accordingly, the Court set aside the interception orders relied on by the CBI and ordered the destruction of copies of the intercepted messages or recordings. The Court also reiterated that these messages and recordings may not be treated as evidence during the complainant's criminal trial.</p> <p>India is a party to United Declaration of Human Rights and International Covenant on Civil and Political Rights.</p> <p>Right to privacy which is recognized under the two aforesaid instruments has been made part of the Indian constitution (Article 21).</p>	<p>There are no international treaties comparable to Convention 108+ to note. However, the ratification of the Universal Declaration of Human Rights does provide for some degree of additional protection.</p>	4
<b>Total</b>				<b>20</b>