



Data Protection Agreement

Applies to Customer's Personal Data

This Data Protection Agreement ("**DPA**"), forms part of the Agreement (as defined below) and applies where, and to the extent that, Cisco Processes Personal Data as a Processor for You when providing Cisco Offers (as defined below) under the Agreement, (each a "**Party**" and together the "**Parties**").

This DPA will become effective on the Effective Date and remain in force for the term of Agreement.

Unless otherwise specified in this DPA, the terms of the Agreement will continue in full force and effect. All capitalized terms not defined in Section 1 or otherwise in this DPA will have the meanings set forth in the Agreement. Any privacy or data protection related clauses or agreement previously entered into by Cisco and You, with regards to the subject matter of this DPA, will be superseded by and replaced with this DPA. No one other than a Party to this DPA, their successors and permitted assignees will have any right to enforce any of its terms.

1. Definitions

- 1.1. "**Affiliates**" means, any corporation or company that directly or indirectly controls, or is controlled by, or is under common control with the relevant party, where "control" means to: (a) own over 50% of the relevant party; or (b) be able to direct the affairs of the relevant party through voting rights or other lawful means (e.g., a contract that allows control). Unless otherwise explicitly agreed by the Parties, any legal entities which become part of the Cisco group of companies through an acquisition or merger (each an "**Acquired Entity**") are not considered Cisco Affiliates for the purposes of this DPA unless the Cisco Offers of such Acquired Entity are available for You to purchase on the applicable Price List.
- 1.2. "**Agreement**" means the written or electronic agreement between You and the applicable Cisco entity for the provision of the Cisco Offers to You or any other terms where the parties expressly agree to this document (e.g.: the Cisco General Terms ("**General Terms**")). For the avoidance of doubt, where You have purchased a Cisco Offer from a Cisco Partner, "Agreement" means the General Terms.
- 1.3. "**Cisco**" means the applicable Cisco entity that is party to the Agreement.
- 1.4. "**CCPA**" means the California Consumer Privacy Act (Cal. Civ. Code §§ 1798.100 to 1798.199) as amended by the California Privacy Rights Act ("**CPRA**"), and any related regulations or guidance provided by the applicable regulators.
- 1.5. "**Cisco Offer**" means Cisco branded (a) hardware, (b) usage rights in software or cloud services, (c) technical support included in a subscription offer and (d) incidental technology and resources acquired by You.
- 1.6. "**Controller**" means an entity that determines the purposes and means of the processing of Personal Data. It will have the same meaning ascribed to "controller" under the GDPR and other equivalent terms under applicable Data Protection Laws (e.g.: "Business" as defined under the CCPA), as applicable.
- 1.7. "**Customer**" or "**You**" means the Party identified in the Agreement receiving Cisco Offers from Cisco under the Agreement.
- 1.8. "**Data Breach**" means a breach of the Information Security Exhibit, leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.
- 1.9. "**Data Protection Laws**" means all mandatory applicable laws that apply to the Processing of Personal Data under the Agreement.
- 1.10. "**Data Subject**" means the individual to whom Personal Data relates (e.g.: "Consumer" as defined under the

CCPA).

- 1.11. **“GDPR”** means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons regarding the processing of Personal Data and on the free movement of such data (General Data Protection Regulation).
- 1.12. **“Information Security Exhibit”** means the document describing the measures that Cisco implements to secure Personal Data, which can be found [here](#).
- 1.13. **“Personal Data”** means any information about, or related to, an identified or identifiable natural person Processed by Cisco and/or its Affiliates on behalf of You. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual, natural person.
- 1.14. **“Price List”** means the price lists published at Cisco.com corresponding to the Cisco entity that sells the applicable Cisco Offer.
- 1.15. **“Privacy Data Sheet(s)”** and **“Offer Disclosure(s)”** means the applicable document located on Cisco’s [Trust Portal](#) that describes the Processing activities in relation to the Cisco Offer(s) supplied to You under the Agreement. If a Privacy Data Sheet or an Offer Disclosure is attached to or referenced in this DPA, this DPA only refers to Cisco’s role as a Processor as detailed in the respective Privacy Data Sheet or Offer Disclosure, unless the Parties have explicitly agreed otherwise herein.
- 1.16. **“Processing”** means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, recording, securing, organization, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction. **“Processes”** and **“Process”** will be construed accordingly.
- 1.17. **“Processor”** means an entity that processes Personal Data on behalf of a Controller. It will have the same meaning ascribed to “processor” under the GDPR and other equivalent terms under other Data Protection Laws (e.g.: “Service Provider” as defined under the CCPA), as applicable.
- 1.18. **“Representatives”** means either Party’s (including its Affiliates’) officers, directors, employees, agents, contractors, temporary personnel, subcontractors and consultants.
- 1.19. **“Subprocessor”** means another Processor engaged by Cisco to carry out Processing of Your Personal Data, as set forth in the applicable Privacy Data Sheet(s) or Offer Disclosure(s).

2. Processing of Personal Data

- 2.1. The Parties agree that, for this DPA, (i) You will be the Controller and Cisco will be the Processor and/or (ii) You will be the Processor and Cisco will be a further Processor.
- 2.2. Cisco Processes Personal Data as part of this DPA as follows:
 - a. The duration of the Processing under this DPA is determined by You and as set forth in the Agreement.
 - b. The purpose of the Processing under DPA is the provision of the Cisco Offers by Cisco to You as specified in the Agreement and as further detailed in the respective Privacy Data Sheet(s) or Offer Disclosure(s).
- 2.3. You will:
 - a. use the Cisco Offers in compliance with Data Protection Laws;
 - b. ensure all instructions given by You to Cisco in respect of the Processing of Personal Data are at all times in accordance with Data Protection Laws;
 - c. ensure all Personal Data provided to Cisco has been collected in accordance with Data Protection Laws and that You have all authorizations and/or consents necessary to provide such Personal Data to Cisco;
 - d. keep the amount of Personal Data provided to Cisco to the minimum necessary for the provision of the Cisco Offers;and

- e. when acting as a Processor, be responsible for passing on to the Controller all the information, assistance and notices needed to comply with its obligations as a Controller under Data Protection Laws, as well as the details of the applicable Privacy Data Sheets or Offer Disclosures, given that You are the Party having a direct relationship with the Controller; and be responsible for passing on to Cisco all Controller's requests and instructions related to the Processing of Personal Data under this DPA.

2.4. Cisco will:

- a. only Process Personal Data in accordance with Data Protection Laws, the applicable Privacy Data Sheet(s) or Offer Disclosure(s), the Information Security Exhibit, this DPA, and any other of Your agreed documented instructions. Cisco will promptly notify You if Cisco reasonably believes that any of Your instructions are inconsistent with Data Protection Laws;
- b. ensure its applicable Representatives who may Process Personal Data have written contractual obligations in place with Cisco to keep the Personal Data confidential or are under an appropriate statutory obligation of confidentiality;
- c. appoint data protection lead(s). Upon request, Cisco will provide the contact details of the appointed person(s);
- d. assist You as reasonably needed to respond to requests from supervisory authorities, Data Subjects, customers, or others to provide information related to Cisco's Processing of Personal Data;
- e. if required by Data Protection Laws, court order, subpoena, or other legal or judicial process to Process Personal Data other than in accordance with Your instructions, notify You without undue delay of any such requirement before Processing the Personal Data (unless mandatory applicable law prohibits such notification, in particular on important grounds of public interest);
- f. maintain records of the Processing of any Personal Data received from You under the Agreement;
- g. not lease, sell, distribute, or otherwise encumber Personal Data unless mutually agreed to by the Parties in a separate agreement;
- h. not combine Personal Data received from or on behalf of You and Personal Data collected by Cisco's own interactions with the Data Subject other than as provided in the Agreement or as otherwise permitted by Data Protection Laws;
- i. provide such assistance as You reasonably require (either on its own behalf or on behalf of its customers), and Cisco or a Representative is able to provide, in order to meet any applicable filing, approval or similar requirements in relation to Data Protection Laws;
- j. provide such information and assistance as You reasonably require (taking into account the nature of Processing and the information available to Cisco) to enable Your compliance with Your obligations under Data Protection Laws with respect to:
 - i. security of Processing;
 - ii. data protection impact assessments (as such term is defined by the GDPR);
 - iii. prior consultation with a supervisory authority regarding high-risk Processing; and
 - iv. notifications to the applicable supervisory authority and/or communications to Data Subjects by You in response to any Data Breach;
- k. on termination of the DPA for whatever reason, cease to Process Personal Data, and upon Your written request and without undue delay, (i) return, or make available for return, Personal Data in its possession or control, or (ii) securely delete or permanently render unreadable or inaccessible existing copies of the Personal Data; unless continued retention and Processing is required or is permitted by Data Protection Laws and/or mandatory applicable law. At Your request, Cisco will give You confirmation in writing that it has fully complied with this Section 2.4 (k) or provide a justification as to why such compliance is not feasible.

3. Transfers of Personal Data

Cisco may transfer and Process Personal Data to and in locations where Cisco or its Subprocessors Process Personal Data to provide the Cisco Offers, as further detailed in the respective Privacy Data Sheet(s) or Offer Disclosure(s). Cisco will

conduct such transfers in accordance with the transfer mechanisms set out at Cisco's [DPA Portal](#), which in any event will be subject to the terms and conditions of this DPA. Any further changes to such transfer mechanisms approved with an official decision by the applicable competent authority will be incorporated by reference to this DPA and a copy of the new transfer mechanism will be available at Cisco's DPA Portal.

4. Subprocessing

- 4.1. Where Cisco appoints a Subprocessor, Cisco will execute a written agreement with the Subprocessor containing terms at least as protective as this DPA. Current Subprocessor(s) are listed in the applicable Privacy Data Sheet(s) or Offer Disclosure(s).
- 4.2. Cisco will not subcontract its obligations under this DPA to new Subprocessors, in whole or in part, without providing You with at least 30 days advance notice (e.g.: by publishing this information at Cisco's [Trust Portal](#) and/or by email upon Your subscription at Cisco's [Trust Portal](#)) and an opportunity to object. If within 10 days of Cisco's notice, You object to the proposed subcontracting by providing reasonable grounds related to the protection of the Personal Data and the Parties cannot resolve the objection within 30 days of Cisco's notice, then You may on written notice, terminate the applicable part of the Agreement and/or purchase order relating to those Cisco Offers which cannot be provided by Cisco without the use of the Subprocessor(s) giving rise to the objection.
- 4.3. Cisco will be liable for the acts or omissions of Subprocessors to the same extent it is liable for its own actions or omissions under this DPA.

5. Rights of Data Subjects

Data Subject requests. To the extent legally permitted, Cisco will promptly redirect the Data Subjects to send their requests to You or notify You if it receives a Data Subject request. Unless required by Data Protection Laws, Cisco will not respond to any such Data Subject request without Your prior written consent except to redirect the Data Subject request to You. Cisco will provide such information and cooperation and take such action as You reasonably request in relation to a Data Subject request.

6. Security

Controls for the protection of Personal Data. Cisco will implement and maintain the security measures specified in the Information Security Exhibit and regularly monitor compliance with these security measures.

7. Audits and Certifications

Upon Your written request, and subject to the confidentiality obligations set forth in the Agreement, Cisco will make available to You reasonably necessary information to demonstrate Cisco's compliance with the obligations of this DPA and Data Protection Laws, in accordance with the Information Security Exhibit, including copies of third-party audit reports or certifications it maintains in the ordinary course of business (such as SOC1, SOC2, SOC3 attestations, or ISO 27001:2013 certifications, or their equivalent under any successor standards) that apply to the relevant Cisco Offer. The security certifications that Cisco holds for the Cisco Offers can be found on Cisco's [Trust Portal](#).

8. Notification and Communication

- 8.1. Notification. Cisco will notify You within 48 hours of confirmation of a Data Breach relating to Your Personal Data. Cisco will provide all such timely information and cooperation as You may reasonably require for You to fulfil Your Data Breach reporting obligations under (and in accordance with the timescales required by) Data Protection Law. Cisco will further take such measures and actions as it considers necessary or appropriate to remedy or mitigate the effects of the Data Breach and will keep You informed in connection with the Data Breach.
- 8.2. Information Security Communication. Except as required by mandatory applicable law, Cisco agrees that it will not inform any third party of a Data Breach referencing or identifying You, without Your prior written consent. Cisco will reasonably cooperate with You and law enforcement authorities concerning a Data Breach. Cisco will retain, for an appropriate period of time, all information and data within Cisco's possession or control that is directly related to any Data Breach. If disclosure of the Data Breach referencing or identifying You is required by mandatory applicable law, Cisco will work with You regarding the timing, content, and recipients of such disclosure.

- 8.3. Post-incident. Cisco will reasonably cooperate with You in any post-incident investigation, remediation, and communication efforts.
- 8.4. Complaints or notices related to Personal Data. If Cisco receives any official complaint, notice, or communication that relates to Cisco's Processing of Personal Data or either Party's compliance with Data Protection Laws in connection with Personal Data, to the extent legally permitted, Cisco will promptly notify You and, to the extent applicable, Cisco will provide You with commercially reasonable cooperation and assistance in relation to any such complaint, notice, or communication.

9. Liability

- 9.1. Each Party's respective direct liability to Data Subjects or applicable supervisory data protection authorities which cannot be limited or excluded by mandatory applicable law will be unlimited.
- 9.2. Except for any liability which cannot be limited or excluded under mandatory applicable law, the aggregate liability of Cisco for all Data Breaches and any breach of this DPA (whether for breach of contract, misrepresentations, negligence, strict liability, other torts or otherwise) will not exceed US\$1,000,000.
- 9.3. Where a Data Breach and/or breach of this DPA is also a breach of any confidentiality or non-disclosure obligations in the Agreement, the liability cap in Section 9.2 will apply.