Dated: July 13, 2023

This Data Processing Addendum ("**DPA**") is made a part of and incorporated into the agreement entered into by and between the PubMatic, Inc. ("**PubMatic**") and the party identified in the signature block of the originating Agreement ("**Supplier**"), governing the PubMatic's use of the Supplier's services (the "**Agreement**" or "Contract"). In the event of a conflict between the Agreement and this DPA, this DPA shall control to the extent of the conflict with respect to the Vendor's Processing and disclosure of any Data (including Personal Data).

1. **DEFINITIONS**
    1. **"Affiliate"** means any entity that is directly or indirectly controlled by, controlling or under common control with PubMatic and/or Supplier (as applicable). "Control" for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
    2. **"Authorized Affiliate"** means any PubMatic Affiliate permitted to use the Services pursuant to the Contract(s) between PubMatic and Supplier but has not signed its own agreement with Supplier.
    3. "**Applicable Privacy Law(s)**" means all worldwide data protection and privacy laws and regulations applicable to the Personal Data in question, including, where applicable, European Data Protection Law.
    4. **"Authorized Persons"** means any person who processes Personal Data on Supplier's behalf, including Supplier's employees, officers, partners, principals, contractors and Sub-processors.
    5. **"European Data Protection Law"** means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("GDPR"); (ii) the EU e-Privacy Directive (Directive 2002/58/EC); (iii) any national data protection laws made under or pursuant to (i) or (ii); (iv) the Swiss Federal Data Protection Act of 19 June 1992 and its corresponding ordinances ("**Swiss DPA**") and (v) in respect of the United Kingdom, GDPR as it forms part of United Kingdom law pursuant to Section 3 of the European Union (Withdrawal) Act 2018 and the Data Protection Act 2018 (together, "**UK Privacy Law**"), in each case, as superseded, amended or replaced.
    6. **"Standard Contractual Clauses"** means Module 1 (Controller to Controller), Module 2 (Controller to Processor) or Module 3 (Processor to Processor), as applicable, of the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 located at https://eur-lex.europa.eu/eli/dec_impl/2021/914, completed in accordance with this DPA.
    7. **"Personal Data"** means any PubMatic Data relating to an identified or identifiable natural person ("data subject") and/or any PubMatic Data that is deemed personal data or personally identifiable information under Applicable Privacy Laws.
    8. **"Privacy Shield"** means the EU-US and Swiss-US Privacy Shield Frameworks, as operated by the U.S. Department of Commerce.

9. **“Privacy Shield Principles”** means the Privacy Shield Framework Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision of 12 July 2016 pursuant to the Directive, details of which can be found at www.privacyshield.gov/eu-us-framework.
10. **“PubMatic Data”** means all information (i) provided to Supplier by or at the direction of PubMatic; (ii) created or obtained by Supplier on behalf of PubMatic; or (iii) which Supplier accesses at the direction of PubMatic , in the course of Supplier’s performance under the Contract(s), including (but not limited to) any information that pertains to PubMatic and/or is Confidential Information (as defined under the Contract(s)).
11. **"Restricted Transfer"** means: (i) where the GDPR applies, a transfer of Personal Data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; (ii) where the UK Privacy Law applies, a transfer of personal data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of personal data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner;
12. **“Security Incident”** means any unauthorized or unlawful breach of security leading to, or reasonably believed to have led to, the accidental or unlawful destruction loss, alteration, unauthorized disclosure or access to PubMatic Data and/or Business Contact Data.
13. **“Sub-processor”** means any third party (including any Supplier’s affiliate) engaged directly or indirectly by Supplier to process any Personal Data relating to this DPA and/or the Contracts. The term “Sub-processor” shall also include any third party appointed by a Sub-processor to process any Personal Data relating to this DPA and/or the Contracts.
14. "**UK Addendum**” means the International Data Transfer Addendum (version B1.0) to the EU Commission Standard Contractual Clauses issued by UK Information Commissioners Office under S.119(A) of the UK Data Protection Act 2018, as amended, superseded or replaced from time to time.
15. The terms **“Controller”**, **“Processor”**, "**personal data**" and **“processing”**, have the meanings given to them in Applicable Privacy Laws. If and to the extent that Applicable Privacy Laws do not define such terms, then the definitions given in European Data Protection Law will apply.

2. **ROLE AND SCOPE OF PROCESSING**
    1. **Roles of the Parties and Details of Processing.** Supplier shall process Personal Data under the Contract(s) as a Processor acting on behalf of PubMatic and/or its Affiliates (whether acting as Controller or acting as a Processor on behalf of third party Controllers). Supplier agrees that it will process Personal Data in compliance with the terms of this DPA.
    2. **Supplier’s Processing of Personal Data.** Supplier shall at all times: (i) process the Personal Data only for the purpose of providing the Services to PubMatic under the Contract(s) and in accordance with PubMatic’s documented instructions

(of which this DPA shall form part); (ii) not process the Personal Data for its own purposes or those of any third party.

3. **Supplier's Notification Obligations Regarding PubMatic Instructions.** Suppliers shall promptly notify PubMatic in writing, unless prohibited from doing so under Applicable Privacy Law, if:
    1. It becomes aware or believes that any data processing instruction from PubMatic violates Applicable Privacy Law;
    2. It is unable to comply with PubMatic 's data processing instructions for any reason; and/or
    3. It is unable to comply with the terms of the Contract(s) (including this DPA) as they relate to or govern the processing of Personal Data and/or the security of PubMatic Data for any reason.
4. **Business Contact Data.** PubMatic shall disclose to Supplier contact information relating to PubMatic's representatives for (i) invoicing, billing and other business inquiries, (ii) information on usage of the Services, and (iii) contract management, which may include personal data (**"Business Contact Data"**). Supplier shall comply with all applicable laws and its applicable privacy policies with respect to the Processing of Business Contact Data and use Business Contact Data only for the purposes outlined in this Section 2.4.
5. **No Rights for Supplier.** Except as expressly set forth to the contrary in this DPA and the Contract(s), Supplier acknowledges that it has no right, title or interest in PubMatic Data (including all Personal Data, intellectual property or proprietary information) and may not sell, rent or lease PubMatic Data to anyone.

3. **SUBPROCESSING**
    1. **Appointment of Sub-processors.** Supplier shall not subcontract any processing of the Personal Data to a Sub-processor without the prior written consent of PubMatic. Notwithstanding the foregoing, PubMatic consents to Supplier engaging Sub-processors to process the Personal Data provided that:
        1. Supplier has or shall provide upon request a list of its current Sub-processors prior to the date of the execution of the Agreement and this DPA and thereafter provides at least 30 days prior written notice to PubMatic of the engagement of any new Sub-processor (including details of the processing and location) and Supplier shall update the list of all Sub-processors engaged to process Personal Data under this Agreement in writing and send such updated version to PubMatic prior to the engagement of the Sub-processor;
        2. Supplier imposes the same data protection terms on any Sub-processor it engages as contained in this DPA (including the Privacy Shield Principles and/or other data transfer provisions, where applicable); and
        3. Supplier remains fully liable for any breach of this DPA or the Contract(s) that is caused by an act, error or omission of such Sub-processor.
    2. **Objection Right for New Sub-Processors.** PubMatic may object to the appointment or replacement of a Sub-processor within 20 days after PubMatic first receives prior notice of such change in accordance with Section 3.1(a) above, provided such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss in good faith commercially

reasonably alternative solutions. If the parties cannot reach resolution within a reasonable period of time, which shall not exceed thirty (30) days, Supplier will either not appoint or replace the Sub-processor or, if this is not possible, PubMatic may terminate the Contract(s) (in whole or in part), by providing written notice to Supplier. PubMatic shall receive a refund of any prepaid fees for the period following the effective date of termination in respect of the terminated products or services without imposing a penalty for such termination on PubMatic.

4. **DATA SUBJECT RIGHTS AND COOPERATION**
    1. **Data Subject Request.** Supplier shall reasonably cooperate with PubMatic to enable PubMatic (or its third-party Controller) to respond to any requests, complaints or other communications from data subjects and data protection supervisory authorities, regulatory or judicial bodies relating to the processing of Personal Data and Business Contact Data under the Contract(s), including requests from data subjects seeking to exercise their rights under Applicable Privacy Laws. In the event that any such request, complaint or communication is made directly to Supplier, Supplier shall promptly pass this onto PubMatic and shall not respond to such communication without PubMatic's express authorization.
    2. **Subpoenas and Court Orders.** If Supplier receives a subpoena, court order, warrant or other legal demand from a third party (including law enforcement, data protection supervisory authority, or other public or judicial authorities) seeking the disclosure of Personal Data, Supplier shall not disclose any information but shall immediately notify PubMatic in writing of such request, and reasonably cooperate with PubMatic if it wishes to limit, challenge or protect against such disclosure, to the extent permitted by applicable laws.
    3. **Data Privacy Impact Assessments ("DPIA's").** Supplier will provide reasonable assistance to PubMatic (or its third-party Controller) in connection with data protection impact assessments and any consultation with applicable data protection authorities in respect of any processing of Personal Data under the DPA, where such assessments and consultation are deemed necessary by PubMatic (or a third-party Controller).
5. **DATA ACCESS & SECURITY MEASURES**
    1. **Confidentiality and Limitation of Access.** Supplier shall ensure that any Authorized Person is subject to a strict duty of confidentiality (whether a contractual or statutory duty) and that they process the Personal Data only for the purpose of delivering the Services under the Contract(s) to PubMatic. Supplier shall ensure that Supplier's access to Personal Data is limited to those personnel performing Services in accordance with this DPA.
    2. **Security Measures.** Supplier will implement and maintain all appropriate technical and organizational security measures to protect PubMatic Data and Business Contact Data from Security Incidents and to preserve the security, integrity and confidentiality of such data ("**Security Measures**"). Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Such measures shall at a minimum include: the pseudonymization and encryption of

personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a Security Incident; a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of processing. At a minimum, Supplier agrees to the Security Measures identified at Annex II to this DPA.

6. **SECURITY INCIDENTS**
    1. **Notification of Security Incidents.** In the event of a Security Incident, Supplier shall promptly (and in no event later than 24 hours of becoming aware of such Security Incident) inform PubMatic and provide written details of the Security Incident, including the type of data affected and the identity of affected person(s) as soon as such information becomes known or available to Supplier.
    2. **Suppliers Obligations Following Security Incident.** Furthermore, in the event of a Security Incident, Supplier shall:
        1. provide timely information and cooperation as PubMatic may require to fulfil PubMatic's data breach reporting obligations under Applicable Privacy Laws or to comply with or respond to any inquiries by a data protection supervisory authority or any lawsuit arising from the Security Incident, including without limitation collecting and preserving all evidence pertaining to the Security Incident and the investigation conducted by Supplier;
        2. take such measures and actions as are appropriate to remedy or mitigate the effects of the Security Incident and shall keep PubMatic up-to-date about all developments in connection with the Security Incident; and
        3. reimburse PubMatic for the reasonable costs for PubMatic to prepare and send all notifications that are legally required or reasonably necessary (as determined in the sole discretion of PubMatic). At the written request of PubMatic, Supplier agrees to provide, at its sole expense, credit monitoring and identity theft protection services to individuals affected by a Security Incident involving Personal Data of those individuals.
    3. The content and provision of any notification, public/regulatory communication or press release concerning the Security Incident shall be solely at PubMatic's discretion, except as otherwise required by applicable laws.
7. **SECURITY REPORTS & INSPECTIONS**
    1. **Supplier Security Standards.** Supplier shall maintain records in accordance with ISO 27001 or similar Information Security Management System ("**ISMS**") standards. Upon request, Supplier shall provide copies of relevant external ISMS certifications, audit report summaries and/or other documentation reasonably required by PubMatic to verify Supplier's compliance with this DPA.
    2. **Right of Inspection.** While it is the parties' intention ordinarily to rely on Supplier's obligations set forth in Section 7.1 to verify Supplier's compliance with this DPA, PubMatic (or its appointed representatives) may carry out an inspection of the Supplier's operations and facilities during normal business hours and subject to reasonable prior notice where PubMatic considers it necessary or appropriate (for example, without limitation, where PubMatic has reasonable

concerns about Supplier's data protection compliance, following a Security Incident or following instruction from a data protection authority).

8. **INTERNATIONAL TRANSFERS**
    1. **International Transfers.** Supplier and/or its Affiliates shall not process or transfer any Personal Data and/or Business Contact Data in or to a territory other than the territory in which the Personal Data and/or Business Contact Data was first collected (nor permit such data to be so processed or transferred) unless it takes all such measures as are necessary to ensure such processing or transfer is in compliance with Applicable Privacy Laws (including such measures as may be communicated by PubMatic to Supplier). Supplier shall inform PubMatic of any international transfers of Personal Data in advance of making the transfer and shall assist PubMatic in assessing the parties' respective obligations to comply with Applicable Privacy Laws.
    2. **Privacy Shield Flow Downs.** To the extent that PubMatic and/or the Authorized Affiliates are self-certified to the Privacy Shield, Supplier represents and warrants that it shall:
        1. provide (and procure all Sub-processors that provide) at least the same level of protection to such Personal Data as is required by the Privacy Shield Principles and the Security Measures set forth in Section 5.2 of this DPA;
        2. promptly notify PubMatic if it makes a determination that it can no longer meet its obligations under Section 8.2(a) above, and in such event, to work with PubMatic and promptly take all reasonable and appropriate steps to stop and remediate (if remediable) any processing until such time as the processing meets the level of protection as is required by Section 8.2(a); and
        3. immediately cease (and procure all Sub-processors immediately cease) processing such Personal Data if in PubMatic 's sole discretion, PubMatic determines that Supplier has not or cannot correct any non-compliance with Section 8.2(a) above in accordance with Section 8.2(b) within a reasonable time frame.
    3. **Transfer Mechanism.** The parties agree that when the transfer of personal data from PubMatic (as exporter) to Supplier (as importer) is a Restricted Transfer and European Data Protection Law applies, the transfer shall be subject to the appropriate Standard Contractual Clauses, which shall be deemed incorporated into and shall form part of this DPA, as follows:
        1. in relation to Personal Data that is protected by the GDPR and processed in accordance with Section 2.1 of this DPA, (i) Module Two (controller to processor transfers), or Module 3 (processor to processor transfers) will apply, as appropriate; (ii) in Clause 7, the optional docking clause will apply; (iii) in Clause 9, Option 2 will apply, and the time period for prior notice of sub-processor changes shall be as set out in Section 3 of this DPA; (iv) in Clause 11, the optional language will not apply; (v) in Clause 17, Option 1 will apply, and the Standard Contractual Clauses will be governed by Irish law; (vi) in Clause 18(b), disputes shall be resolved before the courts of Ireland; (vii) Annex I of the Standard Contractual

Clauses shall be deemed completed with the information set out in Annex I to this DPA, as applicable; and (viii) Annex II of the Standard Contractual Clauses shall be deemed completed with the information set out in Annex II to this DPA;

2. in relation to Business Contact Data that is protected by the GDPR and processed in accordance with Section 2.4 of this DPA, the Standard Contractual Clauses will apply completed as follows: (i) Module One will apply (controller to controller transfers); (ii) in Clause 7, the optional docking clause will apply; (iii) in Clause 11, the optional language will not apply; (v) in Clause 17, Option 1 will apply, and the Standard Contractual Clauses will be governed by Irish law; (vi) in Clause 18(b), disputes shall be resolved before the courts of the Ireland; (vii) Annex I of the Standard Contractual Clauses shall be deemed completed with the information set out in Annex I to this Agreement, as applicable; and (viii) Annex II of the Standard Contractual Clauses shall be deemed completed with the information set out in Annex II to this Agreement;
3. in relation to personal data that is protected by the UK Privacy Law, the Standard Contractual Clauses shall apply in accordance with Sections 8.3(a) and 8.3(b) of this DPA (as applicable), but as modified and interpreted by the Part 2: Mandatory Clauses of the UK Addendum, which shall be incorporated into and form an integral part of this DPA. Any conflict between the terms of the Standard Contractual Clauses and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum. In addition, tables 1 to 3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Annex I (as applicable) and Annex II of this DPA and table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party";
4. in relation to personal data that is protected by the Swiss DPA, the Standard Contractual Clauses shall apply in accordance with Sections 8.3(a) and 8.3(b) of this DPA (as applicable), but with the following modifications: (i) any references in the Standard Contractual Clauses to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA and the equivalent articles or sections therein; (ii) any references to "EU", "Union", "Member State" and "Member State law" shall be interpreted as references to Switzerland and Swiss law, as the case may be; (iii) any references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the relevant data protection authority and courts in Switzerland; and (iv) the Standard Contractual Clauses shall be governed by the laws of Switzerland and disputes shall be resolved before the competent Swiss courts;
5. in the event that any provision of this DPA and/or the Agreement contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail;
6. Supplier will not participate in any other Restricted Transfers of personal data unless the Restricted Transfer is made in compliance with Applicable

Privacy Laws and pursuant to Standard Contractual Clauses implemented between the relevant exporter and importer of the personal data, as necessary in order to comply with Applicable Data Protection Law.

4. **Disclosures**. Supplier acknowledges that PubMatic may disclose this DPA and any relevant privacy provisions in the Contract(s) to the US Department of Commerce, the Federal Trade Commission, European data protection authority, or any other US or EU judicial or regulatory body upon their request.
5. **Alternative Transfer Mechanism.** To the extent that PubMatic adopts a data export mechanism not described in this DPA (including any new version of or successor to the Standard Contractual Clauses pursuant to applicable European Data Protection Law) for the transfer of Data ("**Alternative Transfer Mechanism**"), such Alternative Transfer Mechanism shall apply instead of any mechanism described in this DPA. Notwithstanding anything to the contrary, an Alternative Transfer Mechanism shall only apply to the extent that it complies with Applicable Privacy Law applicable to the country where the processing activities take place. Supplier agrees to execute any document and take any appropriate action as reasonably necessary to give effect to such Alternative Transfer Mechanism.

9. **DELETION & RETURN**
    1. Upon PubMatic's request, or upon termination or expiry of this DPA, Supplier shall destroy or return to PubMatic all Personal Data (including copies) in its possession or control (including any Personal Data processed by its Sub-processors). This requirement shall not apply to the extent that Supplier is required by any applicable law to retain some or all of the Personal Data, in which event Supplier shall isolate and protect the Personal Data from any further processing except to the extent required by such law.
10. **LIABILITY**
    1. Notwithstanding anything else to the contrary in the Contract(s), Supplier acknowledges and agrees that:
        1. (a) it shall be liable for any loss of PubMatic Data (including Personal Data) and Business Contact Data arising under or in connection with the Contract(s) and this DPA to the extent such loss results from any failure of Supplier (or its Sub-processors) to comply with its obligations under this DPA and/or Applicable Privacy Laws; and
        2. (b) any exclusion of damages or limitation of liability that may apply to limit the Supplier's liability in the Contract(s) shall not apply to the Supplier's liability arising under or in connection with this DPA, howsoever caused, regardless of how such amounts or sanctions awarded are characterized and regardless of the theory of liability, which liability shall be expressly excluded from any agreed exclusion of damages or limitation of liability.
    2. The parties acknowledge and agree that any breach by Supplier of this DPA shall constitute a material breach of the Contract(s), in which event and without prejudice to any other right or remedy available to it, PubMatic may elect to immediately terminate the Contract(s) in accordance with the termination provisions in the Contract(s).

Annex I

Data Processing Description

1. **i) LIST OF PARTIES**

Data exporter(s):

Name:	PubMatic, Inc.
Address:	See Agreement
Contact person's name, position and contact details:	See Agreement
Activities relevant to the data transferred under these Clauses:	Receipt of services offered by Supplier.
Signature and date:	See signature and date of Agreement

Data importer(s):

Name:	Supplier (as defined in the Agreement)
Address:	See Agreement
Contact person's name, position and contact details:	See Agreement
Activities relevant to the data transferred under these Clauses:	Receipt of services offered by Supplier.
Signature and date:	See signature and date of Agreement

iii) DESCRIPTION OF PROCESSING / TRANSFER

Part (a) – Applicable to EU SCCs Modules 2 and 3 (controller/processor to processor transfers)

PubMatic as controller or processor

Supplier as processor

Categories of data subjects whose personal data is transferred:	May include but not limited to: PubMatic employees, customers, and prospective customers
Categories of personal data transferred:	May include but not limited to: Contact details (name, email, telephone, address) and professional details (role)
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	N/A. However, PubMatic may submit special categories of data to the Services, the extent of which is determined and controlled by the PubMatic in its sole discretion and the Supplier shall ensure compliance with security measures
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	On a continuous basis for the duration of the agreement unless otherwise agreed in writing
Nature of the processing:	For the performance of the Services in the Agreement
Purpose(s) of the data transfer and further processing:	May include but not limited to: purpose necessary to perform the Services or as may be instructed by PubMatic
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	For the duration of the Agreement, unless otherwise agreed upon in writing.

Part (b) – Applicable to EU SCCs Module 1 (controller to controller transfers) – Business Contact Data

PubMatic as controller

Supplier as controller

Categories of data subjects whose personal data is transferred:	PubMatic employees and representatives
Categories of personal data transferred:	Business contact information (email addresses, telephone numbers, addresses)
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	N/A
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous
Nature of the processing:	Storage and use for the purposes listed below.
Purpose(s) of the data transfer and further processing:	(i) Invoicing, billing and other business inquiries, (ii) information on usage of the Services, and (iii) contract management.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	Duration of the Agreement.

iii) COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority will be (i) for Personal Data protected by the GDPR, determined in accordance with Clause 13 of the Standard Contractual Clauses; (ii) for Personal Data protected by the Swiss DPA, the Federal Data Protection and Information Commissioner

("FDPIC"); and (iii) for Personal Data protection by UK Privacy Law, the Information Commissioners Office (the "ICO").

Annex II

Technical and Organisational Measures

The technical and organisational measures implemented by the processor/data importer (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Measure	**Description**
Measures of pseudonymisation and encryption of personal data	Supplier shall: • practice stronger security measures including implementation of privacy-by-design into the secure SDLC process to prevent personal data from being directly linkable to the data subject. • have management and organizational controls in place to prohibit internal teams, any relevant partners, and sub-processors, from re-identifying data processing in connection with the Agreement. • If acting as a pseudonymisation entity on behalf of the controller, Supplier agrees to apply pseudonymisation onto all data values in such a way that the attacks like brute force and dictionary attacks become infeasible. • have an approved written data pseudonymisation & encryption policy which is reviewed at least annually • use Industry-standard cryptographic techniques that are immediately applied to personal data, including but not limited to, hashing with key or salt, encryption, tokenization, as well as other relevant approaches to ensure data cannot be reidentified by unauthorised parties.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Supplier shall keep Data strictly confidential and represent that it has implemented adequate physical, technical, and organizational measures, which are reasonable based upon the sensitivity of the Data and/or necessary to secure the Personal Data and to prevent unauthorized access, disclosure, alteration, or loss of the same considering relevant risks presented by the processing. Such measures shall include, but shall not be limited to: • Preventing access by unauthorized persons to processing facilities and systems, where Data is processed or used (physical access control). • Preventing unauthorized use of processing systems (admission control).

	• Ensuring that those persons authorized to use a processing system are only able to access Data within the scope of their access rights, and that Data cannot be read, copied, modified or deleted without authorization during processing or use and after recording (virtual access control). • Ensuring that, during electronic transfer, transportation or when being saved to data carriers, Data cannot be read, copied, modified or deleted without authorization, and that it is possible to check and establish to which bodies the transfer of Data by means of data transmission facilities is envisaged (transmission control). • Ensuring that it is possible to check and ascertain whether and by whom Data has been accessed, modified, or deleted from processing systems (input control), and ensuring that such access, modification, and deletion of Data is, in fact, monitored for any unusual or suspicious activities. • Ensuring that Data processed under these terms can only be processed in accordance with the instructions issued by PubMatic (assignment control). • Ensuring that Data is protected against accidental malfunctions or loss (availability control). • Ensuring that Data collected for different purposes can be processed separately (separation control). • Maintaining a process for regularly testing, assessing, and evaluating the effectiveness of physical, technical, and organizational measures to ensure the security of the processing. • Ensuring that Supplier has developed and implemented appropriate privacy and data protection policies and procedures, and that all personnel who are involved in processing the Data have been appropriately trained to process the Personal Data in accordance with such policies and procedures as well as in accordance with these terms and Applicable Privacy Law • Practice data categorization and manage assets in accordance with the privacy requirements based on the personal data residing on them. • Access control lists & file permissions and are monitored and updated regularly. • Employees are trained about privacy considerations both at a generic org-wide level and as per the nature of their role. • review all data processing, transfer, and storage mechanisms. • Version control, data logs, granular access control, and checksums are implemented to ensure integrity is enforced. • At least once annually, relevant security measures to the processing of personal data are reviewed and tested for alignment with industry good practices.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of	Supplier shall: • implement measures for preventive measures such as redundancy, failover, and Redundant Array of Independent Disks (RAID) into system design. • perform Security audits routine including updating systems, networks, and applications

a physical or technical incident	• utilize detection tools such as network/server monitoring software and anti-virus solutions • do regular backups, review & test business continuity readiness plans and disaster recovery plans. • have a Data Recovery and Business Continuity plan with detailed corrective measures in the event of data loss, including timely communication with customers • At least once annually, Security measures relevant to the processing of personal data are reviewed and tested for alignment with industry good practices.
Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Supplier shall: • have policies in areas such as remote access, asset management and password controls including data privacy policy that talks in detail about data privacy measures implemented by Supplier. • have a Business Continuity Plan & Measures for protecting personal data as a part of disaster recovery program. How is data secured, accessed, recovered, and maintained. • assess high-risk data and processing activities and develop mitigating solutions to prevent or reduce risks. • perform a Data Protection Impact Assessment. • ensure that Supplier have effective and compliant data protection policies and procedures in place. These should be readily available to employees as a form of guidance and support. Supplier document your obligations, objectives, and controls in accordance with the regulatory guidelines • Supplier do regular reporting which includes data protection risks, mitigating measures and requirements needed for effective technical and organisational measures. • ensure that employees, contractors, and visitors understand what your data protection obligations are and help to maintain compliance. • have all the policies, controls, and measures in place including audit your policies to ensure those policies and controls remain fit for purpose, perform a self-assessment on a regular basis to review the key compliance areas and identify any gaps before they become a breach. • ensure that your business relationships also comply with the regulatory guidelines and the law as much as you are, Supplier conduct employees background screening, and put extensive security and data protection measures into place.
Measures for user identification and authorisation	Supplier shall ensure that: • Users are identified as being in a role that stipulates what privileges they have. Additionally, their user respective user id's which would restrict what data they have access to.

	• Access control lists are specified mentioning which users have access to what resource and how access to those resources is controlled. Operational and technical controls are in place to ensure that access to systems that process personal data is only granted to authorized users with a “need to know • it has defined and implemented a policy which controls measures like messages encryption by • electronic signature, • access • obligatory encryption of the traffic among system nodes, • safe approach to important remote data using technologies like 2FA & VPN data • risk prevention and reduction of unauthorised intrusions into computer systems • technical measures are well co-ordinated, planned, managed, implemented, and are included in business processes. Incoming message filtration: • control of all communications from / towards internet / intranet – permission to establish communication granted only to particular computers; • hiding of the complete intranet by using concepts of Network Address Translation, Virtual IP address etc. so the outgoing messages are given different addresses.
Measures for the protection of data during transmission	Supplier shall: • Implement robust network security controls to help protect data in transit. • make use of Network security solutions like firewalls and network access control to secure the networks used to transmit data against malware attacks or intrusions. • use proactive security measures that identify at-risk data and implement effective data protection for data in transit and at rest. • use solutions which are in line with your policies that enable user prompting, blocking, or automatic encryption for sensitive data in transit. • have policies for systematically categorizing and classifying all company data, no matter where it resides, to ensure that the appropriate data protection measures are applied
Measures for the protection of data during storage	Supplier shall: • have written policies specifying the appropriate levels of security for the diverse types of data that it has. including security models, procedures, and tools in place to apply appropriate protections. Supplier policies to also include details on the security measures that are deployed on the storage devices used in your environment • have implemented Role-based access control to access & secure data storage system including use of multi-factor authentication mechanism to access the data, change default passwords on their storage devices and enforce the use of strong passwords as per the guidelines defined in your password complexity requirements policy. • have deployed a solution which gives Supplier data loss prevention (DLP) capabilities to find and stop any attacks in progress.

- practice usage of strong network security systems, such as firewalls, anti-malware protection, security gateways, intrusion detection systems to defend against cyberattacks and malicious actors from ever gaining access to the storage devices.
- have appropriate security measures in place on the systems that will be used to access stored data.
- have redundant storages, which will ensure availability and performance of the stored data while its being accessed.
- have a defined SPOC / Team who need to make sure that the backup systems and processes are adequately running. Also, the backup systems have the same level of data security in place as primary systems.

Measures for ensuring physical security of locations at which personal data are processed	Supplier shall: • ensure access to IT, server rooms, systems containing personal data is restricted. • use highly secured access credentials that are difficult to clone, fully trackable, and unique to each individual. • Multi-factor authentication (MFA) is enabled to unlock a door or access the building containing systems holding personal data. • structure permissions to employ least-privilege access throughout the physical infrastructure • have set up automated security alerts to monitor and identify suspicious activity in real-time as a part of physical security • have installed perimeter security to prevent intrusion. Physical barriers like fencing and landscaping help establish private property and deter people from entering the premises. • use access control systems to provide the next layer of security and keep unwanted people out of the building. • Integrate Supplier access control with other physical security systems like video surveillance and user management platforms to fortify your security. • employ cyber and physical security convergence for more efficient security management and operations. • regularly test your physical security measures to ensure you are protected against the newest physical security threats. • Ensure changes in the physical systems are always communicated with the respective stakeholders.
Measures for ensuring events logging	**Supplier shall:** • have a defined Audit & logging Policy which covers what types of security events you want to be recorded in the security event logs of your servers and workstations • have a central logging system for complete monitoring, analysis, and reporting

	• have an Event monitoring- Real-time alerts & notification solution in place which allows at a minimum, to traceable back the events at their origination point. • do not log personal data as a part of logging capabilities to avoid risk of a data breach. • perform code reviews as a standard engineering best practice. As part of this process, pay attention to log statements and call out any potentially problematic logs. • verify that no personal data is being logged. • train your employees about the risk of logging sensitive information. • logs are relational data sets, like key/value pairs, rather than just text. So that they can be better searched and analysed
Measures for ensuring system configuration, including default configuration	Supplier shall ensure: • that critical or material security updates/patches will be installed according to the Supplier's internal Patch Management Policy a. in client operating systems; b. in server operating systems reachable via public networks (e.g., webservers); c. in application programs (incl. browser, plugins, PDF-reader, etc.); d. in security infrastructure (virus scanner, firewalls, IDS-systems, content filters, routers, and so forth.); and e. in server operating systems of internal servers. • Reasonable measures are used for the protection of end-devices, servers, and other infrastructure elements against unauthorized access (such as multi-level virus protection concept, content filters, application firewall, intrusion detection systems, desktop firewalls, system hardening, content encryption). • The Supplier has implemented the following sharing control measures insofar as Personal Data will be received, transferred, or transported by the Supplier: • Reasonable measures for securing network infrastructure (e.g., intrusion detection systems, use of 2-factor authentication for remote access, separation of networks, encrypted network protocols, and so forth.) • Encryption – Supplier implements encryption technology which commensurate with the state-of-the-art to be prescribed so that Personal Data will be incapable of being read, copied, changed, or removed during electronic transmission or during transport for storage on data carriers, such as RSA 2048. Data carrier encryption with – state of the art – algorithms and protocols to be classified as secure (e.g., TLS based protocols) for the protection of mobile devices (notebooks, tablet PCs, smartphones, etc.) and data carriers (external hard drives, USB sticks, memory cards, and so forth). • Implementation of technical security measures for export and import interfaces (hardware and application related).
Measures for internal IT and IT security governance and management	Supplier shall ensure: • IT risk assessment about the IT system processing and operational environment, threats, vulnerabilities, impact, and controls, enables

identification of the control objectives and activities to be tested for design and implementation effectiveness and its operating effectiveness

Supplier shall ensure that:

- Access shall be limited to the minimum necessary to perform the assigned duties (principle of least privilege).
- Access to devices must be authenticated
- Anti-malware software and definitions are updated automatically.
- Its IT team shall examine the device believed to contain or to have contained, corporate data where necessary for investigatory or control purposes on a regular basis.
- Team members shall be positively identified, authorized, and authenticated before they are granted access to company information resources.
- Reviews of non-administrative and administrative user access rights shall be performed at least annually.
- Change authorizations are done by the IT and Security Teams along with the CAB board.
- review all the changes following the implementation of the change into the production environment.
- employees are trained and educated on internet browsing and email best practices to help protect against malware, phishing, and ransomware.

Measures for certification/assurance of processes and products

- The IT and Operations teams are responsible for implementing anti-malware capabilities. They establish a patch management process for systems they support and a procedure to remain aware of new vulnerabilities. These teams are also responsible for ensuring the following take place:
- Different flavours of O.S systems used in the environment, including Linux systems have approved anti-malware software installed and operating which is centrally administered by IT Team. Anti-malware software is configured to scan all files before being accessed and/or written to disk.
- IT and Operations teams are responsible for the administration & management of IT networks for the purposes of security and availability. All remote network-level access and administration are restricted by firewall authentication.
- IT Systems including the components which comprise them, shall be managed and controlled to limit threats and vulnerabilities.
- IT Systems controls shall ensure the protection and security of the information processing services and applications
- The IT teams shall ensure that IT systems are segregated (using authentication, physical and logical access restrictions) from each other using network ACLS, firewalls, VPNs, security groups, etc. They establish specific segments for each office location, guest wireless, team member wireless, development/test, stage, and production environments.
- As a part of IT security governance, implement and enforce a system of effective internal controls and procedures

Measures for ensuring data minimisation	Supplier shall: • Ensure that personal data is adequate, relevant, and not excessive for the purpose; · Limit categories of personal data chosen for processing to a data collection that is directly relevant for the originally specified purposes; • Consider and make use, if feasible, of special privacy enhancing technologies that allow for avoiding excessive use of personal data or enabling the use of anonymised data. Any further processing should require customer consent unless there is a legal basis.
Measures for ensuring data quality	Supplier shall: • ensure Data quality by meeting ensuring the completeness, accuracy and timeliness, validity & uniqueness of the personal data. • have comprehensive data quality controls to resolve all data inaccuracies around personal data. • agree to take inventory of inconsistencies, errors, duplicates, and recording and correct any problems Supplier come across to make sure the data that goes into your infrastructure is as high-quality as it can be. • review & audit certain datasets as part of the data quality • identify personal data locations and assign responsibility for each dataset to ensure its quality. • track data quality scores, categorize sensitive information, monitor data's location, establish access rights, and enact usage restrictions.
Measures for ensuring limited data retention	Supplier shall: • agree not to retain personal data for longer than is necessary for the purpose for which it is processed. • ensure that records must not be retained beyond the period indicated in the Records Retention Schedule unless the record is identified as information subject to a litigation hold or other valid business reason. • Ensure that the Personal Data are capable of being deleted at any time upon request of the PubMatic. • Implement processes, tools, and documentation for secure deletion in a manner, such that recovery of the data is not possible • Provide its employees with specifications regarding how and when data are to be deleted.
Measures for ensuring accountability	Supplier shall: • have internal policies containing formal instructions for data processing procedures; Contractors are being carefully vetted regarding data security; The Supplier personnel are trained periodically to maintain awareness regarding data protection and security requirements.

	• maintain relevant documentation and adopt additional measures as necessary as a part of data accountability • put in place internal mechanisms and control systems that ensure compliance and provide evidence – such as audit reports – to demonstrate compliance to external stakeholders, including supervisory authorities • be responsible for its compliance as per the regulatory guidelines and must be able to demonstrate that compliance. • maintain documentation for all its data sharing operations. • implement a "data protection by design and default" approach, putting in appropriate technical and organisational measures to implement data protection principles and safeguard individual rights. • ensure that staff in its organisation who are likely to make decisions about sharing data have received the right training to do so appropriately.
Measures for allowing data portability and ensuring erasure	If a data subject seeks to object to the processing of, or seeks to access, rectify, erase, restrict or block Personal Data pertaining to him or her, or exercise any rights regarding automated decision-making, withdrawal of consent, profiling or portability, Supplier shall co-operate and promptly inform PubMatic DPO at dpo@pubmatic.com to take the actions required under the Applicable Privacy Law in accordance with PubMatic's instructions.