

## DATA PROCESSING ADDENDUM

All capitalized terms not defined in this Data Processing Addendum (“DPA”) have the meaning given to them in other parts of the Agreement.

### 1. DEFINITIONS

**1.1 “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.

**1.2 “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.

**1.3 “Data Protection Laws”** means all applicable laws and regulations regarding the Processing of Personal Data.

**1.4 “Data Subject”** means an identified or identifiable natural person.

**1.5 “Instructions”** means Data Controller’s documented data Processing instructions issued to Data Processor in compliance with this DPA.

**1.6 “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.

**1.7 “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.

**1.8 “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.

**1.9 “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.

**1.10 “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.

### 2. SCOPE OF THE PROCESSING

**2.1 COMMISSIONED PROCESSOR.** Data Controller appoints Data Processor to Process Personal Data on behalf of Data Controller as described in the Agreement and in accordance with the Instructions.

**2.2 INSTRUCTIONS.** The Agreement constitutes Data Controller’s initial 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 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 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:

**3.1.1. 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.

**3.1.2. 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.

**3.1.3. 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.

**3.2 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 the Agreement, 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 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 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 unlawful Instructions received from Data Controller. Where Data Processor believes 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 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 the Agreement. 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, are secured in an effort to prevent tampering, and are monitored for anomalies by a trained security team. ServiceNow shall provide a logging capability in the platform that captures login and actions taken by users in the ServiceNow application. Customer has full access to application audit logs within its instance(s), including successful and failed access attempts to Customer's instance(s). Customer is responsible for exporting application audit logs to Customer's syslog server through available built-in platform features.

**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. ServiceNow shall use NIST 800-88 industry standard (or substantially equivalent) destruction of sensitive materials, including Customer Data, before such media leaves ServiceNow's data centers for disposition.

**4.5** DATA PROCESSOR ASSISTANCE. Data Processor will assist Data Controller in ensuring compliance with Data Controller's obligations pursuant to Data Protection Laws 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 data protection impact assessments and prior consultations with supervisory authorities, where required. For clarity, Data Controller is solely responsible for carrying out its obligations under Data Protection Laws and this DPA. Data Processor shall not undertake any task that can be performed by Data Controller.

**4.6** 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](mailto: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. Each party shall cooperate with the other party by providing all reasonable information requested in the event the other party is required to produce such information to a data protection authority.

## **6. BREACH NOTIFICATION**

**6.1 NOTIFICATION.** Data Processor will report to Data Controller any accidental or unlawful destruction, loss, alteration, unauthorized disclosure, of or access to Customer Data (“**Breach**”) 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 technical 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 CERTIFICATIONS AND ATTESTATIONS.** ServiceNow shall establish and maintain sufficient controls to meet certification and attestation for the objectives stated in ISO 27001, ISO 27018, SSAE 18 / SOC 1 and SOC 2 Type 2 (or equivalent standards) for the Security Program supporting the Subscription Service. At least once per calendar year, ServiceNow shall obtain an assessment against such standards and audit methodologies by an independent third-party auditor and make the executive reports available to the Customer.

**7.2 AUDIT.** Data Processor shall allow for and contribute to audits that include inspections by granting Customer (either directly or through its representative(s); provided that such representative(s) shall enter into written obligations of confidentiality and non-disclosure directly with ServiceNow), access to all reasonable and industry recognized documentation evidencing ServiceNow’s policies and procedures governing the security and privacy of Customer Data and its Security Program through ServiceNow’s self-access documentation portal (“**ServiceNow CORE**”) and at no additional costs (“**Audit**”). The information available in ServiceNow CORE will include documentation evidencing ServiceNow’s Security Program, as well as ServiceNow’s privacy policies and procedures regarding personal information processed within the Subscription Service, copies of certifications and attestation reports (including audits) listed above.

**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.

**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 G.K. (Japan) (collectively, “**Sub-Processor Affiliates**”). Data Processor will notify Data Controller of changes regarding such Sub-Processor Affiliates through Data Processor’s 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: **(a)** notify Data Controller by email to Customer’s designated contact(s) or by notification within the Support Portal (or other mechanism used to notify its customer base); and **(b)** ensure such Sub-Processor entered into a written agreement with Data Processor (or the relevant Data Processor Affiliate) requiring 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 10 days after receipt of Data Processor’s notice if Data Controller reasonably determines such Sub-Processor is unable to Process Personal Data in accordance with the terms of this DPA (“**Objection Notice**”). In the event Data Controller submits its Objection Notice, Data Processor shall reasonably consider such objection and will notify Data Controller if it intends to provide the applicable Subscription Service or Professional Services with the use of the Sub-Processor at issue (“**Processor Notice**”). Customer may terminate the applicable Order Form(s), Use Authorization(s) with respect to the Professional Service or Subscription Service requiring use of the Sub-Processor at issue upon written notice to ServiceNow within 10 days of the date of Processor Notice (“**Termination Period**”). ServiceNow will, as Customer’s sole and exclusive remedy, refund to Customer any unused prepaid fees following the effective date of termination for the terminated services. For clarity, Data Processor will not engage the new Sub-Processor at issue until the expiration of the Termination Period.

**8.3 LIABILITY.** Use of a Sub-Processor will not relieve, waive, or diminish any obligation of Data Processor 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 AND ADEQUACY.** Where required under Data Protection Laws, Data Processor or Data Processor’s Affiliates shall require Sub-Processors to abide by **(a)** the Standard Contractual Clauses for Data Processors established in third countries; or **(b)** another lawful mechanism for the transfer of Personal Data as approved by the European Commission.

///

///

///

Remainder of page intentionally left blank

## APPENDIX 1

### DETAILS OF PROCESSING

#### 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 Laws, 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 is subject to the following basic processing activities:

- All activities necessary for the performance of the Agreement.