

## European Union General Data Protection Regulation Policy

This European Union General Data Protection Regulation Policy (the “**GDPR Policy**”) is incorporated into the End User Subscription Agreement between the parties (the “**Agreement**”), and details the additional terms and conditions that apply to Carbon Black Inc. (“**Carbon Black**”) processing of Personal Data as required by Article 28 of the General Data Protection Regulation. All capitalized terms not defined in this GDPR Policy will have the meanings set forth in the Agreement. This GDPR Policy is effective as of the effective date of the Agreement (“**Effective Date**”).

### 1. Definitions.

- a. “General Data Protection Regulation” or “GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- b. “Personal Data” means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- c. “Subprocessor” means other processors used by Carbon Black to process data.
- d. The terms “data subject”, “processing”, “processor”, and “supervisory authority” as used herein have the meanings given in the GDPR.

### 2. Processing of Personal Data.

For purposes of this GDPR Policy, Customer and Carbon Black agree that Customer is the controller of Personal Data and Carbon Black is the processor of such data, except when Customer acts as a processor of Personal Data, in which case Carbon Black is a subprocessor to Customer. This GDPR Policy applies to the processing of Personal Data, within the scope of the GDPR, by Carbon Black on behalf of Customer. The GDPR Policy does not limit or reduce any data protection commitments Carbon Black makes to Customer in the Agreement between Carbon Black and Customer. The GDPR Policy does not apply where Carbon Black is a controller of Personal Data.

### 3. Relevant GDPR Obligations: Articles 28, 32, and 33.

- a. Carbon Black may engage Subprocessors to provide certain services on its behalf. As applicable, Carbon Black will provide advanced notice of the name and location of such Subprocessor. If Customer continues on to utilize such services after receipt of such notice, or does not object to such Subprocessor within 30 days of the notice, Customer will be deemed to approve of the sub-processing by the Subprocessor. By executing the Agreement, Customer consents to (i) Carbon Black’s use of the Subprocessors detailed in the current (as of the Effective Date of this GDPR Addendum) Third Party Subprocessors’ List , and (ii) Carbon Black engaging its controlled subsidiaries as Subprocessors (list available upon request) at its discretion (together, referred to as “Approved Subprocessors”).

- b. Processing by Carbon Black shall be governed by this GDPR Policy under European Union (hereafter “Union”) or Member State laws binding on Carbon Black with regard to Customer. The Personal Data processing details are:
- The subject-matter of the processing is limited to Personal Data within the scope of the GDPR;
  - The duration of the processing shall be for the duration of the Customer’s right to use the Products and until all Personal Data is deleted or returned in accordance with Customer instructions or the terms of the Agreement;
  - The nature and purpose of the processing shall be to provide the applicable Product(s) pursuant to the Agreement;
  - The types of Personal Data processed may include elements listed in the Documentation; and
  - The categories of data subjects are Customer’s representatives and end users, such as employees, contractors, collaborators, and customers.
- c. Carbon Black shall:
- (1) process the Personal Data only on documented instructions from Customer (which includes those instructions specified in the Agreement), unless required to do so by Union or Member State law to which Carbon Black is subject; in such a case, Carbon Black shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
  - (2) ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
  - (3) take all measures required pursuant to Article 32 of the GDPR;
  - (4) taking into account the nature of the processing, assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer’s obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR. If Carbon Black receives a request from Customer’s data subject to exercise their rights under the GDPR, Carbon Black will redirect the data subject to make such request directly to Customer;
  - (5) assist Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to Carbon Black;
  - (6) delete or, upon Customer’s request, return all the Personal Data to Customer after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the Personal Data. Carbon Black may retain contact details, being names, e-mail addresses, mail addresses, and telephone numbers, exchanged by the parties and other administrative information related to the provision of the Services for the purposes of administering the terminated business relationship as per Carbon Black’s records retention schedule.
  - (7) make available to Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer.
- d. Carbon Black shall immediately inform Customer if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

- e. Where Carbon Black engages a Subprocessor for carrying out specific processing activities on behalf of Customer, the same data protection obligations as set out in the GDPR Policy shall be imposed on that Subprocessor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor fails to fulfil its data protection obligations, Carbon Black shall remain fully liable to the Customer for the performance of that other processor's obligations.
- f. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Customer and Carbon Black shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
- (1) the pseudonymisation and encryption of Personal Data;
  - (2) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  - (3) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
  - (4) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
- g. In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.
- h. Customer and Carbon Black shall take steps to ensure that any natural person acting under the authority of Customer or Carbon Black who has access to Personal Data does not process them except on instructions from Customer, unless he or she is required to do so by Union or Member State law.
- i. Carbon Black shall notify Customer without undue delay after becoming aware of a personal data breach. Such notification will include that information a processor must provide to a controller under GDPR Article 33(3) to the extent such information is available to Carbon Black.
- j. Carbon Black may transfer and process Personal Data in the United States or any other country where Carbon Black or its controlled subsidiaries or Subprocessors operate. Customer appoints Carbon Black to perform any such transfer of Personal Data in compliance with GDPR. Carbon Black represents that it is EU-U.S. and Swiss-U.S. Privacy Shield Framework certified (Certification available at <https://www.privacyshield.gov/participant?id=a2zt0000000TRgHAAW&status=Active>) and complies with onward transfer provisions. In case the EU-U.S. and/or Swiss-U.S. Privacy Shield framework ceases to exist or Carbon Black is no longer certified, Carbon Black shall execute other available data transfer mechanism, such as the EU Standard Contractual Clauses.