Data Processing Addendum

(Last Updated: March 11, 2025)

This Data Processing Addendum ("DPA") is incorporated into and supplements the agreement and/or order form(s) by and between Customer and BigID (collectively, 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.

1. Definitions.

1.1. "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with a party hereto for so long as control exists. "Control" means ownership of more than 50% of the voting securities of an entity.

1.2. "**Applicable Data Protection Laws**" means any law, statute, regulation or other binding restrictions applicable to the Processing of Personal Data under this DPA, including, to the extent applicable, the GDPR, the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act ("CCPA"), and similar privacy data protection laws in other jurisdictions.

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

1.4. "**BigID**" means the BigID entity that is a party to both the Agreement and to this DPA.

1.5. "**Controller**" means an entity which determines the purposes and means of the Processing of Personal Data, including as applicable any "Business" as that term is defined by the CCPA.

1.6. "**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.

1.7. "**Customer Data**" means data, documents, content, intellectual property, or information of any kind input into the Software by or on behalf of Customer or output from Customer's use of the Software.

1.8. "**Data Subject**" means the identified or identifiable person to whom Personal Data relates, including, as applicable, any "Consumer" as that term is defined by the CCPA.

1.9. "**Data Subject Request**" means a request from a Data Subject to exercise its rights with respect to Personal Data granted to Data Subjects by Applicable Data Protection Laws.

1.10. "**EU Standard Contractual Clauses**" means module two of the EU 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 forth in Schedule 2 (International Transfers Information) to this DPA. As of the date of this DPA, the EU Standard Contractual Clauses are available here.

1.11. "**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.

1.12. “**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”).

1.13. “**Personal Data**” means any information contained within Customer Data relating to: (i) an identified or identifiable natural person or (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data under Applicable Data Protection Laws). Personal Data expressly includes “Personal Information”, as that term is defined by the CCPA.

1.14. “**Processing**” or “**Process**” 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.

1.15. “**Processor**” means an entity which Processes Personal Data on behalf of a Controller, or a “Service Provider” as that term is defined by the CCPA.

1.16. “**Security Incident**” means any confirmed breach of security that leads to the accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure of or access to Personal Data Processed by BigID and/or its Subprocessors in connection with the provision of the Software and Services. “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.

1.17. “**Services**” means the advisory services and support provided by BigID and its Affiliates.

1.18. “**Software**” means BigID's software, utilities, connectors, and/or applications as described in an order form, together with any updates made available to Customer by BigID.

1.19. “**Subprocessor**” 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.

1.20. “**Supervisory Authority**” means (i) in the European Union, an independent public authority which is established by a member state of the European Union 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.

1.21. “**UK Addendum**" means the UK Addendum to the EU Standard Contractual Clauses issued under Section 119A(1) of the Data Protection Act 2018, as amended or replaced from time-to-time, and completed with the details set forth in Schedule 2 to this DPA. As of the date of this DPA, the UK Addendum is available here.

1.22. “**US Data Protection Laws**” means the CCPA, Virginia Consumer Data Protection Act (“VCDPA”), 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.

2.1. 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 Subprocessors pursuant to the requirements set forth below.

2.2. Customer's Responsibilities. 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 be consistent with the terms of the Agreement and this DPA and 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. Further, Customer shall be responsible for ensuring that the Personal Data provided to BigID is limited to that which is necessary for BigID's provision of the Software and Services.

2.3. BigID's Responsibilities. BigID shall Process Personal Data on behalf of Customer and only in accordance with Customer's documented instructions and for the purposes set forth 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 such notice. BigID shall inform Customer if it considers that 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. BigID shall have no liability for any third-party claim arising from its act or omission to the extent that such liability arises from Customer's instructions.

2.4. Details of the Processing. The subject matter of Processing of Personal Data by BigID, 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 to this DPA.

2.5. Customer Security. BigID shall implement appropriate technical and organizational measures designed to protect Personal Data from Security Incidents and to preserve the security and confidentiality of the Personal Data, in accordance with BigID's security standards described in Schedule 3 (Security Measures) to this DPA. 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 materially degrade or diminish the overall security of the Software and Services.

2.6. 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" under applicable US Data Protection Laws. For the avoidance of doubt, BigID shall comply with the following obligations under the CCPA, acting as a Service Provider:

a. BigID will retain, use and/or disclose Personal Data only for the specified business purpose as set forth in the Agreement and to comply with Customer's instructions for Processing Personal Data.

b. Customer shall not instruct BigID to Process or disclose Personal Data other than as necessary for the explicit business purpose to perform the Services described in the Agreement, DPA, and as otherwise mutually agreed between the parties.

c. BigID shall not "sell" or "share" (as defined by the CCPA) Personal Data provided to BigID.

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 Subprocessors that are bound by terms consistent with those set forth in this DPA.

e. If BigID receives deidentified Customer Data, BigID will not attempt to reidentify the information, in accordance with US Data Protection Laws.

3. Compliance Activities.

3.1. **Compliance**. BigID, as Processor, has complied, and will continue to comply, with all Applicable Data Protection Laws. Customer, as Controller, shall be responsible for ensuring that, in connection with its provision of Personal Data to BigID and its use of the Software and Services:

a. It has complied, and will continue to comply, with all Applicable Data Protection Laws; 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 and this DPA.

3.2. **Data Subject Requests**. BigID shall, to the extent legally permitted, promptly notify Customer, within five (5) business days, if BigID receives a Data Subject Request. Data Subject Requests may include, for example, the right of access, right to rectification, right of erasure, right to data portability, and/or right to object to the Processing. Taking into account the nature of the Processing, BigID shall reasonably 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 Applicable Data Protection Laws.

3.3. **Requests from Government Officials**. BigID shall, to the extent legally permitted, promptly notify the Customer if a Supervisory Authority or law enforcement authority makes any inquiry or request for disclosure regarding Personal Data. BigID will provide reasonable support to Customer so that Customer may object to such request.

3.4. **Data Protection Assessments**. Upon Customer's request, BigID shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under Applicable Data Protection Laws to carry out data protection impact assessments and/or data protection assessments related to Customer's use of the Software and Services, to the extent (i) Customer does not otherwise have access to the relevant information, and (ii) such information is available to BigID. BigID shall provide reasonable assistance to Customer in the cooperation or prior consultation with regulators, including Supervisory Authorities, in the performance of its tasks relating to this Section 3.4 of this DPA, to the extent required under Applicable Data Protection Laws.

3.5. **Security Obligations.** Upon Customer's request, BigID shall provide Customer with reasonable cooperation and assistance to enable Customer to fulfil its security obligations under Applicable Data Protection Laws.

4. International Data Transfers.

4.1. **Data Transfer Safeguards**. Customer acknowledges and agrees that BigID may transfer Personal Data internationally to BigID personnel for support and maintenance, and to its Subprocessors in order to provide the Services, provided certain conditions are met, including (1) the transfer is being made to a jurisdiction deemed adequate by the European Data Protection Board ("EDPB") and subject to appropriate safeguards (e.g., through the use of the EU Standard Contractual Clauses and appropriate security measures), and/or (2) by implementing and maintaining the technical and organizational security measures outlined in Schedule 3 to this DPA.

4.2. **Data Privacy Framework**. BigID is a member of the EU-US Data Privacy Framework ("DPF"), whereby BigID commits to complying with DPF Principles with respect to international transfers of Personal Data between Europe and the US.

4.3. **EU Standard Contractual Clauses**. The EU Standard Contractual Clauses 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 GDPR, and (ii) Customer's European Authorized 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 EU Standard Contractual Clauses shall be amended in accordance with the UK Addendum, and

b. subject to both the UK GDPR and the EU GDPR, then BigID and Customer shall comply with the EU Standard Contractual Clauses (i) as they stand, and (ii) 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 each party's obligations under the EU Standard Contractual Clauses.

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

5. Subprocessors.

5.1. **Subprocessors**. Customer acknowledges and agrees that BigID may engage Subprocessors in connection with the provision of the Software and Services on behalf of Customer. BigID shall maintain a current list of its Subprocessors at https://bigid.com/sub-processors/ (the "Subprocessor List"). BigID will: (i) enter into a written agreement with each Subprocessor imposing data protection obligations on the Subprocessor as required by Applicable Data Protection Laws and no less protective than those in this Agreement, to the extent applicable to the nature of the services provided by such Subprocessor; and (ii) remain responsible to Customer for the performance of such Subprocessor's data protection obligations under such agreement.

5.2. **Changes to Subprocessors**. Periodically, BigID may need to modify its Subprocessor List, in which case, BigID shall provide a notification of such updates to Customer. Customer shall have the right to object to any change to the Subprocessor List by providing written notice to

BigID within thirty (30) days of the date notice is issued on grounds that the Subprocessor is not reasonably capable of meeting applicable obligations under the Agreement. In the event of Customer's objection, 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 Subprocessor with regard to Personal Data or will offer an alternative to provide the Software and Services without such Subprocessor; (b) BigID will take the corrective steps requested by Customer in its objection (which remove Customer's objection) and proceed to use the Subprocessor with regard to Personal Data; or (c) if neither (a) or (b) are reasonable and the objection has not been resolved to the good faith 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.

5.3. **Emergency Replacement**. BigID may replace a Subprocessor 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 Subprocessor List online as soon as reasonably practicable, and Customer shall retain the right to object to the replacement Subprocessor pursuant to Section 5.2 above.

6. Security.

6.1. **Controls for the Protection of Personal Data**. BigID shall implement appropriate technical and organizational measures designed to protect Personal Data from Security Incidents and to preserve the security and confidentiality of the Personal Data, in accordance with the measures pursuant to Article 32 of the GDPR and as described in BigID's security standards described in Schedule 3 to this DPA. Customer acknowledges that the security measures outlined in Schedule 3 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 materially degrade or diminish the overall security of the Software and Services.

6.2. **Security Incident**. Within seventy-two (72) hours of becoming aware of a Security Incident, BigID shall notify Customer and, upon Customer's request, shall provide such timely information as Customer may reasonably require to enable Customer to fulfil any data breach reporting obligations under and to demonstrate compliance with Applicable Data Protection Laws. BigID will promptly investigate and remediate the cause of such a Security Incident.

6.3. **Third-Party Certifications and Audits**. Upon Customer's written request, and not more than once per year, and subject to the confidentiality obligations set forth in the Agreement, BigID shall respond to Customer's reasonable third-party risk assessment, which may be satisfied by a BigID-generated questionnaire or resource (e.g., a SIG Lite) 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 most recent third-party audits or certifications, as applicable, to demonstrate its compliance with this DPA.

6.4. **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, except to the extent that BigID is required by any applicable law to retain some or all of the Personal Data. 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 those limited purposes that require the retention, for so long as BigID retains the Personal Data. Where the Customer is located in Europe, references to law in this Section 6.4 shall be restricted to laws of Europe.

6.5. BigID Personnel.

a. Confidentiality. BigID shall ensure that any person that it authorizes to Process the Personal Data (including its staff, agents, subcontractors, and Subprocessors) for support and/maintenance shall be subject to a duty of confidentiality that shall survive the termination of their employment and/or contractual relationship. BigID shall ensure that its personnel engaged in the Processing of Personal Data are informed of the sensitive nature of the Personal Data and have received appropriate training on their responsibilities.

b. Reliability. BigID shall take commercially reasonable steps to ensure the reliability of any BigID personnel engaged in the Processing of Personal Data.

c. 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.

7. Miscellaneous.

7.1. Privacy Representative. BigID has a privacy representative who is accountable for compliance with Applicable Data Protection Laws. The representative can be reached at privacy@bigid.com.

7.2. Conflict. If there is a conflict between the Agreement and this DPA, the terms of this DPA will control.

7.3. Disputes. 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.

7.4. Term. 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.

IN WITNESS WHEREOF, the parties have caused this Addendum and the attached Schedules to be executed below by their duly authorized signatories as of the Addendum Effective Date:

BIGID INC.	**CUSTOMER**
By: ______________________________	By: ______________________________
Name: ____________________________	Name: ____________________________
Title: ______________________________	Title: _____________________________
Date: _____________________________	Date: ______________________________

SCHEDULE 1 – DETAILS OF THE PROCESSING

1. **Nature and Purpose of Processing**. BigID (and its Subprocessors) will Process Personal Data as necessary to provide the Software and Services pursuant to the Agreement and as further instructed by Customer in its use of the Software and Services. This includes:
   - **a.** Providing the Software and Services to the Customer.
   - **b.** For Customer's use of the Software and Services, including any Processing initiated by Customer's users in their use of the Software and Services.
   - **c.** To comply with documented reasonable instructions provided by Customer where such instructions are consistent with the terms of the Agreement.
   - **d.** Performing the Agreement and applicable orders, this DPA and/or other contracts executed by the parties.
   - **e.** Providing support and technical maintenance, if set forth in the Agreement.
   - **f.** Resolving disputes.
   - **g.** Enforcing the Agreement, this DPA and/or defending BigID's rights.
   - **h.** Management of the Agreement, this DPA and/or other contracts executed by the parties, including but not limited to the payment of fees, account administration, accounting, tax, management, and/or litigation.
   - **i.** Complying with applicable laws and regulations, including cooperating with local and foreign tax authorities, preventing fraud, and handling money laundering and terrorist financing matters.
   - **j.** All tasks related with any of the above.

2. **Duration and Frequency of Processing, and Period for which Personal Data will be Retained**. Subject to Section 6.4 of this DPA, BigID will Process Personal Data on a continuous basis for the duration of the Agreement, unless otherwise agreed upon in writing.

3. **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:
   - **a.** Customer's users, consumers, prospects, business partners, vendors, customers and/or clients (who are natural persons);
   - **b.** Customer's users authorized by Customer to use the Software and Services;
   - **c.** Customer's employees, agents, advisors, vendors, freelancers (who are natural persons).

4. **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:
   - **a.** First and last name;
   - **b.** Title;
   - **c.** Position;
   - **d.** Employer;
   - **e.** Contact information (email, phone, physical address);
   - **f.** ID data;
   - **g.** Professional and/or personal life data; and/or
   - **h.** Localization data.

SCHEDULE 2 – INTERNATIONAL TRANSFERS INFORMATION

Part I: EU Standard Contractual Clauses

Transfers of Personal Data protected by the GDPR shall be subject to the EU Standard Contractual Clauses, subject to the following:

1. Annex I.A is completed with the names, addresses and contact persons of the parties as set forth in the Agreement.

2. The signatures of each party and date of the Agreement are deemed to be inserted.

3. The role of Customer is specified as "controller" and the role of the BigID is specified as "processor".

4. Annex I.B is completed with the information set forth in Schedule 1 to this DPA, as well as the details of the restrictions and safeguards set forth 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.

5. Annex II is completed with the details of the technical and organizational measures set forth in Schedule 3 to this DPA.

6. Annex I.C is completed as follows:

a. Where Customer’s Processing of Personal Data does not fall within the scope of the EU GDPR, then the UK Information Commissioner’s Office is inserted as the competent supervisory authority, as per the UK Addendum.

b. Where Customer’s Processing of Personal Data falls within the scope of the EU GDPR, then the competent supervisory authority will be (i) the supervisory authority in the member state of the European Union in which Customer is established, (ii) if Customer is not established in the European Union, the member state of the European Union in which Customer has appointed its European Union representative, or (iii) if Customer is not established in the European Union and has not appointed a European Union representative, the Irish Data Protection Commission.

7. In Clause 7, the optional docking clause will not apply.

8. Option 1 is deleted from Clause 9(a) and the relevant time period shall be as set forth in Section 5.2 above. The “agreed list” referred to in this clause shall be the Subprocessor List referenced in Section 5.1 of this DPA.

9. The optional wording in Clause 11(a) is deleted.

10. Option 2 is deleted from Clause 17, and:

a. Where Customer’s Processing of Personal Data does not fall within the scope of the EU GDPR, then the governing law shall be the laws of England and Wales; but

b. Where Customer’s Processing of Personal Data falls within the scope of the EU GDPR, then the governing law shall be the laws of the Republic of Ireland.

11. Clause 18(b) is completed as follows:

a. Where Customer’s Processing of Personal Data does not fall within the scope of the EU GDPR, with the words “England and Wales”; or

b. Where Customer’s Processing of Personal Data falls within the scope of the EU GDPR, with the words "the Republic of Ireland".

12. By signing this DPA, each party is deemed to have signed the EU Standard Contractual Clauses incorporated herein, including the UK Addendum, where applicable, as of the Effective Date of this DPA.

13. If there is any conflict between this DPA and the EU Standard Contractual Clauses, the EU Standard Contractual Clauses will prevail.

Part II: UK Addendum to the EU Standard Contractual Clauses

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

1. 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 are as set forth in the Agreement.

2. Tables 2 and 3 are completed with the information about the EU Standard Contractual Clauses set forth in this Schedule, applying to a transfer in accordance with Clause 4.5 of this DPA, where relevant. The first option in Table 2 is selected, and that table is completed with the date of the Agreement.

3. Table 4 is completed so that either party may terminate 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 been terminated, 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

This Schedule 3 is incorporated by reference into and made a part of this DPA. All capitalized terms not defined in these Security Measures or in this 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 11 (Secure Coding Practices) shall apply. "Hosted Software" means BigID Software made available for access and use to Customer on demand via the internet.

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 that is designed to (i) safeguard Personal Data and (ii) ensure a level of security appropriate to the risk associated with the Processing.

2. **Security Certifications and Audits.** BigID will maintain a certificate from a reputable third-party certification authority evidencing 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. Upon Customer's written request, no more than once annually, BigID will provide a copy of its most recent third-party ISO certification or audit summary; its SSAE18 SOC 2, Type II audit report; and/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 who may have access to Personal Data in the performance of their services (collectively, "Representatives"). All Representatives are subject to confidentiality obligations no less stringent than those set forth in the Agreement. Further, to the extent lawful in the relevant jurisdiction, BigID conducts industry-standard background checks of all Representatives. BigID will not hire or engage any Representative if the background check shows that the individual was convicted of a crime involving theft, dishonesty, fraud or computer-related crimes.

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

5. **Anti-Malware Services.** BigID leverages third-party anti-malware program services designed to (i) protect against malware impacting system services and function, and (ii) provide runtime protection against malicious executables.

6. **Physical Security.** BigID uses commercially reasonable efforts to confirm that its Subprocessors maintain physical access security controls for their data centers, including layers of defense-in-

depth security, such as perimeter fencing, video cameras, security personnel, secure entrances, and real-time communications networks. For clarity, BigID is a remote-first company and uses Subprocessors to Process and store Customer Data.

7. **Data Disposal.** Upon termination or expiration of the Agreement, BigID shall, delete and make irretrievable all Personal Data in BigID's possession pursuant to the terms of this DPA and the Agreement within thirty (30) days of termination/expiration of the Agreement unless otherwise mutually agreed to. For the avoidance of doubt, Customer may export its Customer Data from the Software at any time.

8. **Access Control and Password Management Policy.**

    a. **General.** 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, and to remove access of personnel on a timely basis in the event of a change in job responsibilities or job status.

    b. **Password Requirements.** BigID maintains a password policy and an automated password management system that is designed to enforce the policy requirements. The policy covers all applicable systems, applications, and databases. 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.

    c. **Multi-factor Authentication.** BigID uses a single sign-on multi-factor authentication service for authenticating its Representatives and for authenticating access to the systems that support and operate the Hosted Software. All connections to production systems are brokered through a privileged access management solution, which logs the unique user ID that created the connections. Only Representatives of BigID who need to know can access the production system through the privileged access management solution, and all access to this solution requires authentication through a single sign-on multi-factor authentication service.

    d. **Access Credentials.** Customer is solely responsible for safeguarding its access credentials and for controlling access to the production environment under the Agreement.

9. **Disaster Recovery and Business Continuity Plans.** BigID has implemented and maintains disaster recovery and business continuity plans that include recovery to a different region from the primary Processing and storage region. BigID periodically tests the plans, which are designed to: (a) restore applications and operating systems; and (b) demonstrate periodic testing of restoration from the back-up location.

10. **Assigned Security Responsibility.** BigID has designated a security official and has defined security roles for the development, implementation, and maintenance of its security program

11. **Secure Coding Practices.** BigID has implemented an industry-standard secure software lifecycle, which includes the OWASP Secure Coding Practices Quick Reference Guidelines. BigID's practices also include comprehensive security testing of all code, a risk assessment process, and secure code training for its developers.

12. **External Attestations.** BigID, on at least an annual basis, 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. BigID engages third parties to conduct a SOC 2 type 2 attestation, ISO 27001, and other relevant certifications

13. **Change and Configuration Management.** BigID maintains policies and procedures for managing changes to the Hosted Software, which include (a) a process for documenting, testing, and approving the promotion of changes into production; and (b) a security patching process that requires patching systems in a timely manner based on a risk analysis.

14. **Security Incident Response.** BigID has a security incident response plan that defines the roles and responsibilities of the security team in the event of a Security Incident. The plan covers the following components:

    a. **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 inform Customer of a Security Incident in accordance with this DPA and the Agreement.

    b. **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. If BigID makes any statements about a Security Incident, it will not name or identify Customer without Customer's prior written consent, unless such disclosure is required by Applicable Law.

    c. **Cooperation with Customer.** Upon Customer's request, BigID will cooperate with Customer to investigate any Security Incident and seek to identify the specific Customer Data involved in the Security Incident. Upon Customer's reasonable request, unless prohibited by Applicable Data Protection Laws, BigID will: (a) provide information regarding the nature and consequences of the Security Incident; and (b) reasonably assist Customer to notify affected parties, if required by Applicable Data Protection Laws. For the avoidance of doubt, 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.

15. **Security Monitoring and Vulnerability Scans.** BigID monitors production systems, including error logs on servers, disks and security events for any suspicious or malicious activities. Monitoring may include:

a. Conducting vulnerability scans of any servers, applications, and if applicable, endpoints and network devices deployed in the Hosted Software, to be performed periodically to identify, mitigate or remediate any vulnerabilities.

b. Subscribing to vulnerability intelligence services and/or to information security advisories and other relevant sources that provide insights about emerging security threats.

c. Reviewing changes affecting systems handling authentication, authorization, and auditing.

d. Reviewing privileged access to the Hosted Software to validate that privileged access is appropriate.

e. Engaging third parties to perform network vulnerability assessments and penetration testing on an annual basis. Such third-party security assessments include, at a minimum, a penetration test conducted by a reputable third-party, as well as additional tests and assessments for security vulnerabilities, as is deemed appropriate or identified by industry-recognized organizations (e.g., OWASP Top 10). Upon request, BigID may share an executive summary of penetration test results which are deemed suitable for external distribution.

f. Maintaining industry standard event logging for servers, applications, and networking equipment to facilitate Security Incident management. BigID maintains such logs for at least one (1) year.

g. Classifying vulnerabilities in accordance with the Common Vulnerability Scoring System or a successor industry standard risk rating methodology.

h. Mitigating and/or remediating vulnerabilities in the Hosted Software that are known to allow direct unauthorized access to Personal Data, whether by applying an available patch or taking other reasonable actions in the following time frames:

CVSSv3 Score	Severity	BigID Developed Software	Third-Party Software
Zero-day	Emergency	Within 48 hours of discovery.	Within 48 hours of patch availability.
9.0 - 10.0	Critical	Within 7 days of discovery.	Within 7 days of receiving notice of patch availability from the third-party vendor.
7.0 - 8.9	High	Within 30 days of discovery.	Within 30 days of receiving notice of patch availability from the third-party vendor.
4.0 - 6.9	Medium	Within 90 days of discovery.	Within 90 days of receiving notice of patch availability from the third-party vendor.

16. **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) industry standards; (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.