VENDOR DATA PROTECTION ADDENDUM

This Vendor Data Protection Addendum ("***DPA***") is entered into as of _____ and is retroactively effective as of the last date of signature below ("***DPA Effective Date***"). This DPA is incorporated into and forms part of the Agreement
(as defined below) between ServiceNow (as defined below) and _____ acting on its own behalf and on behalf of its Affiliates ("***Vendor***") (collectively, the "***Parties***"). This DPA reflects the parties' obligations with respect to Personal Data Processed as part of the Services (all as defined below).

In the event of a conflict between the terms of this DPA and the Agreement with respect to the subject matter herein, the terms of this DPA govern. Any data protection agreements that may already exist between the Parties as of the last signature date of this DPA as well as any earlier version of data security terms to which the Parties may have agreed to are superseded and replaced by this DPA in their entirety.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 the Agreement.

1. DEFINITIONS

1.1 "***Affiliate"*** 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 applicable master agreement, contractor services agreement, terms of service, order form, purchase order, contract or other legal document that governs Vendor's provision of the Services or relationship of the Parties.

1.3 ***"Controller***" means the legal person or entity which alone or jointly with others, determines the purposes and means of Processing of Personal Data.

1.4 "***Data Protection Laws***" means all applicable laws and regulations regarding the Processing of Personal Data, including, where applicable, the European Union's General Data Protection Regulation (2016/679) and the California Consumer Privacy Act of 2018 effective as of January 1, 2020 ("***CCPA***"), each as may be amended from time to time.

1.5 ***"Data Subject"*** means an identified or identifiable natural person. For clarity, Data Subject includes any "consumer" as that term is defined by the CCPA.

1.6 ***"Personal Data"*** means any information relating to, directly or indirectly, a Data Subject or household that is collected, accessed, used, disclosed or otherwise Processed by Vendor in its provision of Services.

1.7 ***"Process", "Processes" or "Processing"*** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

1.8 "***Processor***" means the legal person or entity that Processes Personal Data on behalf of the Controller.

1.9 "***Restricted Transfer***" means any transfer of Personal Data from within the European Economic Area (EEA) to countries outside of the EEA which are not subject to an adequacy decision by the European Commission, where such transfer would be prohibited by Data Protection Laws.

1.10 "***ServiceNow***" means ServiceNow, Inc. and its Affiliates.

1.11 "***ServiceNow Data***" means all ServiceNow data processed by Vendor pursuant to the terms of the Agreement.

1.12 **"*Services*"** means any products or services, including professional services, provided by Vendor pursuant to the Agreement and/or any related statements of work or order forms.

1.13 ***"Sub-Processor"*** means any party engaged by Vendor (when acting as Processor on behalf of ServiceNow) that Processes Personal Data.

1.14 *"**Standard Contractual Clauses (controllers)**"* or "***Controller SCCs***" means the model clauses for the transfer of Personal Data to Controllers established in third countries approved and updated by the European Commission from time to time, the approved version of which, in force at the DPA Effective Date, is that set out in the European Commission's Decision 2004/915/EC of 27 December 2004 as such model clauses are available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004D0915&from=EN.

1.15 ***"Standard Contractual Clauses (processors)"*** or "***Processor SCCs***" means the model clauses for the transfer of Personal Data to Processors approved and updated by the European Commission from time to time,

the approved version of which, in force at the DPA Effective Date, is set out in the European Commission's Decision 2010/87/EU of 5 February 2010 as such model clauses are available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087&from=en.

2. ROLES OF THE PARTIES

2.1 The Parties agree that the status of each party as a 'controller,' 'processor,' or other categories of defining the Parties' roles under Data Protection Laws is a question of fact determined under Data Protection Laws.

2.2 The Parties further agree that, with effect from the DPA Effective Date, the Parties intend that the applicable data protection roles of the Parties are ServiceNow acting as Controller and Vendor acting as Processor and that, as such, Vendor shall comply with the Processor related obligations set out in Clauses 4 and 5 hereof. However, in the event that the Parties agree that: (i) Vendor is actually acting as Controller in writing; or (ii) Vendor is in fact a Controller pursuant to Data Protection Laws with respect to the delivery of some or all of the Services, then Vendor shall comply with Controller related obligations set out in Clauses 3 and 5 hereof. All other provisions in this DPA apply irrespective of whether Vendor acts as Controller or Processor.

2.3 Vendor certifies that it understands all of its restrictions and obligations under applicable Data Protection Laws and shall comply with all Data Protection Laws that apply to its Processing of Personal Data under the Agreement, including, where applicable, Data Protection Laws on collection, sharing and transfer of Personal Data.

3. CONTROLLER OBLIGATIONS

3.1 Where Vendor Processes Personal Data as a Controller pursuant to the terms of the Agreement, Vendor shall:

3.1.1. unless otherwise agreed by the Parties, do so as an independent Controller, and not a joint Controller with ServiceNow;

3.1.2. represent and warrant that it has all necessary rights and a valid legal basis (as defined by applicable Data Protection Laws) to Process such Personal Data (including but not limited to, where applicable, to disclose Personal Data to ServiceNow)**.** Upon request by ServiceNow, Vendor shall promptly provide proof of its legal basis of Processing;

3.1.3. be solely responsible for any Data Subject requests stemming form the administration of this Agreement, including, but not limited to, requests for access and deletion, it receives with respect to Service Now Personal Data it Processes or any Personal Data it may collect or share with ServiceNow;

3.1.4. fully cooperate and assist ServiceNow in responding to requests related to Data Subject's rights granted under Data Protection Laws, including rights to access, rectify, restrict Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or not be subject to an automated individual decision making (collectively, "***Data Subjects Requests***") upon ServiceNow's request;

at least forty-five (45) days prior to engaging any new or additional third-party that may access ServiceNow Data ("***Third-Party Provider***"), notify ServiceNow by email to vendornotifications@servicenow.com of its intent to use a Third-Party Provider. Such prior notification shall identify the name and the services the Third-Party Provider is engaged to provide. Vendor shall enter into a written agreement with such Third-Party Provider that protects ServiceNow Data to the same standard required of Vendor under this DPA and the Agreement.

4. PROCESSOR OBLIGATIONS

4.1 Where Vendor Processes Personal Data as a Processor pursuant to the terms of the Agreement, Vendor shall:

4.1.1. process Personal Data as required for the provision of Services;

4.1.2. promptly;

4.1.3. When appropriate, promptly notify ServiceNow if it receives any Data Subject Requests made directly by Data Subjects or a Data Subject's representative as permitted by law. Vendor shall not respond to any such Data Subject Request without ServiceNow's prior written consent except to confirm that the request relates to ServiceNow;

4.1.4. When appropriate under 4.1.3, either provide ServiceNow with the ability to fulfill such Data Subject Request independently or shall fully cooperate with ServiceNow so that ServiceNow can respond to such Data Subject Requests within the timeframe required under Data Protection Laws. For the avoidance of doubt, Vendor shall provide all reasonable assistance to ServiceNow in complying with any Data Subject Requests;

4.1.5.

5. INTERNATIONAL DATA TRANSFERS

5.1 The following provisions shall apply when Vendor acts as Controller:

5.1.1 Where ServiceNow (as data exporter) makes a Restricted Transfer to Vendor (as data importer), the Controller SCCs, which are incorporated herein by this reference if such a Restricted Transfer takes place, shall apply to the Parties in respect of such Restricted Transfer. In such case, the information populated in the Controller SCCs set out in Attachment 3 hereof shall also apply.

5.1.2 Notwithstanding the absence of signatures in the Controller SCCs set out in Attachment 3 hereof, the Parties agree that such Controller SCCs are binding on the Parties, as applicable, in the event of a Restricted Transfer. Vendor expressly agrees that ServiceNow may update the details of Processing, including categories of data and categories of data subjects, as described in the Controller SCCs set out in Attachment 3 hereof as necessary to align with its use of the Services from time to time.

5.1.3 Where Vendor (as data exporter) makes a Restricted Transfer to another Controller or Processor, it shall enter into the Controller SCCs or Processor SCCs as applicable in respect of such Restricted Transfer. Vendor shall also ensure that the Processor SCCs are in place in respect of any Restricted Transfer to any of its ultimate Third-Party Providers.

5.2 The following provisions shall apply when Vendor acts as Processor on behalf of ServiceNow:

5.2.1 Where ServiceNow (as data exporter) makes a Restricted Transfer to Vendor (as data importer), the Processor SCCs, which are incorporated herein by this reference if such a Restricted Transfer takes place, shall apply to the Parties in respect of such Restricted Transfer. In such case, the information populated in the Processor SCCs set out in Attachment 2 hereof shall also apply.

5.2.2 Notwithstanding the absence of signatures in Processor SCCs set out in Attachment 2 hereof, the Parties agree that such Processor SCCs are binding on the Parties, as applicable, in the event of a Restricted Transfer. Vendor expressly agrees that ServiceNow may update the details of Processing, including categories of

data and categories of Data Subjects, as described in the Processor SCCs set out in Attachment 2 hereof as necessary to align with its use of the Services from time to time.

5.2.3 Vendor may not make any transfer of Personal Data relating to the Services to a Controller (other than ServiceNow). Where Vendor (as data exporter) makes a Restricted Transfer to a permitted Sub-Processor, it shall enter into a contract with such Sub-processor which contains the provisions in the Processor SCCs. Vendor shall also procure that the Processor SCCs are in place in respect of any Restricted Transfer to any of its ultimate Sub-Processors.

5.3 Clauses 5.1 or 5.2 above shall not apply to a Restricted Transfer if other compliance steps (which may include, but shall not be limited to, obtaining explicit consents from Data Subjects) have been taken to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Laws. Vendor expressly agrees that it shall provide evidence of such other compliance steps (e.g., consents of Data Subjects) upon ServiceNow's request.

5.4 Where applicable, Vendor warrants that during the term of the Agreement, it shall maintain EU – US and Swiss – US Privacy Shield certification and comply with its obligations under the Privacy Shield Framework set forth by the United States Department of Commerce with respect to the Processing of Personal Data transferred from the EEA and Switzerland to the United States.

6. SECURITY

Vendor shall have in place appropriate technical and organizational security measures to safeguard ServiceNow Data, including Personal Data, for protection of the security, confidentiality and integrity of such data, as further described in the Data Security Exhibit attached hereto as Attachment 1 and incorporated herein by this reference.

7. BREACH OBLIGATIONS

7.1 NOTIFICATION REQUIREMENTS. Vendor shall notify ServiceNow of any confirmed accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to ServiceNow Data, including Personal Data contained therein, ("***Breach***") within seventy-twor (72) hours of becoming aware of such Breach. Vendor's notification must:

7.1.1. describe the nature of the Breach including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of records concerned;

7.1.2. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

7.1.3. describe the likely consequences of the Breach;

7.1.4. describe the measures taken or proposed to be taken by Vendor to address the Breach, including, where appropriate, measures to mitigate its possible adverse effects; and

7.1.5. include relevant logs, alerts, indicators of compromise, intelligence and other relevant content that is material to the investigation of the Breach.

7.2 COOPERATION. Where ServiceNow is investigating an actual Breach, Vendor shall cooperate with ServiceNow, such cooperation shall include, providing any necessary information to assist in ServiceNow's investigation. Vendor agrees that ServiceNow may conduct a risk assessment at any time where it becomes aware of a Breach. In the event ServiceNow suspects or discovers a Breach in its use of Vendor's Services, ServiceNow shall contact Vendor's designated contact listed below in this Clause 7.2. Vendor shall notify ServiceNow of any changes to the contact information during the term of the Agreement.

7.3 Please provide the contact information of personnel or team responsible for data security and privacy (e.g., data protection officer, data security officer or other privacy or security personnel):

Name/Group: _____
Email: _____
Address: _____
Telephone Number: _____

8. AUDITS

Vendor shall provide access to and make available all information ServiceNow may need to ensure Vendor's compliance with the Agreement that ServiceNow conducts.

9. FURTHER VENDOR COVENANTS

9.1 Without prejudice to Clauses 2 and 3 of this DPA and where ServiceNow provides Vendor with Personal Data, Vendor shall only retain, use or disclose such Personal Data for the specific purpose of performing the Services and Vendor expressly agrees that it is prohibited from using such Personal Data for any other purpose, commercial or otherwise. Vendor expressly agrees that it shall not sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, ServiceNow Data, including any Personal Data contained therein, for monetary or other valuable consideration.

9.2 Vendor shall provide full cooperation and assistance to ServiceNow to satisfy ServiceNow's compliance obligations to respond to inquiries, investigations or requests made by a supervisory authority (as defined by Data Protection Laws), in relation to the Personal Data Vendor Processes pursuant to the Agreement.

9.3 When allowed by law, Vendor shall promptly notify ServiceNow in the case of an investigation by a government official, audit or inquiry by a data protection authority or any law enforcement agency regarding the Processing of Personal Data, unless prohibited by applicable law.

9.4 Vendor shall ensure that all Vendor personnel with access to Personal Data are subject to a duty of confidence, have received appropriate training on their privacy and security responsibilities, and only access such data to perform their duties.

9.5 Vendor shall keep detailed records of its Processing activities pursuant to the Agreement and this DPA, and shall make those records available to ServiceNow at ServiceNow's request.

9.6 Vendor shall return all ServiceNow Data at any time during the term of the Agreement upon ServiceNow's request and provide ServiceNow with thirty (30) days to request the return of ServiceNow Data ("***Return Period***") after termination or expiration of the Agreement. Vendor shall promptly, but in no event later than thirty (30) days after the Return Period, delete all ServiceNow Data. Upon request by ServiceNow, Vendor shall promptly provide a certificate of deletion of all ServiceNow Data.

9.7 Upon ServiceNow's request, Vendor agrees to enter into additional terms as may be required by Data Protection Law.

10. MISCELLANEOUS

This DPA constitutes the complete and exclusive understanding and agreement of the Parties with respect to the subject matter herein. Any waiver, modification or amendment of any provisions of this DPA will be effective only if in writing and signed by the Parties hereto.

[signature page follows]

IN WITNESS WHEREOF, the parties have executed this DPA as of the DPA Effective Date:

SERVICENOW, INC.:	**VENDOR:**
By:	By:
Name:	Name:
Title:	Title:
Date:	Date:

///
///
///
Remainder of page intentionally left blank.

ATTACHMENT 1
DATA SECURITY EXHIBIT

This Data Security Exhibit describes the minimum technical, organizational and physical security measures Vendor takes to protect ServiceNow Data. Capitalized terms not otherwise defined in this Data Security Exhibit will have the meaning given to them in other parts of the DPA.

1. SECURITY PROGRAM

While providing Services, Vendor will maintain a written information security program of policies, procedures and controls governing the Processing, transmission and security of ServiceNow Data (the "***Security Program***") to protect ServiceNow Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.

Vendor shall regularly test, assess and evaluate the effectiveness of the Security Program and at least annually review and update the Security Program to address new and evolving security technologies, changes to industry standard practices, and changing threats to the security, confidentiality and integrity of ServiceNow Data, and to ensure that these risks are addressed. For clarity, no such update shall materially reduce the commitments, protections or overall level of service provided to ServiceNow 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 ServiceNow Data.

2.2. TECHNICAL SECURITY MEASURES.

2.2.1. Access Administration. Access to ServiceNow Data by Vendor's employees and contractors is protected by authentication and authorization mechanisms. User authentication is required to gain access to ServiceNow Data. 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 Services provides user and role-based access controls.

2.2.3. Logging and Monitoring. Vendor logs activities, which are centrally collected and secured to prevent tampering and are monitored for anomalies by a trained security team. Upon request, Vendor shall promptly make such logs available to ServiceNow.

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

2.2.5. Vulnerability Management. Vendor conducts periodic independent security risk evaluations to identify critical information assets, assess threats to such assets, determine potential vulnerabilities, and remediate any identified vulnerabilities in a timely manner. When software vulnerabilities are revealed and addressed by a vendor patch, Vendor will obtain the patch from the applicable vendor and apply it promptly and only after such patch is tested and determined to be safe for installation in all production systems.

2.2.6. Antivirus. Vendor 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. Vendor ensures that only authorised changes are made to the platform, applications and production infrastructure. The risk to ServiceNow Data shall be assessed and the results of the assessment documented.

2.2.8. Data Separation. ServiceNow Data shall be maintained in a separate environment from Vendor's other customers and Vendor's corporate infrastructure.

2.2.9. Encryption. ServiceNow data shall be encrypted in transit and at rest in line with Industry best practice guidelines.

2.3. ADMINISTRATIVE SECURITY MEASURES.

2.3.1. Data Center Inspections. Vendor must perform routine reviews at each data center to ensure that it continues to maintain the security controls necessary to comply with the Security Program. Where Vendor uses a third-party data center provider, Vendor must perform, at least an annual assessment, to include, where possible an onsite review of the security controls at each data center to ensure continued compliance to the agreements in place, including the DPA and this Data Security Exhibit.

2.3.2. Personnel Security. Vendor performs background screening on all employees and all contractors who have access to ServiceNow Data, subject to applicable law.

2.3.3. Security Awareness and Training. Vendor maintains a privacy and security awareness program that includes appropriate training of Vendor personnel on data privacy and the Security Program. Training is conducted at time of hire and at least once per year.

2.3.4. Vendor Risk Management. Vendor maintains a vendor risk management program that assesses all vendors that access, store, process or transmit ServiceNow Data for appropriate security controls and business disciplines.

3. SERVICE CONTINUITY AND DISASTER RECOVERY

Vendor shall implement and document appropriate and adequate business continuity and disaster recovery plans to ensure that Vendor can continue to or resume providing the Services promptly after a disruptive event. Vendor will regularly test and monitor the effectiveness of its business continuity and disaster recovery plans at least annually or as otherwise requested by ServiceNow. Vendor shall provide ServiceNow with its written business continuity and disaster recovery plan upon request.

4. CERTIFICATIONS AND AUDITS

4.1. CERTIFICATIONS AND ATTESTATIONS. Vendor 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 Services. At least once per calendar year, Vendor shall obtain an assessment against such Standards by an independent third-party auditor.

4.2. AUDITS AND CORRECTIVE ACTIONS.

4.2.1. Audits. Vendor shall make available to ServiceNow all information necessary to demonstrate compliance with its obligations under the Agreement and this Data Security Exhibit and allow for and contribute to audits, including remote inspections, conducted by ServiceNow or another auditor mandated by ServiceNow.

4.2.2. Corrective Actions. Upon request by ServiceNow**,** Vendor shall discuss the results of the audit conducted pursuant to Clause 4.2.1 (Audits) above.

5. MONITORING AND INCIDENT MANAGEMENT

5.1. MONITORING, MANAGEMENT AND NOTIFICATION.

5.1.1. Incident Monitoring and Management. Vendor will monitor, analyze and respond to security incidents promptly.

5.1.2. Breach Notification. Vendor will report to ServiceNow any Breach without undue delay but in no event later than seventy-two (72) hours of becoming aware a Breach has occurred.

5.1.3. Report. The initial report will be made to ServiceNow's security and legal teams at: security@servicenow.com and legal@servicenow.com respectively. As information is collected or otherwise becomes available to Vendor, and unless prohibited by applicable law, Vendor shall provide any further information regarding the nature and consequences of the Breach to allow ServiceNow 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 Vendor contact from whom additional information may be obtained. Vendor shall inform ServiceNow of the measures that it will adopt to mitigate the cause of the Breach and to prevent future Breaches.

///
///
///
Remainder of page intentionally left blank.

PROCESSOR DETAILS

ATTACHMENT 2

For the purposes of the Standard Contractual Clauses (processors), the data exporter and data importer information are as follows:

Data Exporter: **Name of the data exporting organization:** *ServiceNow, Inc. and its Affiliates*	*Data Importer:* **Name of the data importing organization:** *The Vendor listed above*
Address: *2225 Lawson Lane, Santa Clara, CA 95054 U.S.A.* *(ServiceNow U.S.A. headquarters)*	**Address**: *Address of the Vendor listed above in Clause 7.3 of the DPA*
Tel.: *+1 (408) 501 - 8550*	**Tel**.: *Phone number of the Vendor listed above in Clause 7.3 of the DPA*
Other information needed to identify the organization: N/A	**Other information needed to identify the organization**:

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

This Appendix 1 forms part of the Clauses and must be completed and signed by the parties. Vendor agrees that this ServiceNow may update this Appendix 1 at any time with notice to Vendor.

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 exporter is (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and, (ii) all affiliates of the data exporter either established within the European Economic Area (EEA) and Switzerland or with data subjects based in the EEA and Switzerland that use the services provided by Data Importer as set forth in the underlying agreement for services between the data exporter and data importer (the "Agreement").

Data importer

The data importer is (please specify briefly activities relevant to the transfer):
Data Importer is the entity providing Services to ServiceNow pursuant to the Agreement.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):
The Data Exporter may submit Personal Data, which may include, but is not limited to Personal Data relating to the following categories of Data Subjects: Data exporter's customers and other business contacts; employees and contractors; subcontractors and agents; consultants, prospects and event sponsors and attendees.

Categories of data

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

The Data Exporter may submit Personal Data, which may include, but is not limited to the following categories of Personal Data: first and last name; employer; business role; professional title; department; business contact information (e.g., email, phone, physical address); business network; business experience and; business interests, localization data, connection data, other communication data; and other Personal Data Processed during the use of the Services.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):
The Data Exporter may submit Special Categories of Personal Data, incuding sensitive data, which may include, but is not limited to 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 Processing operations include:

The Data Importer shall Process Personal Data in its provision of the Services pursuant to the terms of the Agreement.

DATA EXPORTER Name: Authorised Signature:	**DATA IMPORTER** Name: Authorised Signature:

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

This Appendix 2 forms part of the Standard Contractual Clauses (processors) 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 measures shall, at a minimum, include those measures set forth in Attachment 1 of this DPA (Data Security Exhibit).

DATA EXPORTER Name: Authorised Signature:	**DATA IMPORTER** Name: Authorised Signature:

CONTROLLER DETAILS

ATTACHMENT 3

For the purposes of the Standard Contractual Clauses (controllers), the data exporter and data importer information are as follows:

Data Exporter: **Name of the data exporting organization:** *ServiceNow, Inc. and its Affiliates*	*Data Importer:* **Name of the data importing organization:** *The Vendor listed above*
Address: *2225 Lawson Lane, Santa Clara, CA 95054 U.S.A.* *(ServiceNow U.S.A. headquarters)*	**Address**: *Address of the Vendor listed above in Clause 7.3 of the DPA*
Tel.: *+1 (408) 501 - 8550*	**Tel**.: *Phone number of the Vendor listed above in Clause 7.3 of the DPA*
Other information needed to identify the organization: N/A	**Other information needed to identify the organization**:

ANNEX B TO THE STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA FROM THE COMMUNITY TO THIRD COUNTRIES (CONTROLLER TO CONTROLLER TRANSFERS)

DESCRIPTION OF THE TRANSFER

Vendor agrees that this ServiceNow may update this Appendix 1 at any time with notice to Vendor.

Data Subjects
The personal data transferred concern the following categories of data subjects:

Data exporter's customers and other business contacts; employees and contractors; subcontractors and agents; consultants, prospects and event sponsors and attendees.

Purposes of the transfer(s)
The transfer is made for the following purposes:

Provide services to ServiceNow pursuant to the Agreement.

Categories of Data
The personal data transferred concern the following categories of data:

The Data Exporter may submit Personal Data, which may include, but is not limited to the following categories of Personal Data: first and last name; employer; business role; professional title; department; business contact information (e.g., email, phone, physical address); business network; business experience and; business interests, localization data, connection data, other communication data; and other Personal Data Processed during the use of the Services.

Recipients
The personal data transferred must be disclosed only to the following recipients or categories of recipients:

Data importer and its approved Sub-Processors.

Sensitive data **(if appropriate)**
The personal data transferred concern the following categories of sensitive data:

Data protection registration information of data exporter (where applicable)
N/A

Additional useful information **(storage limits and other relevant information)**

Contact points for data protection inquires:

Please see above.

///
///
///
Remainder of page intentionally left blank.