Data Processing Addendum

(December 2022)

This Data Processing Addendum ("**DPA**") is incorporated by reference to and made a part of the agreement or Order to which Customer obtains the right or subscription license to use the BigID Software and Services, and is made by and between Customer and BigID (such agreement and any related Orders collectively the "**Agreement**").

This DPA supplements the Agreement and sets out the terms that apply when Personal Data (defined below) is Processed (defined below) by BigID under the Agreement. The purpose of the DPA is to ensure such Processing is conducted in accordance with applicable laws, and with due respect for the rights and freedoms of individuals whose Personal Data are Processed.

Customer understands, acknowledges, and agrees that this DPA applies to itself and, to the extent required under applicable Data Protection Laws and Regulations, to its Authorized Affiliates, if and to the extent BigID processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Software and Services to Customer pursuant to the Agreement, BigID may Process Personal Data on behalf of Customer, and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

Data Processing Terms

1 Definitions

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity for so long as control exists. "**Control**", for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Applicable Data Protection Laws**" means US Data Protection Law and GDPR that are applicable to the processing of Customer Personal Data under this DPA.

"**Authorized Affiliate**" means an Affiliate of Customer which is permitted to use the Software and Services pursuant to the Agreement between Customer and BigID, but has not signed its own Order with BigID.

"**Authorized European Affiliate**" means an Authorized Affiliate which is subject to the data protection laws and regulations of Europe (as defined below).

"**BigID**" means the BigID entity that is a party to both the Agreement and to this DPA, which may be BigID, Inc., a company incorporated in the State of Delaware.

"**Controller**" means an entity which determines the purposes and means of the Processing of Personal Data.

"**Customer**" means the entity that executed the Agreement, together with its Authorized Affiliates (for so long as they remain Authorized Affiliates) which have access to the Software and Services.

"**Customer Data**" means any data, information or material originated by Customer that Customer submits to BigID, collects through its use of the Software and Services, or provides to BigID in the course of using the Software and Services.

"**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

"**De-identified data**" means data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such a person, provided that Customer or BigID possess such data.

"**Europe**" means the European Economic Area (which constitutes the member states of the European Union and Norway, Iceland, and Liechtenstein), as well as, for the purposes of this DPA, the United Kingdom and/or Switzerland.

"**GDPR**" means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation) (the "**EU GDPR**"), as well as, for the purposes of this DPA, (i) the UK General Data Protection Regulation as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); and (ii) the Swiss Federal Data Protection Act passed on 25 September 2020 (the "**Swiss DPA**").

"**Personal Data**" means any information relating to: (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws, where for each (i) or (ii), such data is Customer Data.

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

"**Processor**" means an entity which Processes Personal Data on behalf of a Controller, including as applicable any "service provider" as that term is defined by the US Data Protection Laws.

"**Pseudonymous data**" means personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

"**Security Incident**" means any confirmed breach of security that leads to the accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure of or access to Customer Personal Data processed by BigID and/or its Sub-processors in connection with the provision of the Service. "Security Incident" does not include unsuccessful attempts or activities that do not compromise the security of personal data, including unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"**Services**" means the provision of the products and services by BigID to Customer pursuant to the Agreement.

"**Standard Contractual Clauses**" means module two of the standard contractual clauses annexed to the European Commission's decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the

transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended or replaced from time-to-time, and completed with the details set out in Schedule 2 to this DPA. As at the date of this DPA, the Standard Contractual Clauses are available [here].

"**Sub-processor**" means any Processor engaged by BigID to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA where such entity processes Customer Personal Data.

"**Supervisory Authority**" means (i) in the EU, an independent public authority which is established by an EU Member State pursuant to the EU GDPR, (ii) in the United Kingdom, the UK Information Commissioner's Office, and (iii) in Switzerland, the Swiss Federal Data Protection and Information Commissioner.

"**UK Addendum**" means the UK Addendum to the Standard Contractual Clauses issued under Section 119A of the Data Protection Act 2018, as amended or replaced from time-to-time, and completed with the details set out in Schedule 2 to this DPA. As at the date of this DPA, the UK Addendum is available [here]).

"**US Data Protection Laws**" means the California Consumer Privacy Act ("**CCPA**") and, once implemented, the California Privacy Rights Act ("**CPRA**"), Virginia Consumer Data Protection Act ("**VCDPA**"), Colorado Privacy Act ("**CoICPA**"), Utah Privacy Act ("**UCPA**"), Connecticut Data Privacy Act ("**CTDPA**"), and any other state or federal laws relating to privacy or data protection, and their respective implementing regulations.

2 Processing of Personal Data

1. **Role of the Parties**. The parties acknowledge and agree that with regard to the Processing of Personal Data under the Agreement, Customer is the Controller, BigID is the Processor, and BigID will engage Sub-processors pursuant to the requirements set forth in Section 6 "Sub-processors" below.

2. **Customer's Processing of Personal Data**. Customer shall, in its use of the Software and Services, Process Personal Data in accordance with the requirements of Applicable Data Protection Laws, including any applicable requirement to provide notice to Data Subjects of the use of BigID as Processor. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Applicable Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

3. **BigID's Processing of Personal Data**. BigID shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions, including for the purposes set out in Schedule 1 (Details of the Processing) to this DPA, unless required to process Personal Data for other purposes by applicable law, in which case BigID shall provide prior notice to Customer unless the relevant law prohibits the giving of notice. Where the Customer is located in the European Union, references to law in this section 2.3 shall be restricted to laws of the European Union or a Member State of the European Union. BigID shall inform Customer if it considers that, in its opinion, Customer's instructions would be in breach of Applicable Data Protection Laws, in which case Customer agrees that BigID shall not be required to carry out that Processing.

4. **Details of the Processing**. The subject-matter of Processing of Personal Data by BigID is the provision of the Software and performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 (Details of the Processing) to this DPA.

5. **Customer Security.** BigID shall implement appropriate technical and organizational measures to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of the Customer Personal Data, in accordance with BigID's security standards described in Schedule 3 ("Security Measures"). Customer acknowledges that the Security Measures are subject to technical progress and development and that BigID may update or modify the Security Measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Services.

6. **Additional United States Processing Terms.** Where Customer discloses Personal Data subject to US Data Protection Laws, the following provisions apply with respect to the processing of Personal Data relating to any "consumers" or "households" as defined thereunder:

    a. As a Processor to Customer, BigID will not retain, use, or disclose Personal Data other than as set out in the Agreement or as otherwise permitted by US Data Protection Laws in a manner consistent with a Processor or "Service Provider" (as that term is defined under the CCPA/CPRA).

    b. Customer shall not instruct BigID to process or disclose Personal Data other than as set out for the explicit business purpose to perform the services described in the Agreement, DPA, and as otherwise agreed between the Parties.

    c. BigID shall not "sell" (as defined under US Data Protection Laws) or "share" (as defined by the CPRA) Personal Data provided to BigID in BigID's role as a Processor.

    d. Except as otherwise required or permitted by US Data Protection Laws, BigID shall not release, disclose, disseminate, make available, transfer, or otherwise communicate Personal Data to any third party, except to BigID's Sub-processors that are bound by terms consistent with those set out in this DPA.

3 Rights of the Data Subjects

1. **Data Subject Request**. BigID shall, to the extent legally permitted, promptly notify Customer if BigID specifically receives a request from a Data Subject with regards to Personal Data in order to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a "**Data Subject Request**". Taking into account the nature of the Processing, BigID shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under GDPR and US Data Protection Laws. In addition, to the extent Customer, in its use of the Software or Services, does not have the ability to address a Data Subject Request, BigID shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject

Request, to the extent BigID is legally permitted to do so and the response to such Data Subject Request is required under GDPR and US Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from BigID's provision of such assistance.

4 European Specific Provisions

1. **Compliance**. BigID, as Processor, has complied and will continue to comply with all applicable privacy and data protection laws including, but not limited to, [EU Data Protection Legislation]. Customer, as Controller, shall be responsible for ensuring that, in connection with Personal Data and the provision of the Software and Services to Customer:

   A. It has complied, and will continue to comply, with all applicable privacy and data protection laws, including GDPR; and

   B. It has, and will continue to have, the right to transfer, or provide access to, the Personal Data to BigID for processing in accordance with the terms of the Agreement including this DPA.

2. **Data Protection Impact Assessment**. Upon Customer's request, BigID shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Software and Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to BigID. BigID shall provide reasonable assistance to Customer in the cooperation or prior consultation with a Supervisory Authority in the performance of its tasks relating to this Section 4.2 of this DPA, to the extent required under the GDPR.

3. **Customer Security**. Upon Customer's request, BigID shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's security obligations under the GDPR and US Data Protection Laws.

4. **Supervisory Authorities**. BigID shall, to the extent legally permitted, notify the Customer without undue delay if a Supervisory Authority or law enforcement authority makes any inquiry or request for disclosure regarding Personal Data.

5. **Entry into the Standard Contractual Clauses:** The Standard Contractual Clauses and the additional terms specified in this Section are incorporated into this DPA by reference and apply to transfers of Personal Data to BigID from (i) Customer if it is subject to the data protection laws and regulations of Europe, and (ii) its Authorized European Affiliates. To the extent that any such transfer of Personal Data is:

   A. subject to the UK GDPR and not the EU GDPR, then the Standard Contractual Clauses shall be amended in accordance with the UK Addendum, or

   B. subject to both the UK GDPR and the EU GDPR, then BigID and Customer shall comply with the Standard Contractual Clauses (a) as they stand, and (b) on a parallel basis, as amended by the UK Addendum, but only to the extent the transfer of Personal Data is subject to the UK GDPR and without prejudice to their obligations under the Standard Contractual Clauses.

For the purpose of the Standard Contractual Clauses (including the UK Addendum, where applicable), Customer and any Authorized European Affiliates shall each be deemed a “data exporter”, and BigID shall be deemed the “data importer”.

5 BigID Personnel

1. **Confidentiality**. BigID shall ensure that its personnel engaged in the Processing of Personal Data are informed of the sensitive nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements.
2. **Reliability**. BigID shall take commercially reasonable steps to ensure the reliability of any BigID personnel engaged in the Processing of Personal Data.
3. **Limitation of Access**. BigID shall ensure that BigID’s access to Personal Data is limited to those personnel providing the Software and performing the Services in accordance with the Agreement.
4. **Data Protection Officer**. BigID has an established entity in the EU, wherein an EU Representative can be reached at privacy@bigid.com.

6 Sub-processing

1. **Sub-processors.** Customer acknowledges and agrees that BigID may engage Sub-processors in connection with the provision of the Software and Services on behalf of Customer. The Sub-processors currently engaged by BigID and authorized by Customer are listed at https://bigid.com/sub-processors/ (“**Sub-processor List**”) which shall include the identities and details of those Sub-processors. BigID will: (i) enter into a written agreement with each Sub-processor imposing data protection terms that require the Sub-processor to protect the Customer Personal Data to the standard required by Applicable Data Protection Laws and no less protective than those in this Agreement with respect to the protection of Personal Data, to the extent applicable to the nature of the services provided by such Sub-processor; and (ii) remain responsible to Customer for the performance of such Sub-processor's data protection obligations under such terms.
2. **Changes to Sub-processors**. Periodically, BigID may need to add or make changes to our Sub-processor List. Customer may object to the appointment of an additional Sub-processors within fifteen (15) calendar days of such notice on reasonable grounds relating to the Processing of Personal Data, in which case BigID shall have the right to cure the objection through one of the following options (to be selected at BigID’s sole discretion): (a) BigID will cancel its plans to use the Sub-processor with regard to Personal Data or will offer an alternative to provide the Software and Services without such Sub-processor; or (b) BigID will take the corrective steps requested by Customer in its objection (which remove Customer’s objection) and proceed to use the Sub-processor with regard to Personal Data; or (c) if none of the above options are reasonably available and the objection has not been resolved to the reasonable mutual satisfaction of the parties within a thirty (30) calendar day period after BigID’s receipt of Customer’s objection, either party may terminate the Agreement and Customer will be entitled to a pro-rata refund for prepaid fees for the Software and Services not performed as of the date of termination.
3. **Emergency Replacement**. BigID may replace a Sub-processor if the need for the change is urgent and necessary to provide the Software and Services and the reason for the change is

beyond BigID's reasonable control. In such instance, BigID shall update the Sub-processor List online as soon as reasonably practicable, and Customer shall retain the right to object to the replacement Sub-processor pursuant to Section 6.3 above.

4. **Liability**. BigID shall be liable for the acts and omissions of its Sub-processors to the same extent BigID would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

7 Security

1. **Controls for the Protection of Personal Data**. BigID shall make commercially reasonable efforts to safeguard the Personal Data against any Security Incident, and shall maintain an information security program that includes administrative, physical, and technical measures designed to ensure a level of security appropriate to the risk associated with the Processing activity, including (as applicable) the measures referred to in Article 32 of the GDPR.

2. **Confidentiality of Processing**. BigID shall ensure that any person that it authorizes to Process the Personal Data (including its staff, agents, subcontractors, and Sub-processors) shall be subject to a duty of confidentiality that shall survive the termination of their employment and/or contractual relationship.

3. **Security Incident**. Upon becoming aware of a Security Incident, BigID shall notify Customer without undue delay and pursuant to the terms of the Agreement, but within no more than seventy-two (72) hours, and shall provide such timely information as Customer may reasonably require to enable Customer to fulfil any data breach reporting obligations under application legislation. BigID will take steps to immediately investigate and remediate the cause of such a Security Incident. BigID shall make available any information Customer may reasonably require for the purposes of demonstrating compliance with Customer's obligations under the GDPR and US Data Protection Laws.

4. **Third-Party Certifications and Audits.** Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, BigID shall respond to Customer's reasonable third-party risk assessment and make available to a Customer that is not a competitor of BigID (or Customer's independent, third-party auditor that is not a competitor of BigID) a copy of BigID's then most recent third-party audits or certifications, as applicable, to demonstrate its compliance with this DPA.

5. **Deletion of Data**. Upon termination or expiration of the Agreement, BigID shall, in accordance with the terms of the Agreement and upon request from Customer, delete all relevant Personal Data in BigID's possession, save to the extent that BigID is required by any applicable law to retain some or all of the Personal Data. If Customer elects Where BigID is required by applicable law to retain some or all of the Personal Data, BigID shall extend the protections of the Agreement and this DPA to such Personal Data and limit any further Processing of such Personal Data to only those limited purposes that require the retention, for so long as BigID retains the Personal Data. Where the Customer is located in the European Union, references to law in this section 7.5 shall be restricted to laws of the European Union or a Member State of the European Union.

8 Miscellaneous

1. Except as amended by this DPA, the Agreement will remain in full force and effect.
2. If there is a conflict between the Agreement and this DPA, the terms of this DPA will control.
3. Any claims brought under this DPA shall be subject to the terms and conditions of the Agreement, including but not limited to the exclusions and limitations included therein.
4. This DPA commences on the date of, and will remain in force until expiration or termination of, the Agreement, at which point it shall terminate automatically.

SCHEDULE 1 – DETAILS OF THE PROCESSING

Nature and Purpose of Processing

BigID (and any Sub-processors it engages) will Process Personal Data as necessary to provide the Software and perform the Services pursuant to the Agreement and as further instructed by Customer in its use of the Software and Services. This includes:

1. Providing the Software and Services to the Customer.
2. For Customer to be able to use the Software and Services, including any Processing initiated by Customer's Users in their use of the Software and Services.
3. To comply with documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.
4. Performing the Agreement and applicable Orders, this DPA and/or other contracts executed by the Parties.
5. Providing support and technical maintenance, if agreed in the Agreement.
6. Resolving disputes.
7. Enforcing the Agreement, this DPA and/or defending BigID's rights.
8. Management of the Agreement, the DPA and/or other contracts executed by the Parties, including fees payment, account administration, accounting, tax, management, litigation.
9. Complying with applicable laws and regulations, including for cooperating with local and foreign tax authorities, preventing fraud, money laundering and terrorist financing.
10. All tasks related with any of the above.

Duration and frequency of Processing, and period for which Personal Data will be retained

Subject to Section 7.5 of the DPA, BigID will Process Personal Data on a continuous basis for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects

Customer may submit Personal Data to the Software and Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Customer's end users or consumers and/or clients
- Customer's users authorized by Customer to use the Software and Services
- Prospects, Customers, business partners and vendors of Customer (who are natural persons)
- Employees, agents, advisors, vendors, freelancers of Customers (who are natural persons) or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)

Type of Personal Data

Customer may submit Personal Data to the Software and Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name

- Title
- Position
- Employer
- Contact information (email, phone, physical address)
- ID data
- Professional Life data
- Personal Life data
- Localization data

SCHEDULE 2 – INTERNATIONAL TRANSFERS INFORMATION

When the Standard Contractual Clauses apply:

- Annex I.A is completed with the names, addresses and contact persons of the parties as set out in the Agreement.
- The signatures of each party and date of the Agreement are deemed to be inserted.
- The role of Customer is specified as "controller" and the role of the BigID is specified as "processor".
- Annex I.B is completed with the information set out in Schedule 1 to this DPA, as well as the details of the restrictions and safeguards set out in Schedule 3 to this DPA which, taking into consideration the nature of the data and the risks involved, apply to all Personal Data transferred, including sensitive data.
- Annex II is completed with the details of the technical and organisational measures set out in Schedule 3 to this DPA.
- Annex I.C is completed as follows:
    - Where Customer's processing of the Personal Data does not fall within scope of the EU GDPR, then the UK Information Commissioner's Office is inserted as the competent supervisory authority, as per the UK Addendum.
    - Where Customer's processing of the Personal Data falls within scope of the EU GDPR, then the competent supervisory authority will be either (i) the supervisory authority in the EU member state in which Customer is established, or (ii) (if Customer is not established in the EU) the EU member state in which Customer has appointed its EU representative, or (iii) (if Customer is not established in the EU and has not appointed an EU representative) the Irish Data Protection Commission.
- Option 1 is deleted from clause 9(a) and the relevant time period shall be as set out in Sections 6.3 and 6.4 above. The "agreed list" referred to in this provision shall be the Sub-processor List referred to in Section 6.2 of this DPA.
- The optional wording at clause 11(a) is deleted.
- Option 2 is deleted from clause 17, and:
    - where Customer's processing of the Personal Data does not fall within scope of the EU GDPR, then the governing law shall be the laws of England and Wales; but
    - where Customer's processing of the Personal Data falls within scope of the EU GDPR, the governing law shall be the law of the Republic of Ireland.
- Clause 18(b) is completed as follows:
    - Where Customer's processing of the Personal Data does not fall within scope of the EU GDPR, with the words "England and Wales"; or

- Where Customer's processing of the Personal Data falls within scope of the EU GDPR, with the words "the Republic of Ireland".

When the UK Addendum applies, then in addition to the information relating to the Standard Contractual Clauses set out in this Schedule above:

- Table 1 is completed with the start date being the date of the Agreement, and the legal and trading names, main address, official registration number, key contact name, job title and contact details (including email address) of the Parties as set out in the Agreement. The signatures of each party are deemed to be inserted in the main Agreement.
- Tables 2 and 3 are completed with the information about the Standard Contractual Clauses set out in this Schedule above, applying as relevant to a transfer in accordance with Clause 4.5 of this DPA. The first option in Table 2 is selected, and that table is completed with the date of the Agreement.
- Table 4 is completed so that either Party may end the UK Addendum if the UK Addendum is changed by the UK Information Commissioner's Office, and the Parties agree that once the UK Addendum has ended then the Customer will no longer transfer personal data subject to the UK GDPR to BigID under the Agreement and this DPA unless an alternative transfer safeguard has been put in place to BigID's reasonable satisfaction.

SCHEDULE 3 – SECURITY MEASURES

I. DEFINITIONS; APPLICABILITY

This Schedule 3, Security Measures ("**Security Measures**"), is incorporated by reference to and made a part of the Data Processing Agreement ("**DPA**"). All capitalized terms not defined in these Security Measures or in the DPA shall have the meaning set forth in the Agreement. Customer acknowledges and agrees that these Security Measures may be utilized for a BigID on-premise software deployment or a BigID hosted software deployment; provided, however, in the event of a BigID on-premise software deployment, only Section 2 ("Security Certifications and Audits"), Section 3 ("Security Training, Confidentiality Obligations and Background Checks") and Section 12 ("Secure Coding Practices") of Article III of these Security Measures shall apply.

- **"Hosted Software"** means BigID software and services made available for access and use to Customer on demand via the Internet.

II. CLOUD VENDOR DATA SECURITY CONTROLS

BigID uses a Sub-processor to provide the infrastructure environment to run the Hosted Software (the "**Cloud Vendor**"). Accordingly, the Hosted Software operates within the Cloud Vendor's security framework. BigID reserves the right to change to a different Cloud Vendor pursuant to the terms of the DPA and the Agreement, or to a data center that BigID or its affiliate operates; provided, that, the data security arrangements shall be at least consistent with prevailing industry standards and the provisions in these Security Measures shall not be materially diminished. The current Cloud Vendor security certifications include ISO 27001 and SOC2, which certifications may be modified from time to time by the Cloud Vendor or if BigID changes Cloud Vendors. As part of the process for obtaining and maintaining these certifications, the Cloud Vendor has implemented numerous procedures, including: (a) personnel background checks and security awareness training; (b) physical and logical access control safeguards; (c) incident response plans; and (d) disaster recovery and business continuity plans.

III. BIGID DATA SECURITY PROCEDURES

1. OVERVIEW

While no business can prevent all potential hacking or other criminal conduct, BigID maintains a security program with administrative, physical, and technical measures, together with the Cloud Vendor's security program and security certifications, that is designed to safeguard the Personal Data against any Security Incident and ensure a level of security appropriate to the risk associated with the Processing activity.

Without limiting the foregoing, BigID's security program, which is in addition to the Cloud Vendor's security program, currently includes the elements described in Sections 2 through 17 below.

2. SECURITY CERTIFICATIONS AND AUDITS

BigID will maintain a certificate from a reputable third-party certification authority of BigID's compliance with ISO / IEC 27001: 2013 or any successor standard. BigID will also obtain and maintain an SSAE18 SOC 2, Type II audit report covering any system or process used in the Processing of Personal Data and any system that could pose a risk to such systems and processes. Promptly after receiving written requests from Customer up to once per year, BigID will provide a copy of its most recent third-party ISO certification or audit summary, or SSAE18 SOC 2, Type II audit report, or any recent third-party penetration test attestations or summary statements.

3. SECURITY TRAINING, CONFIDENTIALITY OBLIGATIONS AND BACKGROUND CHECKS

BigID provides a mandatory security and privacy awareness and training program for all BigID employees and contractors (other than Sub-processors) who may have access to Personal Data in the performance of their services (collectively, "**Workers With Access**"). All Workers With Access are also subject to the confidentiality obligations set forth in the Agreement. Further, BigID conducts background checks consistent with prevailing practices for similar companies in connection with the hiring or engaging of all Workers With Access. BigID will not hire or engage any Worker With Access if the background check shows that the individual was convicted of a crime involving theft, dishonesty, fraud or computer-related crimes; provided, however, BigID's commitments with respect to background checks are subject at all times to Applicable Laws pertaining to such background checks.

4. ENCRYPTION PROGRAMS

- **Encryption Policy.** BigID has a documented security cryptography policy that dictates encryption use, applicable encryption standards, and encryption strength.
- **Encryption in Transit.** Encryption in transit utilizing standard encryption technology (e.g., Transport Layer Security (TLS), IPSec, and SMB).
- **Encryption at Rest.** All Personal Data at rest is encrypted using industry standard symmetric encryption.

5. ANTI-MALWARE SERVICES

BigID leverages third-party anti-malware program services intended to protect against malware impacting system services and functions, as further described below:

- BigID provides, supports and maintains an anti-malware service which provides runtime protection against malicious executables.

6. PHYSICAL SECURITY

BigID will use commercially reasonable efforts to confirm that the Cloud Vendor maintains physical access security controls for the data center including, layers of defense-in-depth security that include perimeter fencing, video cameras, security personnel, secure entrances, and real-time communications networks.

7. DATA DISPOSAL

Upon termination or expiration of the Agreement, BigID shall, upon request from Customer, delete all relevant Personal Data in BigID's possession pursuant to the terms of the DPA and the Agreement; provided, however, BigID may retain copies of Customer Data in accordance therewith. Deletion means the Personal Data is rendered inaccessible, undecipherable or otherwise unrecoverable.

8. OTHER ACCESS CONTROLS

As further described under Section 9 ("Access Control and Password Management Policy"), BigID has policies, procedures, and logical controls designed to limit access to the Hosted Software to properly authorized personnel on a "need to know" basis, to prevent those personnel who should not have access from obtaining access and to remove access of personnel on a timely basis in the event of a change in

job responsibilities or job status. For Workers With Access, BigID's standard operating procedures further limit such access to resolving issues with system components rather than viewing any Personal Data (except in situations when incidental viewing of Personal Data may be required in connection with resolving an issue or responding to a Customer request).

9. ACCESS CONTROL AND PASSWORD MANAGEMENT POLICY

- **General Password Requirements.** BigID has an Access Control and Password Management Policy and an automated password management system to enforce the policy requirements. The policy covers all applicable systems, applications, and databases. There are classes of password use in BigID's enterprise and Hosted Software environments, as further detailed below. Industry standard prevailing password practices are deployed to protect against unauthorized use of passwords, including: (a) minimum password length; (b) password complexity; (c) password history; (d) password lockout for failed password attempts; and (e) randomly generated initial passwords.

- **BigID Enterprise Identity and Password Management.** The BigID enterprise uses a single sign-on multi-factor authentication service for authenticating all individuals in the organization and for authenticating access to the systems that support and operate the Hosted Software (the "**Back-End**").
    - **Front-End Access**. BigID employs the following methods respecting access to the user interface (the "**Front-End**"):
        - Customer controls Front-End logins to its Geo through a password management system that employs the user authentication provider, e.g., Active Directory. Customer controls Front-End password policies for Customer's Authorized Users and can choose from any supported authentication provider in the Hosted Software, including length, expiration, reuse, and complexity requirements, lockout, and reset options.
        - BigID supports integration with its single sign-on multi-factor authentication service for customers to restrict access through the Front-End.
    - **Back-End Access.** BigID employs the following methods respecting access to the BackEnd:
        - All connections to Back-End resources are brokered through a privileged access management solution, which logs the unique user ID that created the connections. Only specific members of BigID can access Back-End accounts through the privileged access management solution, and all access to this solution requires authentication through a single sign-on multi-factor authentication service.

10. DISASTER RECOVERY AND BUSINESS CONTINUITY PLANS

The Cloud Vendor and BigID have disaster recovery and business continuity plans in place. These plans include a separate back-up data center and a formal framework by which an unplanned event will be managed to minimize the loss of vital resources. The formal framework includes a defined back-up policy and associated procedures including, documented policies and procedures designed to: (a) restore applications and operating systems; and (b) demonstrate periodic testing of restoration from the back-up location. If BigID makes back-ups to tape or other removable media, all such back-ups shall be encrypted in compliance with the encryption requirements set forth above.

11. ASSIGNED SECURITY RESPONSIBILITY

BigID assigns responsibility for the development, implementation, and maintenance of its security program, including:

- designating a security official with overall responsibility;
- defining security roles for individuals with security responsibilities; and
- performing risk assessments of BigID and the Hosted Software at least annually and whenever major changes to systems or processes occur.

12. SECURE CODING PRACTICES

All BigID developer personnel are required to take a course in security awareness and secure coding, and BigID's coding standards have a strong security component. Among other things, the OWASP Secure Coding Practices Quick Reference Guidelines are integrated into BigID's coding standards. The coding standards are reviewed annually and maintained by the engineering and security teams to remain up to date and enforce the prevailing standards. Standard production source code changes go through a pull request workflow to ensure peer review for code quality and adherence to coding standards. Each commit into a BigID code base requires an approval from another engineer. The approver reviews for compliance with BigID's coding standards prior to accepting any code change. For new features, completion of a structured review process with BigID's security team is required. During this process, each project receives a risk rating based on risk ranking criteria. The higher the risk rating, the more security scrutiny the project is subject to during its lifecycle.

13. SECURITY TESTING

BigID regularly tests the key controls, systems and procedures of its security program to validate that they are properly implemented and effective in addressing the threats and risks identified. Testing currently includes:

- Internal risk assessments
- Use of internal security specialists and/or a third party to conduct web application-level security assessments. These assessments generally test for the OWASP Top 10, which may include the following:
    - Cross-site request forgery;
    - Improper input handling (e.g., cross-site scripting, SQL injection, XML injection, cross-site flashing);
    - XML and SOAP attacks;
    - Weak session management;
    - Data validation flaws and data model constraint inconsistencies;
    - Insufficient authentication;
    - Insufficient authorization;
    - Web application penetration testing:
        - During web application penetration testing, a dedicated penetration testing team looks for security suspects, such as XSS, Cross Site Request Forgery, authentication issues, and authorization issues. BigID uses industry standard tests alongside specialized tests, sometimes customized for new features. The penetration testing team also leverages other penetration testing techniques based on their disparate experiences and knowledge of the Hosted Software.

- On an annual basis, BigID engages an external penetration testing firm for an extensive test covering the functionality of the Hosted Software, including industry standard tests like those from the OWASP, and additional tests that the penetration testing firm deems necessary as it explores the application; and
- Upon request, BigID will provide Customer with an annual penetration test attestation letter.

14. SECURITY MONITORING & AUTOMATED VULNERABILITY SCANS

BigID monitors network and production systems, including error logs on servers, disks and security events for any suspicious or malicious activities. Monitoring generally includes:

- Arranging for automated vulnerability scans of any assets deployed in the Hosted Software, to be performed periodically to identify, mitigate or remediate any vulnerabilities. Assets include any servers, applications, and if applicable, endpoints, and network devices.
- Subscribing to vulnerability intelligence services or to information security advisories and other relevant sources providing current information about system vulnerabilities.
- Reviewing changes affecting systems handling authentication, authorization, and auditing.
- Reviewing privileged Back-End access to the Hosted Software to validate privileged access is appropriate.
- Engaging third parties to perform network vulnerability assessments and penetration testing on an annual basis.
- Maintaining industry standard event logging for servers, applications, and networking equipment to facilitate security incident and event management. BigID maintains such logs for at least one (1) year.
- Classifying vulnerabilities in accordance with industry standard risk rating methodologies (e.g., the Common Vulnerability Scoring System, OWASP, or NIST).
- Mitigating and/or remediating vulnerabilities in the Hosted Software infrastructure or applications that could allow direct unauthorized access to Personal Data, whether by applying an available patch or taking other reasonable actions in the following time frames:

Severity	Policy	
	BigID Hosted Software	**Third-Party Software**
Critical	Before the software is released if found in release testing. Within 30 days of identification of vulnerability if found after release.	Within 7 days of receiving notice of patch availability from the third-party vendor and up to 15 days for testing.
High	Before the software is released if found in release testing. Within 30 days of identification of vulnerability if found after release.	Within 30 days of receiving notice of patch availability from the third-party vendor and up to 60 days for testing.
Medium	Within 60 days of identification of vulnerability.	Within 90 days of receiving notice of patch availability from the third-party vendor and up to 60 days for testing.

15. CHANGE AND CONFIGURATION MANAGEMENT

BigID maintains policies and procedures for managing changes to the Hosted Software. Policies and procedures include:

- a process for documenting, testing, and approving the promotion of changes into production; and
- a security patching process that requires patching systems in a timely manner based on a risk analysis.

16. SECURITY INCIDENT RESPONSES

- **Cyber Operations Team.** BigID has a Cyber Operations Team that: (a) is capable of meeting on short notice to address any incidents; and (b) focuses on continuous development and improvement of procedures to be followed in the event of any Security Incident involving Personal Data or any Security Incident involving any application or system directly associated with the Processing of Personal Data. Procedures currently include:
  - **Roles and responsibilities:** BigID's Cyber Team will act in coordination with additional security and engineering resources throughout the incident response process;
  - **Investigation:** assessing the risk the incident poses and determining who may be affected in accordance with the DPA;
  - **Communication:** internal reporting as well as the Security Incident notification process set forth in the DPA and below;
  - **Recordkeeping:** keeping a permanent record of what was done and by whom to facilitate later analysis in accordance with the DPA; and
  - **Audit:** conducting and documenting root cause analysis and remediation plans in accordance with the DPA.
- **Security Incident Response**
  - **Notification of a Security Incident.** Unless notification is delayed or prohibited by Applicable Law or the actions or demands of a law enforcement agency, BigID will report a Security Incident to Customer's security contact designated to BigID in accordance with the DPA and the Agreement.
  - **BigID Response.** BigID will take reasonable measures to promptly mitigate the cause of any Security Incident, implement any appropriate monitoring protocol and identify the circumstances that allowed the Security Incident to happen to facilitate prevention of any further similar Security Incidents (unless the Security Incident was caused by the acts or omissions of Customer or any of its Authorized Users, in which case Customer shall take such actions). BigID may work with forensic investigators, law firms, and law enforcement agencies to help determine the nature, extent, and source of any Security Incident and may make any disclosures of security records, security logs, and other information that BigID deems appropriate or is required to make under Applicable Laws; provided, that, any disclosures of Customer Data shall require Customer's prior written consent to the extent permitted by Applicable Law, except if BigID would risk fines, penalties or other sanctions or liabilities (or increased fines, penalties or other sanctions or liabilities) for withholding the information. If BigID makes any statements about a Security Incident without the approval of Customer, BigID will not disclose that Customer or Customer Data was involved, unless such disclosure is required by Applicable Law.
  - **Cooperation with Customer.** Upon Customer's request, BigID will cooperate with Customer (and Customer's regulators and insurers) to investigate the Security Incident and seek to identify the specific Customer Data involved in the Security Incident (without charge, except to the extent the Security Incident was caused or contributed to by the acts or omissions of Customer or its Authorized Users). Unless prohibited by Applicable Law, BigID will: (a) provide information regarding the nature and consequences of the Security Incident as such information is collected or otherwise becomes available to BigID; and (b) otherwise reasonably assist Customer to notify

affected individuals, government agencies, regulators, and/or credit bureaus; provided, the parties agree that Customer is solely responsible for determining whether to notify impacted owners of the Customer Data and if regulatory bodies or enforcement commissions applicable to Customer or Customer Data need to be notified, and for providing such notices.

- **Access Credentials.** For clarity, Customer is responsible for safeguarding its access credentials under the Agreement; any breach of such obligation shall constitute a breach of the Agreement.

17. ADJUSTMENT TO THESE DATA SECURITY TERMS

BigID monitors and evaluates its security program on a regular basis and may adjust it and these Security Measures from time to time, as appropriate in light of: (a) prevailing practices; (b) any relevant changes in technology and any internal or external threats to BigID or the Customer Data; and (c) BigID's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.