

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") forms a part of the Agreement under which ServiceNow provides the Subscription Service and Professional Services, and is entered into by and between ServiceNow and Customer. This DPA reflects the parties' agreement with respect to the Processing of Personal Data submitted to the Subscription Service by Customer and is subject to all of the terms of the Agreement.

This DPA consists of three parts: (i) the main body of the DPA (Sections 1 to 10 and Annex 1); (ii) the Standard Contractual Clauses as Attachment 1; and (iii) the Data Security Guide as Attachment 2, all of which are expressly deemed incorporated in the Agreement by this reference.

In the event of any conflict between the terms of this DPA and the terms of the Agreement with respect to the subject matter herein, this DPA shall control. Any data processing agreements that may already exist between parties as well as any earlier version of the Data Security Guide which parties may have agreed to are superseded and replaced by this DPA in their entirety. All capitalized terms not defined in this DPA will have the meaning given to them in other parts of the Agreement.

INSTRUCTIONS FOR EXECUTING THIS DPA

1. This DPA has been pre-signed on behalf of ServiceNow and the Standard Contractual Clauses have been signed on behalf of the ServiceNow processing entities.
2. To fully execute this DPA, the Customer must:
 1. Complete the information in the signature box and sign on Page 9;
 2. Complete the information regarding the Data Exporter on Page 11;
 3. Complete the information in the signature box and sign the signature block for Data Exporter on Page 17;
 4. Complete the information in Appendix 1;
 5. Sign on Pages 21 and 22; and
 6. Submit a completed and fully executed DPA without changes to the printed terms to ServiceNow via privacy@servicenow.com.
3. Upon receipt by ServiceNow of a fully completed and duly executed DPA, this DPA shall become legally binding.

APPLICATION OF THIS DPA

1. If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement and the ServiceNow entity that is party to the Agreement is party to this DPA.
2. If the entity signing this DPA is not a party to the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA, and, to the extent applicable, Affiliates of such Customer will benefit under this DPA as set forth in Section 3.3 (Customer's Affiliates) below.

1. DEFINITIONS

1.1 "Affiliates" means any person or entity directly or indirectly Controlling, Controlled by or under common Control with a party to the Agreement, where **"Control"** means the legal power to direct or cause the direction of the general management of the company, partnership or other legal entity.

1.2 "Agreement" means the Order Form or Use Authorization or other signed ordering document, as applicable, between ServiceNow and Customer and the signed master agreement (if any) for the purchase of the Subscription Service.

1.3 "Data Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data. For purposes of this DPA, Data Controller is Customer and, where applicable, its Affiliates either permitted by Customer to submit Personal Data to the Subscription Service or whose Personal Data is Processed in the Subscription Service.

1.4 "Data Processor" means the natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Data Controller. For purposes of this DPA, Data Processor is the ServiceNow entity that is a party to the Agreement.

1.5 "Data Protection Laws" means all applicable laws and regulations regarding the Processing of Personal Data.

1.6 "Data Subject" means an identified or identifiable natural person.

1.7 "GDPR" means the European Union's General Data Protection Regulation (2016/679).

1.8 "Instructions" means Data Controller's documented data Processing instructions issued to Data Processor in compliance with this DPA.

1.9 "Personal Data" means any information relating to a Data Subject uploaded by or for Customer or Customer's agents, employees, or contractors to the Subscription Service as Customer Data.

1.10 "Process" or "Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.11 "Professional Services" means any consulting or development services provided by or on behalf of ServiceNow pursuant to an agreed statement of work or packaged professional services described or referenced in a signed ordering document.

1.12 "Sub-Processor" means any legal person or entity engaged in the Processing of Personal Data by Data Processor. For the avoidance of doubt, ServiceNow's colocation datacenter facilities are not Sub-Processors under this DPA.

1.13 "Subscription Service" means the ServiceNow software as a service (SaaS) offering ordered by Customer under an Order Form, Use Authorization or other signed ordering document between ServiceNow and Customer.

1.14 "Subscription Term" means the term of authorized use of the Subscription Service as set forth in the Order Form, Use Authorization or other ordering document signed by Customer and ServiceNow.

2. SCOPE OF THE PROCESSING

2.1 COMMISSIONED PROCESSOR. Data Controller appoints Data Processor to Process Personal Data on behalf of Data Controller to the extent necessary to provide the Subscription Service described in the Agreement and in accordance with the Instructions.

2.2 INSTRUCTIONS. The Agreement constitutes Data Controller's written Instructions to Data Processor for Processing of Personal Data. Data Controller may issue additional or alternate Instructions provided that such Instructions are: (a) consistent with the purpose and the scope of the Agreement; and (b) confirmed in writing by Data Controller. For the avoidance of doubt, Data Controller shall not use additional or alternate Instructions to alter the scope of the Agreement. Data Controller is responsible for ensuring its Instructions to Data Processor comply with Data Protection Laws.

2.3 NATURE, SCOPE AND PURPOSE OF THE PROCESSING. Data Processor shall only Process Personal Data in accordance with Data Controller's Instructions and to the extent necessary for providing the Subscription Service and the Professional Services, each as described in the Agreement. Data Controller

acknowledges that all Personal Data it instructs Data Processor to Process for the purpose of providing the Professional Services must be limited to the Customer Data Processed within the Subscription Service.

2.4 CATEGORIES OF PERSONAL DATA AND CATEGORIES OF DATA SUBJECTS. Data Controller may submit Personal Data to the Subscription Service as Customer Data, the extent of which is determined and controlled by Data Controller in its sole discretion and is further described in Appendix 1.

3. DATA CONTROLLER

3.1 COMPLIANCE WITH DATA PROTECTION LAWS. Data Controller shall comply with all of its obligations under Data Protection Laws when Processing Personal Data.

3.2 SECURITY RISK ASSESSMENT. Data Controller agrees that in accordance with Data Protection Laws and before submitting any Personal Data to the Subscription Service, Data Controller will perform an appropriate risk assessment to determine whether the security measures within the Subscription Service provide an adequate level of security, taking into account the nature, scope, context and purposes of the processing, the risks associated with the Personal Data and the applicable Data Protection Laws. Data Processor shall provide Data Controller reasonable assistance by providing Data Controller with information requested by Data Controller to conduct Data Controller's security risk assessment. Data Controller is solely responsible for determining the adequacy of the security measures within the Subscription Service in relation to the Personal Data Processed. As further described in Section 7.1 (Product Capabilities) of the Data Security Guide, the Subscription Service includes, without limitation, column level encryption functionality and role-based access control, which Data Controller may use in its sole discretion to ensure a level of security appropriate to the risk of the Personal Data. For clarity, Data Controller may influence the scope and the manner of Processing of its Personal Data by its own implementation, configuration (i.e., different types of encryption) and use of the Subscription Service, including any other products or services offered by ServiceNow and third-party integrations.

3.3 CUSTOMER'S AFFILIATES. The obligations of Data Processor set forth herein will extend to Customer's Data Controller Affiliates to which Customer provides access to the Subscription Service or whose Personal Data is Processed within the Subscription Service, subject to the following conditions:

3.3.1. COMPLIANCE. Customer shall at all times be liable for its Affiliates' compliance with this DPA and all acts and omissions by a Data Controller Affiliate are considered acts and omissions of Customer; and

3.3.2. CLAIMS. Customer's Data Controller Affiliates will not bring a claim directly against Data Processor. In the event a Data Controller Affiliate wishes to assert a valid legal action, suit, claim or proceeding against Data Processor (a "**Data Controller Affiliate Claim**"): (i) Customer must bring such Data Controller Affiliate Claim directly against Data Processor on behalf of such Data Controller Affiliate, unless Data Protection Laws require that Data Controller Affiliate be party to such Data Controller Affiliate Claim; and (ii) all Data Controller Affiliate Claims will be considered claims made by Customer and are at all times subject to any aggregate limitation of liability set forth in the Agreement.

3.3.3. DATA CONTROLLER AFFILIATE ORDERING. If a Data Controller Affiliate purchased a separate instance of the Subscription Service under the terms of the signed master agreement between ServiceNow and Customer, then such Data Controller Affiliate will be deemed a party to this DPA and shall be treated as Customer under the terms of this DPA.

3.4 COMMUNICATION. Unless otherwise provided in this DPA, all requests, notices, cooperation, and communication, including Instructions issued or required under this DPA (collectively, "**Communication**"), must be in writing and between Customer and ServiceNow only and Customer shall inform the applicable Data Controller Affiliate of any Communication from ServiceNow pursuant to this DPA. Customer shall be solely responsible for ensuring that any Communications (including Instructions) it provides to ServiceNow relating to Personal Data for which a Customer Affiliate is Data Controller reflect the relevant Customer Affiliate's intentions.

4. DATA PROCESSOR

4.1 DATA CONTROLLER'S INSTRUCTIONS. Data Processor will have no liability for any harm or damages resulting from Data Processor's compliance with Instructions received from Data Controller. Where Data Processor believes that compliance with Data Controller's Instructions could result in a violation of Data Protection Laws or is not in the ordinary course of Data Processor's obligations in operating the Subscription Service or delivering Professional Services, Data Processor shall promptly notify Data Controller thereof. Data Controller

acknowledges that Data Processor is reliant on Data Controller's representations regarding the extent to which Data Controller is entitled to Process Personal Data.

4.2 DATA PROCESSOR PERSONNEL. Access to Personal Data by Data Processor will be limited to personnel who require such access to perform Data Processor's obligations under the Agreement and who are bound by obligations to maintain the confidentiality of such Personal Data at least as protective as those set forth herein and in the Agreement.

4.3 DATA SECURITY MEASURES. Without prejudice to Data Controller's security risk assessment obligations under Section 3.2 (Security Risk Assessment) above, Data Processor shall maintain appropriate technical and organizational safeguards to protect the security, confidentiality and integrity of Customer Data, including any Personal Data contained therein, as described in Section 2 (Physical, Technical and Administrative Security Measures) of the Data Security Guide. Such measures are designed to protect Customer Data from loss, alteration, unauthorized access, acquisition, use, disclosure, or accidental or unlawful destruction, and include:

4.3.1. SERVICE ACCESS CONTROL. The Subscription Service provides user and role based access controls. Data Controller is responsible for configuring such access controls within its instance.

4.3.2. LOGGING AND MONITORING. The production infrastructure log activities are centrally collected and are secured in an effort to prevent tampering and are monitored for anomalies by a trained security team.

4.3.3. DATA SEPARATION. Customer Data shall be maintained within a logical single-tenant architecture on multi-tenant cloud infrastructure that is logically and physically separate from ServiceNow's corporate infrastructure.

4.3.4. SERVICE CONTINUITY. The production database servers are replicated in near real time to a mirrored data center in a different geographic region.

4.3.5. TESTING. Data Processor regularly tests, assess and evaluates the effectiveness of its information security program and may periodically review and update the such program to address new and evolving security technologies, changes to industry standard practices, and changing security threats.

4.4 DELETION OF PERSONAL DATA. Upon termination or expiration of the Agreement, Data Processor shall return and delete Customer Data, including Personal Data contained therein, as described in the Agreement.

4.5 DATA CENTERS. Data Processor will host Data Controller's instances of the Subscription Service in data centers located in the geographic regions specified on the Order Form.

4.6 DATA PROTECTION IMPACT ASSESSMENTS (DPIA). Data Processor will, on request, provide Data Controller with reasonable information required to fulfill Data Controller's obligations under GDPR to carry out data protection impact assessments, if any, for Processing of Personal Data within the Subscription Service.

4.7 PRIOR CONSULTATION. Data Processor shall provide reasonable assistance (at Data Controller's expense) in connection with any prior consultation Data Controller is required to undertake with a supervisory authority under Data Protection Laws with respect to Processing of Personal Data in the Subscription Service.

4.8 DATA PROCESSOR ASSISTANCE. Data Processor will assist Data Controller in ensuring compliance with Data Controller's obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of Processing by providing Data Controller with reasonable information requested pursuant to the terms of this DPA, including information required to conduct Data Controller's security risk assessment and respond to Data Subject Requests (defined below). For clarity, Data Controller is solely responsible for carrying out its obligations under GDPR and this DPA. Data Processor shall not undertake any task that can be performed by Data Controller.

4.9 DATA PROTECTION CONTACT. ServiceNow and its Sub-Processor Affiliates (defined below) will maintain a dedicated data protection team to respond to data protection inquiries throughout the duration of this DPA and can be contacted at privacy@servicenow.com.

5. REQUESTS MADE FROM DATA SUBJECTS AND AUTHORITIES

5.1 REQUESTS FROM DATA SUBJECTS. During the Subscription Term, Data Processor shall provide Data Controller with the ability to access, correct, rectify, erase or block Personal Data, or to transfer or port such Personal Data, within the Subscription Service, as may be required under Data Protection Laws (collectively, "Data Subject Requests").

5.2 RESPONSES. Data Controller will be solely responsible for responding to any Data Subject Requests, provided that Data Processor shall reasonably cooperate with the Data Controller to respond to Data Subject

Requests to the extent Data Controller is unable to fulfill such Data Subject Requests using the functionality in the Subscription Service. Data Processor will instruct the Data Subject to contact the Customer in the event Data Processor receives a Data Subject Request directly.

5.3 REQUESTS FROM AUTHORITIES. In the case of a notice, audit, inquiry or investigation by a government body, data protection authority or law enforcement agency regarding the Processing of Personal Data, Data Processor shall promptly notify Data Controller unless prohibited by applicable law. Data Controller shall keep records of the Personal Data Processed by Data Processor, and shall cooperate and provide all necessary information to Data Processor in the event Data Processor is required to produce such information to a data protection authority.

5.4 COOPERATION WITH SUPERVISORY AUTHORITIES. In accordance with Data Protection Laws, Data Controller and Data Processor shall cooperate, on request, with a supervisory authority in the performance of such supervisory authority's task.

6. BREACH NOTIFICATION

6.1 NOTIFICATION. Data Processor will report to Data Controller any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data ("**Breach**") that it becomes aware of without undue delay following determination by ServiceNow that a Breach has occurred.

6.2 REPORT. The initial report will be made to Data Controller's security or privacy contact(s) designated in ServiceNow's customer support portal (or if no such contact(s) are designated, to the primary contact designated by Customer). As information is collected or otherwise becomes available, Data Processor shall provide without undue delay any further information regarding the nature and consequences of the Breach to allow Data Controller to notify relevant parties, including affected Data Subjects, government agencies and data protection authorities in accordance with Data Protection Laws. The report will include the name and contact information of the Data Processor contact from whom additional information may be obtained. Data Processor shall inform Customer of the measures that it will adopt to mitigate the cause of the Breach and to prevent future Breaches.

6.3 DATA CONTROLLER OBLIGATIONS. Data Controller will cooperate with Data Processor in maintaining accurate contact information in the customer support portal and by providing any information that is reasonably requested to resolve any security incident, including any Breaches, identify its root cause(s) and prevent a recurrence. Data Controller is solely responsible for determining whether to notify the relevant supervisory or regulatory authorities and impacted Data Subjects and for providing such notice.

7. CUSTOMER MONITORING RIGHTS

7.1 REMOTE SELF-ASSESSMENTS. Data Processor shall enable remote self-serve assessments of its Security Program (as defined in the Data Security Guide) by granting Data Controller, at all times and at no additional costs, access to the Data Processor self-access documentation portal ("**ServiceNow CORE**"). The information available on ServiceNow CORE will include documentation evidencing Data Processor's policies, procedures and security measures, as well as copies of the certifications and attestations listed in Section 7.2 (Audit) below.

7.2 AUDIT. No more than once per year and upon written request by Data Controller, Customer shall have the right directly or through its representative(s) (provided however, that such representative(s) shall enter into written obligations of confidentiality and non-disclosure directly with Data Processor), to access all reasonable and industry recognized documentation evidencing Data Processor's policies and procedures governing the security of Customer Data ("**Audit**"). Such Audit shall include a written summary report of any assessment performed by an independent third party of Data Processor's information security management system supporting the Subscription Service against the objectives stated in ISO 27001, ISO 27018, SSAE 18 / SOC 1 and SOC 2 Type 2 (or equivalent or successor standards). Data Processor reserves the right to refuse to provide Customer (or its representatives) with any information which would pose a security risk to Data Processor or its customers, or which Data Processor is prohibited to provide or disclose under applicable law or contractual obligation.

7.3 OUTPUT. Upon completion of the Audit, Data Processor and Customer may schedule a mutually convenient time to discuss the output of the Audit. Data Processor may in its sole discretion, consistent with industry and Data Processor's standards and practices, make commercially reasonable efforts to implement Customer's

suggested improvements noted in the Audit to improve Data Processor's Security Program. The Audit and the results derived therefrom are Confidential Information of Data Processor.

7.4 DATA CONTROLLER EXPENSES. Any expenses incurred by Data Controller in connection with the Audit shall be borne exclusively by Data Controller.

8. SUB-PROCESSORS

8.1 USE OF SUB-PROCESSORS. Data Controller authorizes Data Processor to engage Sub-Processors appointed in accordance with this Section 8 to support the provision of the Subscription Service and to deliver Professional Services as described in the Agreement.

8.1.1. SERVICENOW AFFILIATES. As of the Effective Date, Data Processor engages, as applicable, the following ServiceNow Affiliates as Sub-Processors: ServiceNow, Inc. (USA), ServiceNow Nederland B.V. (the Netherlands), ServiceNow Australia Pty Ltd (Australia), ServiceNow Software Development India Private Limited (India), ServiceNow UK Ltd. (United Kingdom), ServiceNow Ireland Limited (Ireland), and ServiceNow Japan K.K. (Japan) (collectively, "**Sub-Processor Affiliates**"). Data Processor will notify Data Controller of changes regarding such Sub-Processor Affiliates through Data Processor's customer support portal (or other mechanism used to notify its general customer base). Each Sub-Processor Affiliate shall comply with the obligations of the Agreement in the Processing of the Personal Data.

8.1.2. NEW SUB-PROCESSORS. Prior to Data Processor or a Data Processor Affiliate engaging a Sub-Processor, Data Processor shall: (i) notify Data Controller by email to Customer's designated contact(s) or by notification within the customer support portal (or other mechanism used to notify its customer base); and (ii) ensure that such Sub-Processor has entered into a written agreement with Data Processor (or the relevant Data Processor Affiliate) requiring that the Sub-Processor abide by terms no less protective than those provided in this DPA. Upon written request by Data Controller, Data Processor shall make a summary of the data processing terms available to Data Controller. Data Controller may request in writing reasonable additional information with respect to Sub-Processor's ability to perform the relevant Processing activities in accordance with this DPA.

8.2 RIGHT TO OBJECT. Data Controller may object to Data Processor's proposed use of a new Sub-Processor by notifying Data Processor within ten (10) days after receipt of Data Processor's notice if Data Controller reasonably determines that such Sub-Processor is unable to Process Personal Data in accordance with the terms of this DPA ("**Controller Objection Notice**"). Data Processor shall notify Data Controller within thirty (30) days from receipt of the Controller Objection Notice if Data Processor intends to provide the applicable Professional Service or Subscription Service with the use of the Sub-Processor at issue, and Customer may terminate the applicable Order Form(s) with respect to the Professional Service or Subscription Service that require use of the Sub-Processor at issue upon written notice to ServiceNow within forty-five (45) days of the date of Controller Objection Notice and, as Customer's sole and exclusive remedy, ServiceNow will refund to Customer any unused prepaid fees.

8.3 LIABILITY. Use of a Sub-Processor will not relieve, waive or diminish any obligation Data Processor has under the Agreement, and Data Processor is liable for the acts and omissions of any Sub-Processor to the same extent as if the acts or omissions were performed by Data Processor.

9. INTERNATIONAL DATA TRANSFERS

9.1 STANDARD CONTRACTUAL CLAUSES. Data Controller and Data Processor agree that Data Controller and relevant Sub-Processor Affiliates will execute the Standard Contractual Clauses attached hereto as Attachment 1 ("**Model Clauses**") for the transfer of Personal Data from the European Economic Area. The parties agree that the Model Clauses and the terms in this Section 9.1 shall only apply to the Processing of Personal Data by Sub-Processor Affiliates (collectively, the "**Data Importer**") in the course of providing the Subscription Service and Professional Services as clarified herein below. The Model Clauses as clarified by this Section 9 apply to: (i) the Customer entity that has executed the Model Clauses as a data exporter if Customer is established within the EEA or Switzerland, or the Customer Affiliate that has executed the Sub-Processor as a data exporter if such Customer Affiliate is established within the EEA or Switzerland; and (ii) all other Affiliates of Customer established within the EEA or Switzerland that have either purchased the Subscription Service or have authorized access to the Subscription Service (each entity qualifying under subsections (i) and (ii), a "**Data Exporter**").

9.1.1. Clause 5(a). In accordance with Section 2.2 (Instructions) of this DPA, Data Importer shall Process Personal Data on Data Exporter's behalf and only in accordance with Data Exporter's instructions. The

parties agree that Data Exporter's complete instructions are set forth in the Agreement. ServiceNow and Customer must agree upon any additional or alternate instructions separately in writing.

9.1.2. Clause 5(f) and Clause 12(2). Data Exporter may exercise its monitoring rights set forth in Section 7 (Customer Monitoring Rights) of this DPA.

9.1.3. Clause 5(h); Clause 5(j); and Clause 11(1). Data Exporter authorizes Data Importer to engage Sub-Processors appointed in accordance with Section 8 (Sub-Processors) to support the provision of the Subscription Service and to deliver Professional Services as described in the Agreement.

9.1.4. Clause 12 (1). Data Exporter agrees that upon expiration or termination of this DPA, Customer shall request the return of Customer Data in accordance with the procedure set forth in the Agreement, and ServiceNow shall make available such Customer Data in accordance with such procedure. The parties agree that the certification of deletion or destruction of Customer Data shall be provided by ServiceNow to Customer only upon Customer's written request, provided that such request is made through the customer support portal prior to the termination or expiration of the Agreement.

9.1.5. Communication under the Model Clauses. The parties agree that all notices, requests, monitoring rights required under the Model Clauses shall be provided, as applicable, to the Customer and the ServiceNow entity that is a party to the Agreement. The Customer shall at all times be responsible for the Data Exporter's compliance with the Model Clauses.

9.1.6. Enforcement. Data Exporter(s) may enforce the terms of this DPA against Data Importer, provided however, that the Customer must bring any valid legal action, suit, claim or proceedings which that Data Exporter would otherwise have if it were a party to this DPA (each a "**Data Exporter Claim**") directly against Data Importer on behalf of such Data Exporter, unless the applicable Data Protection Laws to which the relevant Data Exporter is subject requires that the Data Exporter itself bring or be a party to such Data Exporter Claim. Any Model Clauses executed by Data Importer and Data Exporter shall only be enforceable against Data Importer as integrated with this DPA and shall form the entire agreement with regard to the Processing of Personal Data of such Data Exporter. Any such Data Exporter Claim shall at all times be subject to any aggregate limitation of liability that applies to the Customer under the Agreement. The existence of more than one claim shall not enlarge this limit.

9.2 MODEL CLAUSES WITH NEW SUB-PROCESSORS. Where required under Data Protection Laws, Data Processor or Data Processor's Affiliates shall require Sub-Processors to abide by (i) the Standard Contractual Clauses for Data Processors established in third countries; or (ii) another lawful mechanism for the transfer of Personal Data as approved by the European Commission.

9.3 PRIVACY SHIELD. ServiceNow, Inc. shall comply with the EU-U.S. and Swiss-U.S. Privacy Shield Framework set forth by the United States Department of Commerce with respect to the Processing of Personal Data transferred from the European Economic Area and Switzerland to the United States.

10. GENERAL PROVISIONS

10.1 CONFIDENTIALITY. Data Controller may only disclose the terms of this DPA to a data protection or regulatory authority to the extent required by law or regulatory authority, provided however, that any such disclosure shall be limited to the minimum information necessary to satisfy such disclosure requirement. Data Controller shall use commercially reasonable efforts to ensure that data protection or regulatory authorities do not make this DPA public.

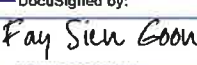
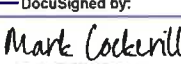
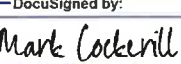
10.2 LIMITATION OF LIABILITY. Customer's remedies with respect to any breach by ServiceNow of the terms of this DPA will be subject to any aggregate limitation of liability under the Agreement. If ServiceNow, Inc., ServiceNow Australia PTY LTD, ServiceNow UK Ltd., ServiceNow Software Development India Private Limited, ServiceNow Ireland Limited and ServiceNow Japan K.K. are not a party to the Agreement, the section of the Agreement titled "Limitations of Liability" (or equivalent) shall apply to ServiceNow, Inc., ServiceNow Australia PTY LTD, ServiceNow UK Ltd., ServiceNow Software Development India Private Limited, ServiceNow Ireland Limited, and ServiceNow Japan K.K. and in such respect any references to ServiceNow shall include ServiceNow, Inc., ServiceNow Australia PTY LTD, ServiceNow UK Ltd., ServiceNow Software Development India Private Limited and the ServiceNow entity who is party to the Agreement.

10.3 TERMINATION. This DPA shall terminate simultaneously and automatically with the termination of the Agreement or expiration of the Subscription Term where Customer does not renew. Notwithstanding the foregoing, ServiceNow shall continue to secure Personal Data in accordance with the terms herein for so long as ServiceNow has access to such Personal Data.

10.4 WAIVERS AND MODIFICATIONS. A waiver of any right is only effective if it is in writing and only against the party who signed such writing and for the circumstances given. Any modification of this DPA must be in writing and signed by authorized representatives of both parties.

10.5 LEGAL EFFECT. This DPA shall only become legally binding between Customer and ServiceNow upon Customer fully completing the steps set forth in "INSTRUCTIONS FOR EXECUTING THIS DPA." The Section "Application of this DPA" specifies which ServiceNow entity is party to this DPA. Notwithstanding the signatures below of any other ServiceNow entity, such other ServiceNow entities are not a party to this DPA. Customer shall at all times be responsible for its Affiliates' compliance with this DPA.

THE PARTIES, EACH ACTING UNDER DUE AND PROPER AUTHORITY, HEREBY EXECUTE THIS DATA PROCESSING ADDENDUM.

Customer:	ServiceNow, Inc.
Individual signing:	Individual signing: Fay Sien Goon
(print name)	
Signature:	Signature:  DocuSigned by: 934AAF50B57841F
Title:	Title: Chief Accounting Officer
Signing Date:	Signing Date: July 31, 2019
ServiceNow Brasil Ltda.	ServiceNow Australia PTY LTD
Individual signing: Katia Ortiz	Individual signing: Mark Cockerill
Signature:  DocuSigned by: 3EE8DDC4E8E64EC	Signature:  DocuSigned by: F49D7F9D555C438
Title: Director	Title: Director
Signing Date: August 6, 2019	Signing Date: July 31, 2019
ServiceNow UK Ltd.	ServiceNow Nederland B.V.
Individual signing: Mark Cockerill	Individual signing: Tom Ellison
Signature:  DocuSigned by: F49D7F9D555C438	Signature:  DocuSigned by: D981756881B34EF
Title: Director	Title: Director
Signing Date: July 31, 2019	Signing Date: August 4, 2019
ServiceNow Japan K.K.	
Individual signing: Adam Pendlebury	
Signature:  DocuSigned by: 3200A7F750E0407...	
Title: Director	
Signing Date: August 1, 2019	

ANNEX 1

DETAILS OF PROCESSING

Nature and Purpose of Processing

Data Processor will Process Personal Data as required to provide the Subscription Service and Professional Services and in accordance with the Agreement.

Duration of Processing

Data Processor will Process Personal Data for the duration of the Agreement and in accordance with Section 4 (Data Processor) of this DPA.

Data Subjects

Data Controller may submit Personal Data to the Subscription Service, the extent of which is solely determined by Data Controller, and may include Personal Data relating to the following categories of Data Subjects:

- Clients and other business contacts;
- Employees and contractors;
- Subcontractors and agents; and
- Consultants and partners.

Categories of Personal Data

Data Controller may submit Personal Data to the Subscription Service, the extent of which is solely determined by Data Controller, and may include the following categories:

- communication data (e.g. telephone, email);
- business and personal contact details;
- and other Personal Data submitted to the Subscription Service.

Special Categories of Personal Data

Data Controller may submit Special Categories of Personal Data to the Subscription Service, the extent of which is solely determined by Data Controller in compliance with Data Protection Law, and may include the following categories, if any:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data or biometric data;
- health information; and
- sex life or sexual orientation.

Processing Operations

The personal data transferred will be subject to the following basic processing activities:

- All activities necessary for the performance of the Agreement.

ATTACHMENT 1

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

Address:

Tel.:; fax:; e-mail:

Other information needed to identify the organisation:

.....
(the data exporter)

And

Name of the data importing organisation: **ServiceNow, Inc.**

Address: 2225 Lawson Lane, Santa Clara, California 95054

Tel.: 1.408.501.8550; fax: 1.858.720.0479; e-mail: privacy@servicenow.com

Other information needed to identify the organisation: Not applicable

Name of the data importing organisation: **ServiceNow Australia PTY LTD.**

Address: Suite 9, Waverley Masonic Centre, 318-322 Stephenson's Road, Mount Waverley VIC 3149 Australia

Tel.: 1.408.501.8550; fax: 1.858.720.0479; e-mail: privacy@servicenow.com

Other information needed to identify the organisation: Not applicable

Name of the data importing organisation: **ServiceNow Software Development India Private Limited**

Address: Knowledge City, 7th Floor, Plot No 2, Phase 1, Survey No.83/1, Raidurg Village,

Serilingampally Hyderabad Rangareddi TG 500081 IN

Tel.: 1.408.501.8550; fax: 1.858.720.0479; e-mail: privacy@servicenow.com

Other information needed to identify the organisation: Not applicable

Name of the data importing organisation: **ServiceNow UK Ltd.**

Address: 1 Bridge Street,

Staines-Upon-Thames, England TW18 4TW

Tel.: 1.408.501.8550; fax: 1.858.720.0479; e-mail: privacy@servicenow.com

Other information needed to identify the organisation: Not applicable

Name of the data importing organisation: **ServiceNow Japan K.K.**

Address: Ark Mori Building, 1-12-32 Akasaka, Minato-ku, Tokyo, Japan

Tel.: 1.408.501.8550; fax: 1.858.720.0479; e-mail: privacy@servicenow.com

Other information needed to identify the organisation: Not applicable

(the data importer)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

- (a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) *'the data exporter'* means the controller who transfers the personal data;
- (c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or

access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;

- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

- (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
- (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature.....

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): Fay Sien Goon.....

Position: Chief Accounting Officer.....

Address: 2225 Lawson Lane

Santa Clara, California 95054

Other information necessary in order for the contract to be binding (if any):

DocuSigned by:
Fay Sien Goon
Signature.....934AAE50B57841E.....

Name (written out in full): Mark Cockerill.....
Position: Director.....
Address: Suite 9, Waverley Masonic Centre,
318-322 Stephenson's Road
Mount Waverley VIC 3149 Australia

Other information necessary in order for the contract to be binding (if any):

DocuSigned by:
Mark Cockerill
Signature.....F49D7F9D555C438

Name (written out in full): Raj Santhanam.....
Position: Director

Address: Knowledge City, 7th Floor, Plot No 2, Phase 1, Survey No.83/1, Raidurg Village,
Serilingampally Hyderabad Rangareddi TG 500081 IN

Other information necessary in order for the contract to be binding (if any):

Signature.....

Name (written out in full): Mark Cockerill.....
Position: Director.....
Address: 1 Bridge Street,
Staines-Upon-Thames, England TW18 4TW

Other information necessary in order for the contract to be binding (if any):

DocuSigned by:
Mark Cockerill
Signature.....F49D7F9D555C438

Name (written out in full): Mark Cockerill.....
Position: Director.....
Address: Ark Mori Building,
1-12-32 Akasaka, Minato-ku, Tokyo, 107-0052 Japan

Other information necessary in order for the contract to be binding (if any):

DocuSigned by:

Signature.....F49D7F8D555C438.....

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix 1 forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Data Importer is a provider of cloud-based solutions that define, structure, manage and automate services across the global enterprise in accordance with the Agreement.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

The Data Exporter may submit Personal Data as part of Customer Data to the Subscription Service, the extent of which is determined and controlled by the Data Exporter in its sole discretion and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

Categories of data

The personal data transferred concern the following categories of data (please specify):

The Data Exporter may submit Personal Data as part of Customer Data to the Subscription Service, the extent of which is determined and controlled by the Data Exporter in its sole discretion and which may include, but is not limited to the following categories of Personal Data:

Special categories of data (if appropriate)

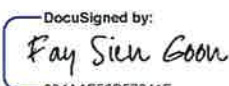
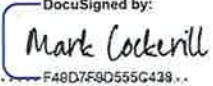
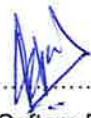
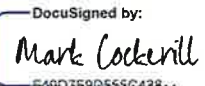
The personal data transferred concern the following special categories of data (please specify):

The Data Exporter may submit Personal Data, including sensitive data, as part of Customer Data to the Subscription Service, the extent of which is determined and controlled by the Data Exporter in its sole discretion and which may include, but is not limited to the following categories of Personal Data:

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The Data Importer shall Process Personal Data in the performance providing and supporting the Subscription Service pursuant to the Agreement.

DATA EXPORTER Name:..... Authorised Signature	DATA IMPORTERS Name: Fay Sien Goon  Authorised Signature 934A6F50B57842F... (on behalf of ServiceNow, Inc.)
DATA IMPORTER Name: Mark Cockerill  Authorised Signature F48D7F8D555C438... (on behalf of ServiceNow UK Ltd.)	DATA IMPORTER Name: Mark Cockerill  Authorised Signature F48D7F8D555C438... (on behalf of ServiceNow Australia PTY LTD)
DATA IMPORTER Name: Raj Santhanam  Authorised Signature (on behalf of ServiceNow Software Development India Private Limited)	DATA IMPORTER Name: Mark Cockerill  Authorised Signature F48D7F8D555C438... (on behalf of ServiceNow Japan K.K.)

///

///

///

Remainder of page intentionally left blank

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix 2 forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data Importer's Security Program shall include the physical, technical and administrative measures detailed in the Data Security Guide of this DPA, which is hereby incorporated in this Appendix 2 in its entirety.

DATA EXPORTER Name:..... Authorised Signature	DATA IMPORTER Name: Fay Sien Goon Authorised Signature (on behalf of ServiceNow, Inc.)
DATA IMPORTER Name: Raj Santhanam Authorised Signature (on behalf of ServiceNow Software Development India Private Limited)	DATA IMPORTER Name: Mark Cockerill Authorised Signature (on behalf of ServiceNow Australia PTY LTD)
DATA IMPORTER Name: Mark Cockerill Authorised Signature (on behalf of ServiceNow Japan K.K.)	DATA IMPORTER Name: Mark Cockerill Authorised Signature (on behalf of ServiceNow UK Ltd.)

ATTACHMENT 2

DATA SECURITY GUIDE

This Data Security Guide forms a part of the Agreement and describes the measures ServiceNow takes to protect Customer Data.

In the event of any conflict between the terms of this Data Security Guide and the terms of the Agreement with respect to the subject matter herein, this Data Security Guide shall control. All capitalized terms not defined in this Data Security Guide will have the meaning given to them in other parts of the Agreement.

1. SECURITY PROGRAM

While providing the Subscription Service, ServiceNow will maintain a written information security program of policies, procedures and controls governing the processing, storage, transmission and security of Customer Data (the "**Security Program**"). The Security Program includes industry-standard practices designed to protect Customer Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. ServiceNow regularly tests, assesses and evaluates the effectiveness of the Security Program and may periodically review and update the Security Program to address new and evolving security technologies, changes to industry standard practices, and changing security threats, although no such update will materially reduce the commitments, protections or overall level of service provided to Customer as described herein.

2. PHYSICAL, TECHNICAL AND ADMINISTRATIVE SECURITY MEASURES

2.1 PHYSICAL SECURITY MEASURES.

2.1.1. Data Center Facilities. (i) Physical access restrictions and monitoring that may include a combination of any of the following: multi-zone security, man-traps, appropriate perimeter deterrents (e.g. fencing, berms, guarded gates), on-site guards, biometric controls, CCTV, and secure cages; and (ii) fire detection and fire suppression systems both localized and throughout the data center floor.

2.1.2. SYSTEMS, MACHINES AND DEVICES. (i) Physical protection mechanisms; and (ii) entry controls to limit physical access.

2.1.3. MEDIA. (i) Industry standard destruction of sensitive materials before disposition of media; (ii) secure safe for storing damaged hard disks prior to physical destruction; and (iii) physical destruction of all decommissioned hard disks storing Customer Data.

2.2 TECHNICAL SECURITY MEASURES.

2.2.1. ACCESS ADMINISTRATION. Access to the Subscription Service by ServiceNow employees and contractors is protected by authentication and authorization mechanisms. User authentication is required to gain access to production and sub-production instances. Access privileges are based on job requirements and are revoked upon termination of employment or consulting relationships. Production infrastructure includes appropriate user account and password controls (e.g., the required use of VPN connections, complex passwords with expiration dates, and a two-factored authenticated connection) and is accessible for administration.

2.2.2. SERVICE ACCESS CONTROL. The Subscription Service provides user and role based access controls. Customer is responsible for configuring such access controls within its instance.

2.2.3. LOGGING AND MONITORING. The production infrastructure log activities are centrally collected and are secured in an effort to prevent tampering and are monitored for anomalies by a trained security team.

2.2.4. Firewall System. An industry-standard firewall is installed and managed to protect ServiceNow systems by residing on the network to inspect all ingress connections routed to the ServiceNow environment.

2.2.5. Vulnerability Management. ServiceNow conducts periodic independent security risk evaluations to identify critical information assets, assess threats to such assets, determine potential vulnerabilities, and provide for remediation. When software vulnerabilities are revealed and addressed by a vendor patch, ServiceNow will obtain the patch from the applicable vendor and apply it within an appropriate timeframe in accordance with ServiceNow's then current vulnerability management and security patch management standard operating procedure and only after such patch is tested and determined to be safe for installation in all production systems.

2.2.6. ANTIVIRUS. ServiceNow updates antivirus, anti-malware, and anti-spyware software on regular intervals and centrally logs events for effectiveness of such software.

2.2.7. CHANGE CONTROL. ServiceNow ensures that changes to platform, applications and production infrastructure are evaluated to minimize risk and are implemented following ServiceNow's standard operating procedure.

2.2.8. DATA SEPARATION. Customer Data shall be maintained within a logical single-tenant architecture on multi-tenant cloud infrastructure that is logically and physically separate from ServiceNow's corporate infrastructure.

2.3 ADMINISTRATIVE SECURITY MEASURES.

2.3.1. DATA CENTER INSPECTIONS. ServiceNow performs routine reviews at each data center to ensure that it continues to maintain the security controls necessary to comply with the Security Program.

2.3.2. PERSONNEL SECURITY. ServiceNow performs background screening on all employees and all contractors who have access to Customer Data in accordance with ServiceNow's then current applicable standard operating procedure and subject to Law.

2.3.3. SECURITY AWARENESS AND TRAINING. ServiceNow maintains a security awareness program that includes appropriate training of ServiceNow personnel on the Security Program. Training is conducted at time of hire and periodically throughout employment at ServiceNow.

2.3.4. VENDOR RISK MANAGEMENT. ServiceNow maintains a vendor risk management program that assesses all vendors that access, store, process or transmit Customer Data for appropriate security controls and business disciplines.

3. SERVICE CONTINUITY

3.1 DATA MANAGEMENT; DATA BACKUP. ServiceNow will host Customer's access and use of purchased instances of the Subscription Service in a pair of data centers that attained SSAE 18 Type 2 attestations or have ISO 27001 certifications (or equivalent or successor attestations) acting in an active/active capacity for the Subscription Term. Each data center includes full redundancy (N+1) and fault tolerant infrastructure for electrical, cooling and network systems. The deployed servers are enterprise scale servers with redundant power to ensure maximum uptime and service availability. The production database servers are replicated in near real time to a mirrored data center in a different geographic region. Each Customer instance is supported by a network configuration with multiple connections to the Internet. ServiceNow backs up all Customer Data in accordance with ServiceNow's standard operating procedure.

3.2 PERSONNEL. In the event of an emergency that renders the customer support telephone system unavailable, all calls are routed to an answering service that will transfer to a ServiceNow telephone support representative, geographically distributed to ensure business continuity for support operations.

4. CERTIFICATIONS AND AUDITS

4.1 CERTIFICATIONS AND ATTESTATIONS. ServiceNow shall establish and maintain sufficient controls to meet the objectives stated in ISO 27001, ISO 27018, SSAE 18 / SOC 1 and SOC 2 Type 2 (or equivalent standards) (collectively, the "**Standards**") for the information security management system supporting the Subscription Service. At least once per calendar year, ServiceNow shall obtain an assessment against such Standards by an independent third-party auditor.

4.2 CUSTOMER MONITORING RIGHTS.

4.2.1. REMOTE SELF ASSESSMENTS. ServiceNow shall enable remote self-serve assessments of its Security Program by granting Customer, at all times and at no additional costs, access to the ServiceNow self-access documentation portal ("**ServiceNow CORE**"). The information available on ServiceNow CORE will include documentation evidencing ServiceNow's policies, procedures and security measures, as well as copies of the certifications and attestations listed in Section 4.2.2 (Audit) below.

4.2.2. AUDIT. No more than once per year and upon written request by Customer, Customer shall have the right directly or through its representative(s) (provided however, that such representative(s) shall enter into written obligations of confidentiality and non-disclosure directly with ServiceNow), to access all reasonable and industry recognized documentation evidencing ServiceNow's policies and procedures governing the security of Customer Data ("**Audit**"). Such Audit shall include a written summary report of any assessment performed by an

independent third party of ServiceNow's information security management system supporting the Subscription Service against the objectives stated in ISO 27001, ISO 27018, SSAE 18 / SOC 1 and SOC 2 Type 2 (or equivalent or successor attestations). ServiceNow reserves the right to refuse to provide Customer (or its representatives) with any information which would pose a security risk to ServiceNow or its customers, or which ServiceNow is prohibited to provide or disclose under applicable law or contractual obligation.

4.2.3. OUTPUT. Upon completion of the Audit, ServiceNow and Customer may schedule a mutually convenient time to discuss the output of the Audit. ServiceNow may in its sole discretion, consistent with industry and ServiceNow's standards and practices, make commercially reasonable efforts to implement Customer's suggested improvements noted in the Audit to improve ServiceNow's Security Program. The Audit and the results derived therefrom are Confidential Information of ServiceNow.

4.2.4. CUSTOMER EXPENSES. Any expenses incurred by Customer in connection with the Audit shall be borne exclusively by Customer.

5. MONITORING AND INCIDENT MANAGEMENT

5.1 MONITORING, MANAGEMENT AND NOTIFICATION.

5.1.1. INCIDENT MONITORING AND MANAGEMENT. ServiceNow will monitor, analyze and respond to security incidents in a timely manner in accordance with ServiceNow's standard operating procedure. ServiceNow's security group will escalate and engage response teams as may be necessary to address an incident.

5.1.2. BREACH NOTIFICATION. ServiceNow will report to Customer any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data (a "**Breach**") without undue delay following determination by ServiceNow that a Breach has occurred.

5.1.3. REPORT. The initial report will be made to Customer security or privacy contact(s) designated in ServiceNow's customer support portal (or if no such contact(s) are designated, to the primary contact designated by Customer). As information is collected or otherwise becomes available, ServiceNow shall provide without undue delay any further information regarding the nature and consequences of the Breach to allow Customer to notify relevant parties, including affected Data Subjects, government agencies and data protection authorities in accordance with Data Protection Laws. The report will include the name and contact information of the ServiceNow contact from whom additional information may be obtained. ServiceNow shall inform Customer of the measures that it will adopt to mitigate the cause of the Breach and to prevent future Breaches.

5.1.4. CUSTOMER OBLIGATIONS. Customer will cooperate with ServiceNow in maintaining accurate contact information in the customer support portal and by providing any information that is reasonably requested to resolve any security incident, including any Breaches, identify its root cause(s) and prevent a recurrence. Customer is solely responsible for determining whether to notify the relevant supervisory or regulatory authorities and impacted Data Subjects and for providing such notice.

5.2 USE OF AGGREGATE DATA. ServiceNow may collect, use and disclose quantitative data derived from Customer's use of the Subscription Service for industry analysis, benchmarking, analytics, marketing, and other business purposes in support of the provision of the Subscription Service. Any such data will be in aggregate form only and will not contain Customer Data.

5.3 COOKIES. When providing the Subscription Service, ServiceNow uses cookies to: (i) track session state; (ii) route a browser request to a specific node when multiple nodes are assigned; and (iii) recognize a user upon returning to the Subscription Service. Customer shall be responsible for providing notice to, and collecting any necessary consents from, its authorized users of the Subscription Service for ServiceNow's use of cookies.

6. PENETRATION TESTS

6.1 BY A THIRD-PARTY. ServiceNow contracts with third-party vendors to perform a penetration test on the ServiceNow application per family release to identify risks and remediation that help increase security.

6.2 BY CUSTOMER. No more than once per calendar year Customer may request to perform, at its own expense, an application penetration test of a sub-production instance of the Subscription Service. Customer shall notify ServiceNow in advance of any test by submitting a request to schedule an application penetration test using ServiceNow's customer support portal per ServiceNow's then-current penetration testing policy and procedure, including entering into ServiceNow's penetration test agreement. ServiceNow and Customer must agree on a mutually acceptable time for the test; and Customer shall not perform a penetration test without ServiceNow's express written authorization. The test must be of reasonable duration, but in no event longer than 14 days and

must not interfere with ServiceNow's day-to-day operations. Promptly on completion of the penetration test, Customer shall provide ServiceNow with the test results including any detected vulnerability. Upon such notice, ServiceNow shall, consistent with industry-standard practices, use all commercially reasonable efforts to promptly make any necessary changes to improve the security of the Subscription Service. Customer shall treat the test results as Confidential Information of ServiceNow subject to the confidentiality and non-use requirements of the Agreement.

7. SHARING THE SECURITY RESPONSIBILITY

7.1 PRODUCT CAPABILITIES. The Subscription Service has the capabilities to: (i) authenticate users before access; (ii) encrypt passwords; (iii) allow users to manage passwords; and (iv) prevent access by users with an inactive account. Customer manages each user's access to and use of the Subscription Service by assigning to each user a credential and user type that controls the level of access to the Subscription Service. Customer shall be responsible for implementing encryption and access control functionalities available within the Subscription Service for protecting all Customer Data containing sensitive data, including credit card numbers, social security and other government-issued identification numbers, financial and health information, Personal Data, and any Personal Data deemed sensitive or "special categories of personal data" under Data Protection Laws. Customer is solely responsible for its decision not to encrypt such data and ServiceNow will have no liability to the extent that damages would have been mitigated by Customer's use of such encryption measures. Customer is responsible for protecting the confidentiality of each user's login and password and managing each user's access to the Subscription Service.

7.2 CUSTOMER COOPERATION. Customer shall promptly apply any application upgrade that ServiceNow determines is necessary to maintain the security, performance or availability of the Subscription Service.

7.3 LIMITATIONS. Notwithstanding anything to the contrary in this Data Security Guide or other parts of the Agreement, ServiceNow's obligations extend only to those systems, networks, network devices, facilities and components over which ServiceNow exercises control. This Data Security Guide does not apply to: (i) information shared with ServiceNow that is not data stored in its systems using the Subscription Service; (ii) data in Customer's VPN or a third-party network; (iii) any data processed by Customer or its users in violation of the Agreement or this Data Security Guide; or (iv) Integrated Products. For the purposes of this Data Security Guide, "**Integrated Products**" shall mean ServiceNow-provided integrations to third-party products or any other third-party products that are used by Customer in connection with the Subscription Service. Customer agrees that its use of such Integrated Products will be: (a) in compliance with all applicable laws, including but not limited to, Data Protection Laws; and (b) in accordance with its contractual agreement with the provider of such Integrated Products. Any Personal Data populated from the Integrated Products to the Subscription Service must be collected, used, disclosed and, if applicable, internationally transferred in accordance with Customer's privacy policy, which will adhere to Data Protection Laws.

///

///

///

Remainder of page intentionally left blank