# Data Protection Agreement

Version Date: March, 2023

This Data Protection Agreement ("DPA") supplements any existing and currently valid Wazuh Support Agreement, Master Services Agreement, Partner Program Terms or other similar agreement (each "Agreement") previously made between Wazuh, Inc. ("Wazuh") and Customer (defined below) (collectively, the "Parties"), if and to the extent: (i) this DPA is required under Applicable Laws (defined below), and (ii) Wazuh Processes Customer Personal Data (both defined below). This DPA supersedes and replaces any prior data protection agreement, or any other prior understanding or agreement, related to the processing of Customer Personal Data in connection with the Agreement.

For avoidance of doubt, execution of this DPA shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses (defined below) incorporated herein by reference.

## 1. Definitions

**1.1.** Capitalized terms not otherwise defined hereunder shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect. Cognate terms shall be construed to have the same meaning.

"Applicable Laws" means any laws that regulate the Processing, privacy or security of Customer Personal Data and that are directly applicable to each respective party to this DPA in the context of Wazuh Processing Customer Personal Data;

"CCPA" means the California Consumer Privacy Act of 2018 (Cal. Civil Code § 1798.100 et seq.), including, but not limited to, amendments of the CCPA or applicable regulations promulgated by the California Privacy Protection Agency;

"Customer" means (i) the person or entity that is indicated below in the signature block, or (ii) if there is no signature block or it is not completed, then Customer is the person or entity that has entered into the Agreement with Wazuh. Customer also means a Customer Affiliate when: (i) Applicable Laws require a direct relationship between Wazuh and the Customer's Affiliate with respect to data protection agreements, (ii) Customer is duly and effectively authorized (or subsequently ratified) to act on its Affiliate's behalf, and (iii) Wazuh processes the Affiliate's Customer Personal Data;

"Customer Personal Data" means any Personal Data Processed by Wazuh or a Subprocessor on behalf of the Customer in the provision of the Services;

"GDPR" means the General Data Protection Regulation 2016/679 ("GDPR") and any local laws implementing or supplementing the GDPR;

“Onward Transfer” means any transfer of Customer Personal Data from Wazuh to a Subprocessor;

“Personal Data” means any data or information that: (a) is linked or reasonably linkable to an identified or identifiable natural person; or (b) is otherwise “personal data,” “personal information,” “personally identifiable information,” or similarly defined data or information under Applicable Data Protection Laws.

"Restricted Transfer" means any export of Customer Personal Data by Customer to Wazuh from its country of origin, either directly or via onward transfer, to a third country in the course of Wazuh’s provision of the Services under the Agreement that is prohibited under Applicable Laws, unless (a) the destination has been recognized as providing an adequate level of data protection by competent data protection authority, or otherwise in a legally binding way, or (b) Wazuh has adopted an appropriate, under Applicable Laws recognized, adequacy mechanism ensuring an adequate level of data protection;

“Services” Shall mean the services and other activities to be supplied to or carried out by Wazuh pursuant to the Agreement.

“Standard Contractual Clauses” means the standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR as to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021; and

"Subprocessor" means any contracted service provider (including any third party and Wazuh Affiliate but excluding an employee of Wazuh or Wazuh sub- contractors unless specified in an applicable Statement of Work) Processing Customer Personal Data in the course of Wazuh’s provisioning of the Services set forth in the Agreement.

**1.3.** The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", “Processor”, "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR. The terms “Exporter” and “Importer” shall have the same meaning as in the Standard Contractual Clauses. The terms “Business,” “Business Purpose,” “Collects,” “Consumer,” “Contractor,” “Person,” “Personal Information,” “Processing,” “Sell,” “Service Provider,” “Share,” and “Third Party” shall have the meaning set forth in the CCPA.

**1.4.** The following terms in the GDPR and the CCPA are understood and construed to have the same meaning: “Controller” and “Business,” “Data Subject” and “Consumer,” “Processor” and “Service Provider,” “Person” and “Subprocessor,” and “Personal Data” and “Personal Information.”

**1.5.** The word "include" shall be construed to mean include without limitation.

## 2. Processing of Customer Personal Data

**2.1.** The Parties acknowledge and agree that Wazuh will process Customer Personal Data in providing the Services in accordance with the purposes and means for Processing Customer Personal Data set out in Exhibit A, and in compliance with Applicable Laws at all times.

**2.2.** Wazuh shall:

2.2.1. Process Customer Personal Data solely in accordance with this Agreement, and exclusively on Customer's written instructions as provided below, and as required by Applicable Laws (the "Documented Instructions"). Any additional or alternate instructions, having an impact to the Services must be agreed upon by the Parties separately in writing;

2.2.2. Unless prohibited by Applicable Law, Wazuh shall inform Customer in advance if Wazuh determines that: (i) Customer's instructions conflict with Applicable Laws; or (ii) Applicable Laws require any Processing contrary to the Customer's instructions;

2.3. Wazuh shall not:

2.3.1. Sell or Share Customer Personal Data provided to Wazuh by the Customer for the Processing except where it does so pursuant to Customer's instructions; and

2.3.2.Combine the Personal Data received from or on behalf of Customer with Personal Data Wazuh has received from another Person or has collected from Wazuh's own interaction with a Data Subject, except where the combining of Personal Data is done in order to perform Processing in line with Customer's instructions, or as otherwise permitted under Applicable Laws.

2.4 Customer shall:

2.4.1. Be responsible for complying with Applicable Laws when making decisions and issuing instructions for the Processing of Customer Personal Data, including securing all permissions, consents or authorizations that may be required; and

2.4.2. Defend and indemnify Wazuh, Wazuh Affiliates, and Wazuh Subprocessors for any claim brought against them arising from an allegation of Customer's breach of this section, whether by a Data Subject or a government authority. This provision does not diminish Customer or Data Subject's rights under Applicable Laws related to Wazuh's adherence to its obligations under Applicable Laws. In the event of such a claim, the Parties shall follow the process set forth in the Agreement and if none, then Wazuh will: (i) notify Customer of such claim, (ii) permit Customer to control the defense or settlement of such claim; provided, however, Customer shall not settle any claim in a manner that requires Wazuh to admit liability without Wazuh's prior written consent, and (iii) provide Customer with reasonable assistance in connection with the defense or settlement of such claim, at

Customer's cost and expense. In addition, Wazuh may participate in defense of any claim, and if Customer is already defending such claim, Wazuh's participation will be at Wazuh's expense.

## 3. Wazuh personnel

Wazuh shall take reasonable steps to:

**3.1**. Implement appropriate security controls designed to ensure access to Customer Personal Data is strictly limited to those individuals who need to know/access the relevant Customer Personal Data as reasonably necessary for the purposes outlined in this DPA, the Agreement or required under Applicable Laws; and

**3.2**. Ensure all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

## 4. Security

**4.1**. 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, Wazuh shall in relation to the Processing of Customer Personal Data maintain appropriate technical and organizational measures as specified in the Agreement and designed to ensure a level of security appropriate to the risk, including, as appropriate, the measures referred to in Applicable Laws.

**4.2.** In assessing the appropriate level of security, Wazuh shall take into account the nature of the data and the Processing activities in assessing the risks posed by a potential Personal Data Breach.

## 5. Subprocessing

**5.1**. To the extent required under Applicable Laws, Customer authorizes Wazuh to appoint (and permit each Subprocessor appointed in accordance with this section to appoint) Subprocessors in accordance with this section 6 and any restrictions in the Agreement.

**5.2**. Wazuh may continue to use those Subprocessors already engaged as of the date of this DPA specified in Exhibit E, subject to Wazuh in each case meeting the obligations set out in section 5.5.

**5.3**. Wazuh shall provide notice of a proposed new Subprocessor to Customer, at least 30 days prior to Wazuh's use of the new Subprocessor to Process Customer Personal Data. During the notice period, Customer may notify Wazuh in writing of any reasonable objections to a change in Subprocessor, and Wazuh may, in its sole discretion, attempt to resolve Customer's objection, including providing the Services without use of the proposed Subprocessor. If (a) Wazuh provides

Customer written notice that it will not pursue an alternative, or (b) such an alternative cannot be made available by Wazuh to Customer within 90 days of Customer providing notice of its objection, then in either case, and notwithstanding anything to the contrary in the Agreement or order, Customer may terminate the Agreement or order to the extent that it relates to the Services which require the use of the proposed Subprocessor.

**5.4.** With respect to each Subprocessor, to the extent required under Applicable Laws, Wazuh shall:

5.4.1. Before the Subprocessor first Processes Customer Personal Data (or, where relevant, in accordance with section 5.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Customer Personal Data required by Applicable Laws, this DPA and the Agreement;

5.4.2. Ensure that the arrangement between Wazuh and Subprocessor is governed by a written contract which offers substantially the same level of protection for Customer Personal Data as required by this DPA and Applicable Laws, including Customer's ability to protect the rights of Data Subjects in the event Wazuh is insolvent, liquidated or otherwise ceases to exist;

5.4.3. Apply an adequacy mechanism recognized by Customer's Supervisory Authority as ensuring an adequate level of data protection under Applicable Laws where Subprocessor's Processing of Customer Personal Data involves a Restricted Transfer;

5.4.4. Maintain copies of the agreements with Subprocessors as Customer may request from time to time. To the extent necessary to protect Confidential Information, Wazuh may redact the copies prior to sharing with Customer; and

5.4.5. Notify Customer of Subprocessor's relevant failure to comply with obligations set out by Applicable Laws and this DPA where Wazuh has received notice of such.

## 6. Data subject rights

**6.1**. Customer represents and warrants to provide appropriate transparency to any Data Subjects concerned of Wazuh's Processing of Customer Personal Data and respond to any request filed by Data Subjects as required under Applicable Laws.

**6.2** . Taking into account the nature of the Customer Personal Data Processing, Wazuh shall:

6.2.1. Not respond to the Data Subject request itself or by Subprocessor unless required by Applicable Laws;

6.2.2. Notify Customer without undue delay if Wazuh or any Subprocessor receives a request from a Data Subject under any Applicable Laws in respect to Customer Personal Data; and

6.2.3. Reasonably assist Customer through appropriate technical and organizational measures to fulfill Customer's obligation to respond to Data Subject requests arising under Applicable Law, and where Customer is unable to respond to Data Subject requests through the information available by the Services; and, use, or disclose the Customer Personal Data outside of the relationship between Wazuh and Customer or for a purpose other than outlined in the Agreement to the extent required by Applicable Laws.

## 7. Personal Data breach

**7.1.** Upon Wazuh becoming aware of any Personal Data Breach affecting Customer Personal Data, Wazuh shall without undue delay, and within the timeframes required by Applicable Laws, notify Customer of such Personal Data Breach. To the extent known, Wazuh shall provide Customer with sufficient information to meet obligations under Applicable Laws to report or inform Data Subjects of such Personal Data Breach.

**7.2**. Wazuh shall cooperate with Customer and take commercially reasonable steps to assist in the investigation, mitigation, and remediation of such Personal Data Breach.

## 8. Obligations to assist Customer

Taking into account the nature of the Processing and information available to Customer in each case solely in relation to Wazuh's Processing of Customer Personal Data, Wazuh shall provide reasonable assistance to Customer with any:

**8.1.** Necessary data protection impact assessments required of Customer by Applicable Laws;

**8.2**. Consultation with or requests of a competent data protection authority;

**8.3.** Inquiries about Wazuh's Processing of Customer Personal Data pursuant to the Agreement and this DPA.

## 9. Deletion of Customer Personal Data

**9.1.** Processing of Customer Personal Data by Wazuh shall only take place for the duration specified in Exhibit A.

**9.2**. At the end of the duration specified in Exhibit A or upon termination of the Services and pursuant to the Agreement:

9.2.1. Customer Personal Data will be deleted within 90 days of the Services being deprovisioned unless the retention of Customer Personal Data is required under Applicable Laws.

**9.3.** Upon Customer's written request, Wazuh shall:

9.3.1. Make Customer Personal Data available for return to Customer where such a request has been made prior to deletion as set forth in the Agreement; and

9.3.2 Provide a written certification of deletion of Customer Personal Data to Customer.

## 10. Audit rights

**10.1**. Subject to sections 10.2 to 10.4, Wazuh shall make available to Customer on request information necessary to demonstrate compliance with Applicable Laws and this DPA.

**10.2**. To the extent required by Applicable Laws, Wazuh shall contribute to audits by Customer or an independent auditor engaged by the Customer, that is not a competitor of Wazuh, in relation to the Processing of the Customer Personal Data.

**10.3**. Information and audit rights of the Customer only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Applicable Laws.

**10.4**. Notwithstanding the foregoing, Wazuh may exclude information and documentation that would reveal the identity of other Wazuh customers or information that Wazuh is required to keep confidential. Any information or records provided pursuant to this assessment process shall be considered Wazuh's Confidential Information and subject to the Confidentiality section of the Agreement.

## 11. Restricted Transfers from jurisdictions requiring safeguards to cross-border data transfer

**11.1**. Where, in the use of the Services or performance of the Agreement, Customer directly, indirectly or via Onward Transfer makes a Restricted Transfer of Customer Personal Data originating from the EEA, Israel, Switzerland and/or the United Kingdom ("UK") to a third country, not determined by the European Commission, on the basis of Article 45 of the GDPR, or another competent supervisory authority under Applicable Laws, offering an adequate level of data protection, and where Wazuh has not adopted another legally sufficient adequacy mechanism and provided notice to the Customer, the Standard Contractual Clauses will be incorporated into this DPA and shall apply as follows:

11.1.1 . The Parties acknowledge and agree:

11.1.1.1. Wazuh will be a Data Importer acting as Processor of Customer Personal Data (or Subprocessor, as the context below requires) to a Restricted Transfer.

11.1.1.2. Where Customer will be a Data Exporter acting as Controller, Module 2 (Controller to

Processor) will apply to a Restricted Transfer.

11.1.1.3. Where Customer will be a Data Exporter acting as a Processor, Module 3 (Processor to Processor) will apply to a Restricted Transfer. Taking into account the nature of the Processing, Customer agrees that it is unlikely that Wazuh will know the identity of Customer's Controllers because Wazuh has no direct relationship with Customer's Controllers and therefore, Customer will fulfill Wazuh's obligations to Customer's Controllers under the Module 3 (Processor to Processor) Clauses.

11.1.1.4. Where Wazuh will be Data Importer Processing Customer Personal Data in its own discretion as Controller in the provisioning of the Services agreed, e.g., for administering the Agreement, Module 1 (Controller to Controller) will apply to the relationship between Customer (Data Exporter) and Wazuh (Data Importer).

11.1.2. Clause 8.1 (Instructions). The Parties acknowledge that Customer's instructions may not conflict with the Services. Any additional or alternate instructions, having impact to the Services, must be agreed upon separately between the Parties. The following is a mutually agreed instruction: (a) Processing of Customer Personal Data in accordance with the Agreement and any applicable orders; (b) Processing initiated by users in their use of the Wazuh Services, and ( c) Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

11.1.3. Clause 8.5 (Duration of processing and erasure or return of data). Customer acknowledges and expressly agrees that the process described in Section 9 of the DPA shall govern the fulfillment of requirements related to data erasure and return of Customer Personal Data.

11.1.4. Clause 8.9(c, d) (Audit). The Parties agree the audits described in Clause 8.9(c, d) shall be carried out in accordance with Section 10 of this DPA. Customer shall promptly notify Wazuh with information regarding any non-compliance discovered during the course of an audit. In order to align efforts and to keep actions consistent, Customer shall be the relevant body carrying out audits towards Wazuh for itself and Controllers, where Customer acts as a Processor under the instruction of a Controller Wazuh has no direct relationship with.

11.1.5. Clause 9 (Use of sub-processors). The Parties agree to and choose option 2 (General written authorization) and specify the time period set forth in Section 5 of this DPA while Customer further acknowledges and agrees that Wazuh may engage existing Subprocessors (Exhibit E), and new Subprocessors as described there. Where Customer is a Processor to Customer Personal Data, Customer agrees and warrants to be duly authorized to receive and pass on information about Wazuh's new Subprocessor engagement to Controllers with whom Wazuh has no direct relationship, assisting Wazuh to meet its obligation under Clause 9 towards the Controllers.

11.1.6. Clause 11(a) (Redress). The Parties agree that the option provided shall not apply.

11.1.7. Clause 13 (Supervision). The options in Clause 13 will be selected in line with the Customer's establishment.

11.1.8. Clause 17 (Governing law). The Parties agree to and choose Option 2; where such law does not allow for third-party beneficiary rights, the Parties agree that this shall be the law of the Netherlands.

11.1.9. The Exhibits A to E of this DPA substitutes the Annexes I to III required under the Standard Contractual Clauses providing the mandatory information under Applicable Laws.

11.1.10. Where the Restricted Transfer concerns Customer Personal Data originating from Switzerland, in line with the Swiss Federal Data Protection and Information Commissioner's statement as of August, 27, 2021, the following additional requirements shall apply to the extent the Customer Personal Data transferred is exclusively subject to the Swiss Data Protection Act (FADP) or to both the FADP and the GDPR: (i) The term 'member state' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 (c ) of these Standard Contractual Clauses. (ii) Insofar as the data transfers underlying these Standard Contractual Clauses are exclusively subject to the FADP, references to the GDPR are to be understood as references to the FADP. Insofar as the data transfers underlying these Standard Contractual Clauses are subject to both the FADP and the GDPR, the references to the GDPR are to be understood as references to the FADP. (iii) Until the revised Swiss Data Protection Act (rev. FADP) enters into force, the provisions of these Standard Contractual Clauses and all Exhibits also protect any Customer Personal Data to the extent that these provisions are applicable to them under Applicable Swiss Laws.

11.1.11. Where the Restricted Transfer concerns Customer Personal Data originating from the UK, the Standard Contractual Clauses will apply subject to the conditions set out by the United Kingdom Information Commissioner Office's ("ICO") International Data Transfer Addendum to the Standard Contractual Clauses ("IDTA") that shall be incorporated herein by reference. The Parties acknowledge and agree that:

11.1.11.1. Table 1 of the IDTA: The party details and contact information in Table 1 of the UK SCCs shall be the party details and contact information as set out in Exhibit B of the DPA. The start date shall be the effective date of the DPA.

11.1.11.2. Table 2 of the IDTA: the Standard Contractual Clauses agreed in this DPA sets out the version of the EU SCCs to which this UK Addendum is appended to, including the selected modules, clauses, optional provisions and Appendix Information.

11.1.11.3. Table 3 of the IDTA: "Appendix Information" means the information which must be provided for the selected modules as set out in the Exhibit A to E of this DPA (other than the Parties), and which for this UK Addendum is set as follows:

I. Exhibit A (Description of Processing and Transfer)

II. Exhibit B (List of Parties)

III. Exhibit C (Competent Supervisory Authority)

IV. Exhibit D (Technical and Organizational Measures)

V. Exhibit E (List of Sub processors, if any).

11.1.11.4. Table 4 of the IDTA: the Parties agree that neither the Importer nor the Exporter may end the UK Addendum as set out in Section 19.

**11.2**. Where the Restricted Transfer concerns Customer Personal Data originating from Argentina, the standard contractual clauses made under Regulation No. 60-E/2016, will be incorporated into this DPA by reference and shall apply to the extent required under Applicable Laws and where this DPA does not provide adequate safeguards.

**11.3**. Where the Restricted Transfer concerns Customer Personal Data originating from another jurisdiction requiring certain privacy safeguards, standard contractual clauses, or any other contractual privacy provisions, not provided through this DPA, the Standard Contractual Clauses will be incorporated into this DPA by reference and shall apply to the extent required under Applicable Laws and where this DPA does not provide adequate safeguards. In such case, the Standard Contractual Clauses, shall apply as follows: (i) Any terms applicable to the GDPR must not be interpreted in such a way as to exclude data subjects from the respective jurisdiction from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c ) of these Standard Contractual Clauses. (ii) Insofar as the data transfers underlying these Standard Contractual Clauses are exclusively subject to the Applicable Law of the respective jurisdiction, references to the GDPR are to be understood as references to this Applicable Law of the respective jurisdiction. Insofar as the data transfers underlying these Standard Contractual Clauses are subject to both the FADP and the GDPR, the references to the GDPR are to be understood as references to the Applicable Law of the respective jurisdiction insofar as the data transfers are subject to the Applicable Law of the respective jurisdiction. For the avoidance of any doubt, by applying the Standard Contractual Clauses in this event, the Parties do not intend to grant third-party beneficiary rights to Data Subjects under the Standard Contractual Clauses when Data Subjects concerned would not otherwise benefit from such rights under the Applicable Laws or this DPA.

## 12. General Terms

**12.1**. Governing law and jurisdiction. The Parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity. Where, in line with section 11 of this DPA the Standard Contractual Clauses apply, and it is required under Applicable Laws, for disputes arising the governing law and jurisdiction are stipulated in Clause 17 of the Standard Contractual Clauses.

**12.2.** Order of Precedence. Any conflict between the terms of the Agreement and this DPA related to the processing of Customer Personal Data are resolved in the following order of priority: (1) the Standard Contractual Clauses (where applicable and materially affecting the adequacy of the Restricted Transfer); (2) this DPA; (3) the Agreement. For the avoidance of doubt, provisions in this DPA, that merely go beyond the Standard Contractual Clauses without contradicting them, shall remain valid. The same applies to conflicts between this DPA and the Agreement where this DPA shall only prevail regarding the Parties' Personal Data protection obligations.

**12.3.** Severability.  Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, should this not be possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein. The foregoing shall also apply if this DPA contains any omission.

**12.4**. Notwithstanding sections 12.2 and 12.3, the terms of the Agreement shall remain in full force and effect.

**12.5.** For the avoidance of doubt, by applying the provisions of this DPA, the Parties do not intend to grant third-party beneficiary rights to Data Subjects under this DPA when those Data Subjects would not otherwise benefit from such rights under the Applicable Laws.

**12.6.** Limitation of Liability. Unless required by Applicable Laws, Customer shall exercise any right or seek any remedy on behalf of itself, its Affiliates, and any other Controller that Customer instructs Wazuh to process Customer Personal Data for under this DPA (collectively, the "Customer Parties"). Customer shall exercise any such rights or seek any such remedies in a combined manner for all Customer Parties together, rather than separately for each entity individually. To the maximum extent allowed by Applicable Laws, the limitations of liability and any exclusions of damages set forth in the Agreement govern the aggregate liability for all Customer Parties' claims arising out of or related to this DPA, and/or the Agreement against Wazuh and any Wazuh Affiliate(s). These limitations of liability and exclusions of damages apply to all claims, whether arising under contract, tort or any other theory of liability, and any reference to the liability of Wazuh means the aggregate liability of Wazuh and all Wazuh Affiliates together for claims by Customer and all other Customer Parties.

12.6.1. To the extent required by Applicable Laws, (i) this section is not intended to modify or limit the Parties' liability for Data Subject claims made against a Party where there is joint and several liability, or (ii) limit either Party's responsibility to pay penalties imposed on such Party by a regulatory authority.

The Parties by their duly authorized representatives have executed this DPA to be effective as of the Effective Date.

**By Wazuh, INC.**

**Signature** ____________________

**Name:** ____________________

**Title:** ____________________

**Date:** ____________________

**Notices:** ____________________

**By Customer**

**Signature** ____________________

**Name:** ____________________

**Title:** ____________________

**Date:** ____________________

**Notices:** ____________________

# EXHIBIT A - Description of processing and transferring Customer Personal Data

This Exhibit A includes certain details of the Processing and Restricted Transfer of Customer Personal Data as required by Article 28(3) GDPR and the Standard Contractual Clauses.

| | Description |
|---|---|
| Categories of data subjects | The categories of data subjects whose personal data may be transferred are determined and controlled by the data exporter in its sole discretion and may include but are not limited to: employees of the data exporter and other third parties using the services of the data exporter. |
| Categories of personal data | • Customer company details; titles, emails, phone numbers, and names of Customer representatives; billing information; business information; and other Data or information that Customer decides to provide to Wazuh by or through the Solutions or any other means or mechanisms.<br>• User and Endpoint data: agent ID, Endpoint name, customer active directory user ID, user name, SMTP user name, configuration data related to active directory integration.<br>• File full path: will only include personal data if the file name as named by Customer includes Data.<br>• In cases of suspected threats, the Wazuh agent collects for each process (file metadata, hash, file type, certificate, command line arguments, network access metadata (IP address, protocol), registry (created keys, deleted keys, modified key names).<br>• Network data (internal network IP address, public IP address (if running cloud-based Management Console).<br>• Management Console Settings received from Management Console (admin user names, emails and phone numbers, endpoint name and user ID, policies names and policies creator name).<br>• Threat information (file path, agent IDs, SMS messages content (which may include user names, IP addresses, file names).<br>• Live network monitoring (URLs, URL headers, time stamps).<br>• Where Customer triggers Wazuh's File Fetching feature: any Data contained in files fetched by Customer's admins. |

| | |
|---|---|
| Sensitive data transferred (if applicable) and applied restrictions or safeguards | Not applicable |
| Frequency of the transfer | For support or engineering, transfers will occur on a one-off through support tickets. Support and maintenance activities by the Wazuh Support team will be initiated upon customer request .<br>For Wazuh Platform/Wazuh Cloud usage, transfers will occur on a continuous basis by uploading and hosting Personal Data. E.ads |
| Nature of the Processing: | Analysis to filter security relevant data (threat detection/management). |
| Purpose(s) of the data transfer and further Processing | Identify security relevant data to protect data exporter's assets. |
| Period for which the Personal Information will be retained, or, if that is not possible, the criteria used to determine that period | For as long as the validity of the Agreement |
| Subject matter of processing | Provision of the Services, as described in the Agreement |
| Duration of processing | For as long as the validity of the Agreement. |

# EXHIBIT B - List of Parties

| | |
|---|---|
| Data Exporter | |
| Name | |
| Address | |
| Contact person's name, position and contact details | |
| Activities relevant to data transferred under these Clauses | Provision of the Services, as described in the Agreement |
| DPO name and contact details (where applicable) | |
| EU representative name and contact details (where applicable) | |
| Role (Controller / Processor) | Controller |
| Data Importer | |
| Name | Wazuh Inc. |
| Address | 1999 S. Bascom Ave Suite 700 PMB #727 Campbell CA 95008, USA |
| Contact person's name, position and contact details | Alberto Gonzalez - COO - alberto.gonzalez@wazuh.com - +1 (408) 610-0385 |
| Activities relevant to data transferred under these Clauses | Provision of the Services, as described in the Agreement |
| DPO name and contact details | Jesus Linares, IT Security Engineer - jesus@wazuh.com |
| EU representative name and contact details (where applicable): | N/A |
| Role (Controller / Processor): | Processor |

# EXHIBIT C - Competent Supervisory Authority

Where Customer makes a Restricted Transfer of Customer Personal Data originating from the EEA, the competent Supervisory Authority shall be determined in accordance with Clause 13 of the Standard Contractual Clauses.

Where Customer makes a Restricted Transfer of Customer Personal Data originating from Switzerland, and the Standard Contractual Clauses apply, the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner with respect to the Customer Personal Data originating from Switzerland.

Where Customer makes a Restricted Transfer of Customer Personal Data originating from the UK, and the Standard Contractual Clauses apply, the competent supervisory authority shall be the ICO with respect to the Customer Personal Data originating from the UK.

Where Customer makes a Restricted Transfer of Customer Personal Data originating from another jurisdiction requiring the determination of the competent supervisory authority under Applicable Laws, the competent supervisory authority shall be determined by Applicable Laws.

# EXHIBIT D - Technical and organizational measures including technical and organizational measures to ensure the security of the Data

| Security Control Category | Description |
|---|---|
| Governance and Security Policies | Wazuh takes the security of critical data and business-related assets very seriously. Therefore, management requires that all employees understand and comply with these policies. It is WAZUH's intended purpose to protect client, employee, financial, protected third party and other corporate information from unauthorized disclosure, modification or destruction throughout the information's lifecycle. To accomplish this, WAZUH has developed this set of IT Security Policies and Procedures in conjunction with a rigorous PCI DSS Compliance Assessment performed by a third party Qualified Security Assessor. These policies offer direction to specific departments and staff members, and it is each individual's responsibility to uphold those policies that directly relate to their position at Wazuh.<br>● Confidentiality agreements are in place for all individuals who can access personal data.<br>● Information Security training is conducted during onboarding and on a regular basis.<br>● No third parties are used for the processing of data other than as described in this Agreement. |
| Network level security | Wazuh attests that a formal process is in place for testing and approval of all network connections and changes to firewall and router configurations. Any and all changes to the firewall and/or router must be approved in advance by the Cloud Information Security Department. The changes must be thoroughly tested (following production standards) as outlined in the Change Control Policy. Examples of changes include:<br>● Upgrades or patches to the firewall system.<br>● Modifications to any firewall software or system.<br>● Additions, deletions, or modifications to the firewall rules.<br>● Add any additional bullets that reference the router(s) and switches. |

| | |
|---|---|
| | The Wazuh firewall(s) must block every path and service that is not specifically approved by this policy. The Wazuh must maintain a “Permitted Network Services and Protocols” form, which outlines the list of currently approved paths and services. All inbound Internet traffic must use a network segmented by a firewall. This segmented zone is known as the “Demilitarized Zone” (DMZ), which adds an additional layer of network security between the Internet and Wazuh’s internal networks so that external entities only have direct connections to devices in the DMZ and not the entire internal network. This inbound traffic must be limited to only those ports deemed necessary for Wazuh business. With the exception of the DMZ, perimeter routers should never be configured to include a route to internal address space. All firewall and router configuration files must be secured to prevent unauthorized tampering. In addition, the start-up configuration files must be synchronized with the secure settings of the running configuration files in order to prevent weaker rules from running in the event that one of these devices re-starts. |
| Intrusion, anti-virus and anti-malware | All Wazuh computer assets, including file servers and email servers managed by employees or third parties, which run the Microsoft Windows OS must comply with this policy. The Cloud Information Security Department must approve any policy exemption in writing. The Cloud Information Security Department is responsible for approving anti-virus/anti-spyware software and configuring it for each system. Users must not be able to disable or otherwise configure the software. The approved software must employ a combination of security measures, such as signature-based detection, heuristics, rootkit detection, as well as “real-time” protection. It must perform real-time scans and log all anti-virus alerts with routing to a central logging location. All anti-virus software should be configured to run daily virus signature updates. For any systems deemed to be not commonly affected by malware, periodic evaluations shall be performed to help identify and assess any evolving malware threats in order to confirm whether these systems do/do not require anti-virus software |
| Cloud hosting | Wazuh’s Cloud platform complies with PCI-DSS and SOC2. |
| Physical site security | Wazuh’s Cloud platform is hosted in AWS so their Physical site security applies.<br>For Wazuh’s physical offices the following applies:<br>Physical access controls must be established to protect hard copy, printed materials and electronic media used to store any Wazuh information.<br>● Access to physical network jacks, wireless access points and handheld devices must be restricted.<br>● Sensitive areas must be monitored by security cameras. The data collected must be stored for at least 3 months.<br>● Relevant facility controls must monitor and/or restrict access to any systems that store or process Wazuh information.<br>It is mandatory for all Wazuh employees, contractors and visitors to clearly |

| | |
|---|---|
| | display their ID badges at all times. Employees should be watchful for unknown persons or fellow employees not displaying an ID badge. |
| Device hardening | Wazuh configuration standards for all system components must be maintained in accordance with industry-accepted system hardening standards. WAZUH shall develop and maintain standards based on one or a combination of the following sources:<br>● Center for Internet Security (CIS)<br>● International Organization for Standardization (ISO)<br>● SysAdmin Audit Network Security (SANS)<br>● National Institute of Standards Technology (NIST)<br>At the time of installation, a 'System Configuration Record' form must be completed for all deployed WAZUH systems. This record must be kept on file for the life of the system and must be updated in the event of a modification. |
| Access control | Wazuh will ensure that the Access Control policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives:<br>● Limit access to system components and cardholder data to only those individuals whose job requires such access.<br>● Access needs are to be defined for each respective role, specifically:<br>○ System components and data resources that each role needs to access for their job function.<br>○ Level of privilege required for accessing resources.<br>● Access rights for privileged users are restricted to the least privileges necessary to perform job responsibilities.<br>● Privileges are assigned to individuals based on job classification and function, such as Role-Based Access Control (RBAC).<br>● An authorization form is required for all access, which must specify required privileges, and must be signed by management.<br>● Access controls are implemented via an automated access control system.<br>● Access control systems are in place on all system components.<br>● Access control systems are configured to enforce privileges assigned to individuals based on job classification and function.<br>● Access control systems have a default Deny All setting.<br>● Security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties. |
| User activity logging | Events Logged<br>In order to reconstruct the following events, all system components must have an automated audit trail implemented.<br>● Invalid logical access attempts. |

| | |
|---|---|
| | - All user access to cardholder data.<br>- Creation or deletion of system-level objects.<br>- All administrative actions utilizing user IDs with access above-and-beyond that of a general user (e.g., root, oracle, administrative privileges).<br>- Access or initialization of audit log files.<br>- Use of changes to identification and authentication mechanisms.<br>- Any increase or elevation of privileges.<br>- All changes, additions, or deletions to any account with root or administrative privileges.<br>- Any user or admin authentication attempts (either valid or invalid).<br>Event Log Structure<br>All system access event logs must contain the following minimum information:<br>- Name of the affected data, system component or resource<br>- User ID<br>- Origination location of event<br>- Type of event<br>- Date and Time that event occurred<br>- Result of the event (success/failure) |
| Transmission Security | To avoid interception or misuse of data, any confidential or sensitive information that is to be transmitted over public networks must be secured using strong encryption tactics, such as: • Transport Layer Security (TLS) 1.1 or greater<br>- Secure Socket Shell (SSH)<br>- Internet Protocol Security (IPSEC)<br>Wazuh will thoroughly document all locations where data is transmitted or received over open, public networks.<br>Wazuh will have process in place ensure the following:<br>- To only accept keys and/or certificates from trusted certificate authorities.<br>- For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported).<br>- For implementation of proper encryption strength per the encryption methodology in use. |
| Availability | Wazuh developed a Disaster Recovery plan with the following characteristics. Objectives<br>The primary objective of maintaining a disaster recovery plan is to develop, test, document a well structured and easily understood plan which will help the service to recover as quickly and effectively as possible from an unseen major disruptive incident which interrupts the service operation. To ensure that planned and tested procedures will work properly during a disruptive incident regardless of personnel or functional changes. |

| | |
|---|---|
| | ● Ensure that planned and tested procedures will work properly during a disruptive incident regardless of personnel or functional changes.<br>● Keep all contact and inventory lists up-to-date.<br>● Ensure periodic testing of the plans is implemented.<br>● Ensure the members of the Disaster Recovery team are comfortable and capable in their roles. Goals<br>● To minimize the interruptions to the normal operations.<br>● To limit the extent of disruption.<br>● To minimize the revenue and reputation impact due to interruption.<br>● To establish alternative means of operations in advance. |

# EXHIBIT E - List of Subprocessors

The controller has authorized the use of the following Subprocessors.

1. For the Wazuh SaaS solution

Name: Amazon Web Services, Inc.

Address: United States

Contact person's name, position and contact details: https://aws.amazon.com/compliance/gdpr-center/

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorized): Hosting of Customer Data.

The (sub-) processors do not access the data.

2. For the Wazuh Support Portal

Name: Jira Software (Atlassian Corporation Plc)

Address: United States

Contact person's name, position and contact details: eudatarep@atlassian.com; https://www.atlassian.com/legal/privacy-policy#other-important-privacy information

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorized): Services for Customer Support.

The (sub-) processors do not access the data.