Vendor Data Processing Addendum

(June 2025)

This Vendor Data Processing Addendum ("Vendor DPA") is incorporated into and supplements the agreement and/or order form(s) by and between BigID and Vendor (collectively, the "Agreement"). In the course of providing the Services to BigID pursuant to the Agreement, Vendor may Process Personal Data on behalf of BigID 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.

1.1. "**Applicable Data Protection Laws**" means any law, statute, regulation or other binding restrictions applicable to the Processing of Personal Data under this Vendor 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.

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

1.3. "**BigID Data**" means data, documents, content, intellectual property, or information of any kind that BigID submits to Vendor, collects through its use of the Services, or provides to Vendor in the course of using the Services.

1.4. "**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.

1.5. "**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.

1.6. "**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.

1.7. "**EU 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 (Standard Contractual Clauses Information) to this Vendor DPA. As of the date of this Vendor DPA, the Standard Contractual Clauses are available here.

1.8. "**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 Vendor DPA, the United Kingdom and/or Switzerland.

1.9. "**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 Vendor DPA, (i) the UK General Data Protection Regulation as it forms part of the law of England, 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”).

1.10. “**Personal Data"** means any information contained within BigID 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.

1.11. “**Processing**” or “**Processes**” 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.

1.12. “**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.

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

1.14. “**Services**” means the services provided by Vendor to BigID pursuant to the Agreement.

1.15. “**Subprocessor**” means any Processor engaged by Vendor to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this Vendor DPA.

1.16. “**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.

1.17. “**UK Addendum**” means the UK Addendum to the 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 out in Schedule 2 to this Vendor DPA. As of the date of this Vendor DPA, the UK Addendum is available here.

1.18. “**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.

1.19. “**Vendor**” means the entity that executed the Agreement that is providing Services to BigID.

1.20. “**Vendor Personnel**” means Vendor’s employees, contractors, and other personnel it employs or contracts within Vendor’s organization.

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, BigID is the Controller, Vendor is the Processor, and Vendor may engage Subprocessors pursuant to the requirements set forth below. Vendor agrees that all BigID Data collected by, accessed, or retained by Vendor in the course of performing the Services remains the property of BigID.

2.2. **BigID’s Responsibilities**. BigID shall, in its use of the 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 Vendor as Processor. For the avoidance of doubt, BigID’s instructions for the Processing of Personal Data shall be consistent with the terms of the Agreement and this Vendor and shall comply with Applicable

Data Protection Laws. BigID shall have sole responsibility for the accuracy, quality, and legality of Personal Data, and the means by which BigID acquired Personal Data.

2.3. **Vendor's Responsibilities**. Vendor shall Process Personal Data in compliance with Applicable Data Protection Laws on behalf of and only in accordance with BigID's documented instructions and solely for the purpose of performing Services as defined in Schedule 1 (Details of the Processing), unless required to process Personal Data for other purposes by applicable law, in which case Vendor shall provide prior notice to BigID unless the relevant law prohibits such notice. Vendor shall inform BigID if it considers that BigID's instructions would be in breach of Applicable Data Protection Laws, in which case BigID agrees that Vendor shall not be required to carry out that Processing.

2.4. **Details of the Processing**. The subject matter of Processing of Personal Data by Vendor, 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 Vendor DPA are further specified in Schedule 1 to this Vendor DPA.

2.5. **Additional United States Processing Terms**. Where BigID 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:

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

b. Upon BigID's reasonable request, Vendor shall make available to BigID all information in its possession necessary to demonstrate Vendor's compliance with the obligations set forth in applicable US Data Protection Laws.

c. In the event Vendor receives or uses deidentified data in connection with the Agreement, Vendor shall implement and adhere to protective measures that ensure such data cannot be traced back to an individual and shall ensure all deidentified data requirements set forth in applicable US Data Protection Laws are implemented. In no event shall Vendor attempt to reidentify any deidentified data, in accordance with US Data Protection Laws.

d. Vendor shall not release, disclose, disseminate, make available, transfer, or otherwise communicate Personal Data to any third party, except to Vendor's Subprocessors that are bound by terms consistent with this Vendor DPA.

e. Vendor shall not sell, share, or resell Personal Data provided to Vendor in Vendor's role as a Service Provider.

3. Compliance Activities.

3.1. **Compliance**. Vendor, as Processor, has complied, and will continue to comply, with all Applicable Data Protection Laws. Vendor agrees to notify BigID within five (5) days of determining that Vendor cannot meet its compliance obligations. BigID, as Controller, shall be responsible for ensuring that, in connection with its provision of Personal Data and its use of the 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, Personal Data to Vendor for Processing in accordance with the terms of the Agreement including this Vendor DPA.

3.2. **Requests Received**.

a. **Data Subject Requests**. Vendor shall, to the extent legally permitted, notify BigID within five (5) days, if Vendor receives a Data Subject Request. Further, Vendor shall assist BigID in complying and fulfilling its obligations with respect to Data Subject Requests. In addition, to the extent BigID, in its use of the Services, does not have the ability to address a Data Subject Request, Vendor shall, upon BigID's request, provide commercially reasonable efforts to assist BigID in responding to such Data Subject Request, to the extent Vendor is legally permitted to do so and a response to such Data Subject Request is required under Applicable Data Protection Laws.

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

c. **Responses to Requests**. Vendor understands that it is not authorized to respond to the requests detailed in 3.3(a) and (b), unless explicitly authorized by BigID, except for a request received from a governmental agency with a subpoena or similar legal document compelling disclosure by Vendor, provided that Vendor notifies BigID in advance of any such disclosure, where legally permitted.

3.3. **Data Protection Assessments**. Upon BigID's request, Vendor shall provide BigID with reasonable cooperation and assistance needed to fulfil BigID's obligation under Applicable Data Protection Laws to carry out data protection impact assessments and/or data protection assessments related to BigID's use of the Services, to the extent (i) BigID does not otherwise have access to the relevant information, and (ii) such information is available to Vendor. Vendor shall provide reasonable assistance to BigID in the cooperation or prior consultation with regulators, including Supervisory Authorities, in the performance of its tasks relating to this Section 3.3 of this Vendor DPA, to the extent required under Applicable Data Protection Laws.

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

3.5. **Remediation**. Vendor shall cooperate fully with BigID to investigate, remediate, and mitigate the effects of the Security Incident, and assist in providing notice to the competent supervisory authority and to individuals, if requested by BigID.

4. **International Data Transfers.**

4.1. **Data Transfer Safeguards.** BigID acknowledges and agrees that Vendor may transfer Personal Data internationally to Vendor personnel and to third parties as needed 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/or (2) by implementing and maintaining the technical and organizational security measures outlined in Schedule 3.

4.2. **Data Transfer Impact Assessments**. Vendor shall assess the privacy and data protection laws of any third country with a Data Transfer Impact Assessment, not including those countries which the EDPB has designated as providing adequate protection, to which it plans

to transfer Personal Data. If Vendor determines that Personal Data may be improperly accessed, Vendor shall immediately notify BigID. In such an event, BigID may object to the planned transfer within thirty (30) days of BigID's receipt of notice. In the event of BigID's objection, Vendor shall have the right to cure the objection through one of the following options (to be mutually selected in good faith between Vendor and BigID): (a) Vendor will cancel its planned transfer; (b) Vendor will take the corrective steps requested by BigID in its objection (which remove BigID's objection) and proceed to transfer Personal Data to the jurisdiction in question; 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 thirty (30) days of Vendor's receipt of BigID's objection, BigID may terminate the Agreement and shall receive a pro-rata refund of prepaid fees for Services not performed as of the date of termination.

4.3. **EU Standard Contractual Clauses**. The EU Standard Contractual Clauses are incorporated into this Vendor DPA by reference and apply to transfers of Personal Data to Vendor from (i) BigID if it is subject to the GDPR, and (ii) BigID's 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 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 Vendor 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), BigID and any Affiliates shall each be deemed a "data exporter", and Vendor shall be deemed the "data importer".

5. **Subprocessors.**

5.1. **Overview.** Vendor shall provide its current list of Subprocessors in Schedule 4 (List of Subprocessors), which shall include the Subprocessor's name, the services for which it is contracted for, and the region in which it hosts BigID Data (the "Subprocessor List"). The Subprocessor List as of the date of execution of this Vendor DPA shall be considered authorized for the Processing of BigID Data by BigID. With respect to each Subprocessor, Vendor must (i) enter into a written contract that (a) requires Subprocessors to act on Vendor's instructions only with respect to Personal Data and (b) obligates Subprocessors to protect Personal Data using technical and organizational measures that are no less protective than the obligations in this Vendor DPA and Applicable Data Protection Laws; and (ii) remain responsible for the acts or omissions of Subprocessors to the same extent Vendor would be liable if performing the services of each Subprocessor directly.

5.2. **Changes to Subprocessors.** If Vendor needs to modify its Subprocessor List, Vendor must notify BigID with no less than sixty (60) days' written notice of any changes. BigID may object to any change to the Subprocessor List on reasonable grounds by informing Vendor within thirty (30) days of receipt of Vendor's notice. In the event of BigID's objection, Vendor shall have the right to cure the objection through one of the following options: (a) Vendor will cancel its plans to use the Subprocessor with regard to Personal Data or will offer an alternative to provide the Services without such Subprocessor; (b) Vendor will take the corrective steps requested by BigID in its objection (which remove BigID's objection) and

proceed to use the Subprocessor with regard to Personal Data; or (c) if none of the above options are reasonably available and the objection has not been resolved to BigID's reasonable satisfaction within thirty (30) days of Vendor's receipt of BigID's objection, BigID may terminate the Agreement and shall be entitled to a pro-rata refund of prepaid fees for the Services not performed as of the date of termination.

6. **Security.**

6.1. **Controls for the Protection of Personal Data**. Vendor shall implement appropriate technical and organizational measures designed to protect BigID Data from Security Incidents and to preserve the security and confidentiality of Personal Data, in accordance with the measures pursuant to Article 32 of the GDPR and as described in the security standards described in Schedule 3 (Security Measures).

6.2. **Security Notifications**.

a. Vendor shall, as soon as reasonably possible and no more than twenty-four (24) hours after Vendor becomes aware of or should have become aware of a Security Incident, notify BigID by e-mail at security@bigid.com. Such notification shall include all, relevant facts that Vendor knows at that time. Vendor shall assist and cooperate with BigID with any necessary or appropriate disclosures and other investigative, remedial, and monitoring measures as a result of any Security Incident.

b. Vendor shall, as soon as reasonably possible and no more than twenty-four (24) hours after Vendor becomes aware of or should have become aware, notify BigID by e-mail at security@bigid.com of any malware or vulnerability within the Services or the related network or systems that store and process BigID Data. Malware can include any virus, malware, program routine, device, or other undisclosed feature, including, without limitation, a time bomb, software lock, drop-dead device, malicious logic, worm, Trojan horse, or trap door that is capable of deleting, disabling, deactivating, corrupting, damaging, impairing, disrupting, modifying, erasing, interfering with, or otherwise harming or providing unauthorized access to BigID Data, hardware, virtual machines, containers, programs, codes, resources, or databases.

6.3. **Audits**. Upon request from BigID, not more than once per year unless preceded by a Security Incident, Vendor shall permit and cooperate with reasonable assessments, audits, or inspections carried out by BigID or BigID's assessor. Assessments may include a BigID-provided information security program questionnaire ("Security Review"). Vendor agrees to fully cooperate with such Security Review and implement all commercially reasonable changes to its information security program that are identified in the Security Review to be required for Vendor's compliance with this Addendum, at Vendor's sole cost and expense. In the event of BigID's audit request, subject to BigID's prior written consent, Vendor may arrange for a qualified and independent auditor to conduct an appropriate assessment, audit, or inspection of Vendor's policies and technical and organizational measures in support of Vendor's obligations pursuant to relevant and applicable US Data Protection Laws, using an industry-standard control standard or framework. Vendor shall furnish a report of any such assessments, audits, or inspections to BigID upon request.

6.4. **Deletion of Data**. Upon termination or expiration of the Agreement or at any time at BigID's written request, Vendor shall delete or return all BigID Data to BigID, unless retention of BigID Data is required by applicable law. Where Vendor is required by applicable law to retain some

or all BigID Data, Vendor shall extend the protections of the Agreement and this Vendor DPA to such BigID Data and limit any further Processing of such BigID Data to those limited purposes that require the retention, for so long as Vendor retains BigID Data.

6.5. Vendor Personnel.

a. **Confidentiality**. Vendor shall ensure that Vendor Personnel engaged in the Processing of Personal Data are informed of the sensitive nature of Personal Data, has been subject to and passed completed background checks, have received appropriate training on their responsibilities, and are bound by written confidentiality agreements. Vendor shall also ensure that Vendor Personnel are made aware of Vendor's obligations under the Agreement and under applicable laws.

b. **Reliability**. Vendor shall take commercially reasonable steps to ensure the reliability of any Vendor Personnel engaged in the Processing of Personal Data.

c. **Limitation of Access**. Vendor shall ensure that access to Personal Data is limited to those Vendor Personnel who require access to provide and operate the Services in accordance with the Agreement.

7. **Cyber and Privacy Insurance.**

In addition to the insurance requirements set forth in the Agreement, Vendor shall maintain, at its sole cost and expense, Privacy and Cybersecurity insurance (or its equivalent) of not less than five million US dollars ($5,000,000). Coverage shall be sufficiently broad to respond to the duties and obligations undertaken by Vendor in this Vendor DPA. Vendor shall maintain this coverage for the duration of the Agreement and for no less than one (1) year thereafter.

8. **Termination and Survival.**

8.1. Vendor shall cease Processing Personal Data upon the termination or expiration of the Agreement.

8.2. The provisions in this Vendor DPA relating to the protection of Personal Data shall survive termination of the Agreement and this Vendor DPA, and remain in effect for as long as Vendor Processes Personal Data.

9. **Miscellaneous.**

9.1. **Privacy Representative**. Vendor has appointed a privacy representative (e.g., a Data Protection Officer) who is accountable for compliance with Applicable Data Protection Laws. The representative can be reached at [to be filled out by Vendor].

9.2. **Amendments**. Upon prior written notice, BigID shall have the right to unilaterally amend the requirements of this Vendor DPA to the extent required to remain in compliance with Applicable Data Protection Laws. Such amendments shall automatically take effect sixty (60) days after notice is provided (or sooner where required to comply with Applicable Data Protection Laws).

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

9.4. **Disputes**. Any claims brought under this Vendor DPA shall be subject to the terms and conditions of the Agreement, including but not limited to the exclusions and limitations included therein.

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.	**VENDOR**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

SCHEDULE 1 – DETAILS OF THE PROCESSING

Nature and Purpose of Processing

Vendor (and its Subprocessors) will Process Personal Data as necessary to perform and operate the Services pursuant to the Agreement and as further instructed by BigID. This includes:

[To be filled out by Vendor]

Duration and frequency of Processing, and Period for which Personal Data will be Retained

[To be filled out by Vendor]

Categories of Data Subjects

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

[To be filled out by Vendor]

Type of Personal Data

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

[To be filled out by Vendor]

SCHEDULE 2 – STANDARD CONTRACTUAL CLAUSES 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 out in the Agreement.
2. The signatures of each party and date of this Vendor are deemed to be inserted.
3. The role of BigID is specified as "controller" and the role of Vendor is specified as "processor".
4. Annex I.B. is completed with the information set out in Schedule 1 to this Vendor DPA, as well as the details of the restrictions and safeguards set out in Schedule 3 to this Vendor 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 organisational measures set forth in Schedule 3 to this Vendor DPA.
6. Annex I.C. is completed as follows:
    a. Where Vendor'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 Vendor'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 BigID is established, (ii) if BigID is not established in the European Union, the member state of the European Union in which BigID has appointed its European Union representative, or (iii) if BigID 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 out in Section 5 above. The "agreed list" referred to in this clause shall be the Subprocessor List referred to in Schedule 4 of this Vendor DPA.
9. The optional wording in Clause 11(a) is deleted.
10. Option 2 is deleted from clause 17, and:
    a. Where BigID'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 BigID's processing of Personal Data falls within 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 BigID's Processing of Personal Data does not fall within the scope of the EU GDPR, with the words "England and Wales"; or

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

12. If there is any conflict between this Vendor 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 out 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 out in this Schedule, applying to a transfer in accordance with Clause 4.4 of this Vendor 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 BigID will no longer transfer Personal Data subject to the UK GDPR to Vendor under the Agreement and this Vendor 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 to and made a part of this Vendor DPA. All capitalized terms not defined in these Security Measures or in this Vendor DPA shall have the meaning set forth in the Agreement. Vendor shall apply the following safeguards to protect BigID Data.

1. **Information Security Program**.

   a. Vendor shall implement and maintain a written information security program in which Vendor implements and maintains administrative, technical, and physical safeguards to ensure the security, confidentiality, and integrity of BigID Data, in compliance with Applicable Data Protection Laws. Vendor shall provide BigID with a copy of its security program promptly following BigID's request. Vendor shall, at a minimum, maintain a security program that: (i) protects against any anticipated threats or hazards to the security or integrity of BigID Data, including a Security Incident; (ii) address how any Security Incident will be handled; (iii) designates a senior employee responsible for overseeing and implementing the security program; and (iv) is appropriate to the nature, size, and complexity of Vendor's business operations. Such security program shall meet current industry standards and comply with Applicable Data Protection Laws. Vendor must not disclose BigID Data to a third party except as permitted in this Vendor DPA or at the specific written request of BigID.

   b. Vendor shall conduct a risk assessment periodically, and will promptly implement, at its sole cost and expense, a corrective action plan to correct any issues that are reported under the assessment or any scanning, vulnerability, or penetration testing. Vendor shall perform at least: (i) quarterly vulnerability scans; and (ii) annual penetration tests. Upon request, Vendor shall provide vulnerability assessment summaries or attestation letters and a description of corrective action plans. BigID may perform or engage a third party to perform vulnerability scans/penetration testing of the Services.

2. **Training**. Vendor will conduct information security awareness training for all employees involved in the delivery of the Services. Employees and contractors using the organization's information systems and services shall be trained on and required to report any observed or suspected information security weaknesses to Vendor's security team.

3. **Hosting**. Vendor shall provide BigID with information regarding the hosting service(s) and their location(s) that Vendor is using to host BigID Data (the "Hosting Services"). Vendor shall provide BigID with no less than sixty (60) days advance written notice, of (a) its intention to change the geographical region of hosting and/or (b) its intention to change the Hosting Service to another Hosting Service. Such notification shall include the name and the new location of the Hosting Service. In any such event, BigID reserves the right to terminate the Agreement on thirty (30) days' notice to Vendor.

4. **Controlling Access to BigID Data**. Vendor shall ensure that access to BigID Data is limited to Vendor Personnel and authorized agents who need to know such information solely for the purposes contemplated under the Agreement. Without limiting the foregoing, Vendor agrees that:

   a. Vendor must have an inventory of all company assets that may access BigID Data. The inventory must record and track asset description, ownership, location, and assigned users, at a minimum.

   b. Vendor must enforce the principle of least privilege (i.e., an individual is only given the minimum access necessary to meet business requirements) when providing Vendor

Personnel with access to systems containing BigID Data. Access to BigID Data must be revoked immediately when no longer required and Vendor must perform reviews of user access to BigID Data at least every 6 months and promptly after any employment changes (e.g., promotion, demotion, or termination).

c. Vendor must ensure only authorized individuals have privileges to create access accounts to systems containing BigID Data. For any BigID production system, Vendor shall ensure that it receives BigID's prior written consent prior to authorizing Vendor Personnel to access such production system.

d. Vendor must ensure that Vendor Personnel accessing (i) BigID Data remotely are authenticated using multi-factor authentication mechanisms via a secure connection, and (ii) Vendor's systems that Process and/or host BigID Data are authenticated using multi-factor authentication and can only be accessed via Vendor-managed endpoints.

e. Vendor shall inform all personnel with exposure or access to BigID Data of Vendor's obligations under these the Agreement and this Vendor DPA and shall ensure all such personnel are bound by legal obligations no less restrictive than the terms of the Agreement.

f. Vendor must keep security event logs, including actual or attempted logon violations and access violations, on systems storing, processing, or transmitting BigID Data to permit tracking of system activity. Security event logs must be retained for a minimum of one (1) year and reviewed regularly for unauthorized or unlawful activity.

g. Vendor shall not use or disclose BigID Data to contact or market to Vendor's customers or employees, including BigID, unless otherwise permitted in writing by BigID.

h. Vendor shall use secure user authentication protocols, including assigning unique identifications and strong passwords to each individual with access to BigID Data. Vendor shall ensure that:

    i. Passwords shall not be Vendor-supplied default passwords and must be stored in a location and format that does not compromise the security of the data they protect. Passwords must be obscured such that unauthorized parties are not able to observe or subsequently recover them; and

    ii. Passwords must be chosen in accordance with industry best practices. Passwords must (a) be no less than twelve (12) characters; (b) require complexity, including character class choices, such as upper-case letters, lower case letters, numeric digits and/or special characters; (c) where available, use a mechanism to prevent the reuse of at least the last five (5) passwords; and (d) be changed after incidents and otherwise as recommended by industry best practices.

i. Access to Vendor systems Processing and/or hosting BigID Data shall be blocked after five (5) unsuccessful attempts to gain access. Inactivity timeouts shall be established for no less than thirty (30) minutes for all systems and applications that Process and/or host BigID Data.

j. Where applicable, Vendor shall enforce clean desk/clear screen policies to make sure that BigID Data is not left unattended in any public place at any time.

5. **BigID Data In-Transit and At-Rest**.

a. Vendor agrees that any BigID Data hosted by Vendor on behalf of BigID shall be logically segregated from information related to any other customer of Vendor. Vendor shall protect its database infrastructure via internet firewalls in accordance with current industry standards on an ongoing basis.

b. BigID Data should not be stored on endpoint devices, mobile devices, external hard drives, or removable media (e.g., USB Thumb Drives, CDs, or DVDs) without BigID's prior written consent. Electronic and paper records containing BigID Data must be stored in a locked room or area where access is controlled.

c. Vendor shall encrypt all records and files containing BigID Data, both at rest and in transit, using an up-to-date industry-standard encryption standard for BigID Data.

d. Vendor must ensure appropriate, up-to-date anti-virus/anti-malware detection software is implemented across all information systems processing BigID Data in its organization.

6. **Deletion of Data**. Vendor shall delete BigID Data in accordance with the National Institute of Standards and Technology ("NIST") Guidelines for Media Sanitization from Vendor's and, where applicable, its Subprocessors' systems. Vendor shall certify in writing within thirty (30) days of BigID's request for destruction that these actions have been completed. Where Vendor is required by applicable law to retain some or all of the BigID Data in its possession, Vendor shall extend the protections of the Agreement and this Vendor DPA to such BigID Data and limit any further use of such BigID Data to only those limited purposes that require the retention, for so long as Vendor retains BigID Data.

7. **Incident Management**.

a. Vendor must ensure that incident management procedures are maintained, that they are communicated to its personnel, and that incidents are logged.

b. In the event of any loss or corruption of BigID Data, Vendor shall use commercially reasonable efforts to restore the lost or corrupted BigID Data from the latest backup maintained by Vendor in accordance with its archival procedures. Such incidents will be recorded and investigated in accordance with Vendor's incident management procedures. Vendor shall notify BigID by email to security@bigid.com, in writing within twenty-four (24) hours of becoming aware of a Security Incident. Vendor's notice shall include, at a minimum: (i) a description of the Security Incident, including the date it occurred and the BigID Data accessed, acquired, lost and/or misused ; (ii) the number of individuals affected and their states of residence; and (iii) a description of the steps taken to investigate the incident, secure Vendor's systems, recover lost information, and prevent the recurrence of further Security Incidents or losses of a similar type. In connection with any Security Incident, Vendor will provide BigID with a copy of applicable forensic report(s).

c. Except as required by applicable law, Vendor agrees that it will not inform any third party of any Security Incident without BigID's prior written consent. If such disclosure is required by applicable law, Vendor agrees to consult with, and obtain the prior approval (which shall not be unreasonably withheld or delayed) of BigID regarding the content of such disclosure. Without limiting the foregoing, BigID will determine which party will make

any disclosure to law enforcement or regulatory authorities regarding a Security Incident and Vendor agrees to abide by BigID's determination.

d. In the event of any Security Incident, Vendor shall cooperate with BigID, at Vendor's cost, to (i) further assess the nature and scope of any such Security Incident and review all records pertaining to BigID, redacted to not compromise Vendor's confidentiality obligations to third parties; (ii) take reasonable and necessary remedial measures to mitigate the risk arising out of the Security Incident; and (iii) provide breach notifications approved by BigID to affected individuals notifying them that their Personal Data was compromised. Vendor shall fully cooperate with all government and regulatory agencies and law enforcement having jurisdiction and authority to investigate a Security Incident.

e. Vendor shall ensure separation of duties for security administration, access review, and security violation investigations. Vendor shall establish separation between development and operations personnel, as well as other potentially conflicting roles.

8. Verification and Auditing.

a. Vendor will maintain a SOC 2 Type 2 attestation covering each of the Trust Services Criteria performed by an industry recognized and qualified independent third-party auditor, at Vendor's expense. Vendor shall provide BigID with a copy of its SOC 2 Type 2 at BigID's request.

b. BigID or its authorized third party has the right, with thirty (30) days advanced written notice, to review the terms, records and/or facilities of Vendor for the purposes of verifying Vendor's compliance with the requirements of these Security Measures. Vendor will provide BigID with access to its site, systems, and records as reasonably necessary and Vendor will make available any relevant Vendor employees and/or contractors. Such verification will be at BigID's expense, unless it reveals material non-compliance with the requirements of these Security Measures, in which case such costs will be paid by Vendor.

9. **Backup and Disaster Recovery**.

a. Vendor must maintain a disaster recovery and business continuity plan defining how BigID Data will be recovered and describing how Vendor will continue operating during the recovery period. Recovery time objectives ("RTO") and recovery point objectives ("RPO") must be defined and shared with BigID upon request.

b. Vendor must test its disaster recovery and business continuity plan at least once per year to validate disaster recovery and business continuity procedures as well as the RTO and RPO. The tests must incorporate scenarios for availability zone failure as well as a regional failure.

c. Vendor must perform regular encrypted backups of BigID Data processed on its information systems.

10. System Development and Secure Coding.

a. Vendor must follow an industry-accepted secure code development lifecycle (e.g., Microsoft SDL). Vendor shall establish an application development and maintenance framework that protects the security and integrity of BigID Data and Vendor's Services in accordance with the OWASP Secure Coding Practices Quick Reference Guidelines and materials referenced therein, as updated periodically.

b. Vendor must have comprehensive security testing integrated into its security development lifecycle, including secure code reviews, SAST and DAST, for all applications that store or process BigID Data.

c. Vendor shall maintain documentation on overall system, network, and application architecture, data flows, process flows, and security functionality for all applications that process or store BigID Data.

d. Vendor will patch all workstations and servers with all current operating system, database, and application patches deployed in Vendor's computing environment according to a schedule predicated on the criticality of the patch. Vendor must perform appropriate steps to help ensure patches do not compromise the security of the information resources being patched.

e. Vendor will employ an effective, documented change management program with respect to the Services as an integral part of its security profile. This includes logically or physically separate environments from production for all development and testing. Vendor shall not use BigID Data in development or testing environments, unless BigID Data has been sufficiently sanitized such that it is aggregated and anonymized.

f. Vendor shall use leading continually updated programs in its coding practices designed to ensure that the Services will be free of any malware.

11. **Security Monitoring and Vulnerability Management**. Vendor must monitor network and production systems, including error logs on servers, disks and security events for any suspicious or malicious activities. Monitoring generally includes:

a. Conducting vulnerability scans of any servers, applications, endpoints, and network devices deployed in or used with the Hosted Services to be performed periodically to identify, mitigate and/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 Services 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. Vendor must maintain such logs for at least one (1) year.

g. Classifying malware and security vulnerabilities in accordance with industry standard risk rating methodologies (e.g., OWASP and NIST) and take prompt appropriate actions to mitigate risks before Vendor is able to provide a security patch. Vendor shall install a suitable tested security patch release that fully removes and remediates identified malware and vulnerabilities within the timeframes set forth in the table below. If BigID Data has been adversely affected by malware or a vulnerability, Vendor shall assist and cooperate with BigID to make any necessary or appropriate disclosures and with respect to other investigative, remedial, and monitoring measures.

CVSSv3 Score	Severity	Vendor 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.

12. **Background Checks**. Vendor shall obtain appropriate background checks for all Vendor Personnel who may have access to BigID Data or any development or testing environments or source code. Vendor will not permit any Vendor Personnel that has failed to pass a background check to have access to BigID Data. Without limiting the generality of the foregoing, Vendor will not permit any Vendor Personnel that has been convicted of, or pleaded guilty or nolo contendere to, a felony or misdemeanor involving theft, dishonesty, fraud, or computer-related crimes, during the prior seven (7) years to have access to BigID Data.

13. **Continuity of Business Operations**. Vendor shall have business continuity and disaster recovery plans established to maintain a level of service consistent with its obligations under the Agreement, including but not limited to procedures to backup all BigID Data to meet its RPO and RTO commitments. Vendor shall periodically, and in any event at least once per year, fully and successfully test such business continuity and disaster recovery plans. Upon request, Vendor shall provide test activity logs and test results for review by BigID. Backups shall be appropriately protected via strong access controls, encryption, and as otherwise required by these Security Measures.

14. **Subprocessors and Subcontractors.** If Vendor uses Subprocessor(s) to host Vendor's Services, or a subcontractor to provide any portion of the Services or related support services, Vendor must ensure that such third-party complies with all requirements applicable to Vendor herein. Vendor shall be liable to BigID for such third party's compliance with the terms of this Vendor DPA and Vendor shall notify BigID immediately if the third-party is in breach of its obligations.

15. **Physical and Environmental Security**. Vendor shall maintain industry-standard physical security controls to safeguard the systems that store and process BigID Data, including but not limited to (i) physical entry controls to ensure that only authorized individuals gain access to such facilities, and (ii) environmental controls to protect against damage from fire, flood, and other forms of man-made or natural disasters.

16. Network Security.

a. Vendor shall use up-to-date versions of system security products such as firewalls, proxies, web application firewalls, and interfaces. Such products must include malware protection, up-to-date patches and virus definitions and must receive the most current security updates on a regular basis. Vendor shall have current anti-virus and malware programs installed and running to scan for and promptly remove viruses and malware on all Vendor endpoints.

b. Vendor shall have a patch management process that includes, but is not limited to, testing patches before installation on all systems used to process and/or host BigID Data or are used to deliver Services to BigID.

c. Vendor shall ensure that its system administrators maintain complete, accurate, and up-to-date information regarding the configuration of all information systems used to process and/or host BigID Data.

d. Vendor shall maintain intrusion detection and prevention processes to identify both internal and external vulnerabilities and risks that may result in a Security Incident.

SCHEDULE 4 – LIST OF SUBPROCESSORS

BigID has authorized Vendor to engage the Subprocessors listed below.

To be completed by Vendor.