DATA PROCESSING AGREEMENT

[Last Updated: July 12, 2023]

This Data Processing Agreement ("**DPA**") forms an integral part of the publisher agreement executed by and between FireArc Technologies Ltd. and its affiliates ("**Company**") and the Publisher ("**Agreement**"). Capitalized terms used herein but not defined herein shall have the meanings ascribed to them in the Agreement.

WHEREAS, the Company is the developer and owner of the technology and platform that enables the Publisher to place interactive units and ads within the Publisher's online digital assets, apps, websites, etc. ("**Publisher Assets**");

WHEREAS, subject to the terms of the Agreement, the Company shall provide the Publisher with the Services, during the use of the Company Services, the Company will process certain Personal Data (as such terms are defined below) on the Publisher's, behalf subject to the terms and conditions of this DPA; and

WHEREAS, the Parties desire to supplement this DPA to achieve compliance with the UK, EU, Swiss, United States and other data protection laws and agree on the following:

1. DEFINITIONS

1.1 "**Adequate Country**" is a country that an adequacy decision from the European Commission.

1.2 "**CCPA**" means the California Consumer Privacy Act (Cal. Civ. Code §§ 1798.100 - 1798.199) of 2018, including as modified by the California Privacy Rights Act ("**CPRA**") once the CPRA takes effect as well as all regulations promulgated thereunder from time to time.

1.3 "**Controller**", "**Processor**", "**Data Subject**", "**Personal Data**", "**Processing**" (and "**Process**"), "**Personal Data Breach**" and "**Special Categories of Personal Data**" shall all have the meanings given to them in EU Data Protection Law. The terms "**Business**", "**Business Purpose**", "**Consumer**", "**Cross Context Behavioral Advertising**", **"First-Party Business",** "**Service Provider**", "**Share**", "**Sale**", "**Third-Party Business**" and "**Sell**" shall have the same meanings as ascribed to them in the CCPA. "**Data Subject**" shall also mean and refer to a "**Consumer**". "**Personal Data**" shall also mean and refer to "**Personal Information**," as such term is defined in the CCPA.

1.4 "**Consent**" means an End User informed and freely given consent that meets the requirements stipulated under Article 7 of the GDPR.

1.5 "**CPA**" means the Colorado Privacy Act C.R.S.A. § 6-1-1301 et seq. (SB 21-190), including any implementing regulations and amendments.

1.6 "**CTDPA**" means the Connecticut Data Privacy Act, S.B. 6 (Connecticut 2022), including any implementing regulations and amendments thereto

1.7 "**Data Protection Law**" means applicable privacy and data protection laws and regulations (including, where applicable, EU Data Protection Law, UK Data Protection Laws, Swiss Data Protection Laws, Israeli Law and the US Data Protection Laws and the Brazilian General Data Protection Law "**LGPD**") as may be amended or superseded from time to time.

1.8 "**EEA**" means the European Economic Area.

1.9 "**End User**" means an individual visiting or browsing the Publisher Assets which interacts with the Interactive Units and Ads displayed therein.

1.10 "**EU Data Protection Law**" means the (i) EU General Data Protection Regulation (Regulation 2016/679) ("**GDPR**"); (ii) Regulation 2018/1725; (iii) the EU e-Privacy Directive (Directive 2002/58/EC), as amended (**e-Privacy Law**); (iv) any national data protection laws made under, pursuant to, replacing or succeeding (i) – (iii); and (iv) any legislation replacing or updating any of the foregoing.

1.11 "**ID**" means (i) a unique identifier stored on an End-User's device; (ii) a unique identifier generated for a specific End User; (iii) an online identifier associated with a particular device; (iii) a cookie ID, agent ID, IP address, URL or RTB tag, or any online identifier identifying an End User or a specific device; (iv) a unique identifier identifying the Publisher and the Publisher Assets.

1.12 "**Israeli Law**" means Israeli Privacy Protection Law, 5741-1981, the regulations promulgated pursuant thereto, including the Israeli Privacy Protection Regulations (Data Security), 5777-2017 and other related privacy regulations.

1.13 "**Publisher Data**" means any and all Personal Data shared or otherwise processed by Company on Publisher's behalf, as detailed in **ANNEX I.**

1.14 "**Security Incident**" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data of the other party. For the avoidance of doubt, any Personal Data Breach of the other party's Personal Data will comprise a Security Incident.

1.15 "**Signal**" shall mean End Users' preference as provided by the Publishers' cookie manager, if and to the extent applicable.

1.16 "**Standard Contractual Clauses"** mean the standard contractual clauses for the transfer of Personal Data to third countries pursuant to the GDPR and adopted by the European Commission **Decision 2021/914** of 4 June 2021 which is attached herein by link reference: https://eur-ex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN.

1.17 "**Swiss Data Protection Laws**" or **"FADP"** shall mean the Swiss Federal Act on Data Protection of June 19, 1992, SR 235.1, and any other applicable data protection or privacy laws of the Swiss Confederation as amended, revised, consolidated, re-enacted or replaced from time to time, and to the extent applicable to the processing of Personal Data under the Agreement.

1.18 "**Swiss SCC"** shall mean the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner

1.19 "**UK Data Protection Laws**" shall mean the Data Protection Act 2018 (DPA 2018), as amended, and EU General Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as incorporated into UK law as the UK GDPR, as amended, and any other applicable UK data protection laws, or regulatory Codes of Conduct or other guidance that may be issued from time to time.

1.20 **"UK GDPR"** shall mean the GDPR as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom or a part of the United Kingdom from time to time.

1.21 "**UK SCC**" means the UK 'International data transfer addendum to the European Commission's standard contractual clauses for international data transfers', available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, as adopted, amended or updated by the UK's Information Commissioner's Office, Parliament or Secretary of State.

1.22 "**US Data Protection Laws**" means any U.S. federal and state privacy laws effective as of the Effective Date of this DPA and applies to Company Processing of Publisher Data, and any implementing regulations and amendment thereto, including without limitation, the CCPA, the CPA, the CTDPA, and the VCDPA.

1.23 "**VCDPA**" means the Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-575 et seq. (SB 1392), including any implementing regulations and amendments thereto.

Any other terms that are not defined herein shall have the meaning provided under the Agreement or applicable Law. A reference to any term or section of US Data Protection Laws, UK Data Protection Laws or GDPR means the version as amended. Any references to the GDPR in this DPA shall mean the GDPR and/or UK GDPR depending on the applicable Law.

2. RELATIONSHIP OF THE PARTIES

2.1 The parties acknowledge that in relation to all Publisher Data, as between the parties, Publisher is the Controller of Publisher Data, and the Company, in the course of providing the Services, is acting as a Processor on behalf of the Publisher.

2.2 The purpose, subject matter and duration of the Processing carried out by the Company on behalf of the Publisher, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects are described in **ANNEX I** attached hereto.

2.3 US Data Protection Laws specification are further detailed in **Annex VII**.

3. REPRESENTATIONS AND WARRANTIES

3.1 The Publisher represents and warrants that: (i) its Processing instructions shall comply with applicable Data Protection Law; and (ii) it will comply with Data Protection Law, specifically with regards to the lawful basis principal for Processing Personal Data.

3.2 Publisher acknowledges and agrees that the End User does not have a direct relationship with the Company, however, certain features of the Company's Services are dependent and based upon End User's Consent or any other demonstrated lawful basis, that shall be obtained by Publisher and which the Company relies on. Publisher also acknowledges that it shall be able to demonstrate such Consent at any time and represents that such Consent

exists. The Company shall not be liable for obtaining Consent or with respect to the Signals, if applicable, provided by the Publisher or the Publisher's consent management, and shall transfer the Signal "as is" and as it was provided to the Advertiser partner. Publisher acknowledges and agrees that such requests are directly transmitted to the Advertiser, and such Advertiser will respond as per Publisher's request. Therefore, the Company, as the technical provider, has no control over such parameters or over the Signal and shall not be responsible for any parameter or Signal that was unlawfully or misleadingly sent by Publisher, nor liable for any damage or damages resulting by it.

3.3 The Publisher shall, or obligate Publisher's consent management platform (CMP) to, (i) provide users with link(s) to the Company's privacy documentation; (ii) disclose in the initial layer of the user interface the number of third party vendors that are seeking consent or pursuing data processing purposes on the basis of their legitimate interest(s); (iii) Ensure that users can re-access the CMP user interface easily to manage their privacy choices. If requested by Company, the Publisher shall provide the Company with applicable evidence of the CMP compliance with this section.

3.4 <u>The Company's Representation and Warranties</u>:

3.3.1. The Company represents and warrants that it: (i) shall process Personal Data on behalf of the Publisher, all in accordance with Publisher's written instructions including the Agreement and this DPA; (ii) in the event the Company is required under applicable laws, including Data Protection Law or any union or member state regulation, to Process Personal Data other than as instructed by Publisher, it shall inform the Publisher of such requirement prior to Processing such Personal Data, unless prohibited under applicable law; and (iii) shall provide reasonable cooperation and assistance to Publisher in ensuring compliance with its obligation to carry out data protection impact assessments with respect to the processing of Personal Data and to consult with the supervisory authority (as applicable).

3.3.2. The Company shall take reasonable steps to ensure: (i) the reliability of its staff and any other person acting under its supervision who may come into contact with, or otherwise have access to and Process Personal Data; (ii) that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; and (iii) that such personnel are aware of their responsibilities under this DPA and any applicable Data Protection Laws and the Company shall enable access solely to the employees on a "need to know" basis.

4. RIGHTS OF DATA SUBJECTS AND THE PARTIES' COOPERATION OBLIGATIONS

4.1 It is agreed that where the Company receives a request from a Data Subject or an applicable authority in respect of Publisher Data processed by the Company, where relevant, it will direct the Data Subject or the applicable authority to the Publisher in order to allow the Publisher to respond directly to the Data Subject's or the applicable authority's request, unless otherwise required under applicable laws. Both parties shall provide each

other with commercially reasonable cooperation and assistance in relation to the handling of a Data Subject's or applicable authority's request, to the extent permitted under Data Protection Law.

4.2 Where applicable, the Company shall assist the Publisher in ensuring that Personal Data processed is accurate and up to date, by informing the Publisher without delay if it becomes aware of the fact that the Personal Data it is processing is inaccurate or has become outdated.

5. SUB-PROCESSOR

5.1 The Publisher acknowledges that the Company may transfer Personal Data to and otherwise interact with third party data processors ("**Sub-Processor**"). The Publisher hereby, authorizes the Company to engage and appoint such Sub-Processorsto Process Personal Data, as well as permits each Sub-Processor to appoint a Sub-Processor on its behalf. the Company may continue to use those Sub-Processors already engaged by it, as listed in **ANNEX III**, and subject to the provision of a 30-day prior notice to the Publisher, the Company may engage an additional or replace an existing Sub-Processor to process Personal Data. In case the Publisher has not objected to the adding or replacing of a Sub-Processor in the allotted time period, such Sub-Processor shall be considered as approved by the Publisher. In the event the Publisher objects, it may, under the Company's sole discretion, suggest the engagement of a different Sub-Processor for the same course of services, or otherwise terminate the Agreement.

5.2 The Company shall, where it engages any Sub-Processor, impose, through a legally binding contract between The Company and the Sub-Processor, data protection obligations no less onerous than those set out in this DPA on the Sub-Processor ("**Contract**"). The Company shall ensure that the Contract will require the Sub-Processor to provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of Data Protection Law.

5.3 The Company shall remain fully responsible to the Publisher for the performance of the Sub-Processor's obligations in accordance with the Agreement. The Company shall notify the Publisher of any failure by the Sub-Processor to fulfil its contractual obligations.

6. TECHNICAL AND ORGANIZATIONAL MEASURES

6.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, and without prejudice to any other security standards agreed upon by the parties, the Company shall implement appropriate physical, technical and organizational measures to protect the Publisher Data as required under Data Protection Laws to ensure lawful processing of Publisher Data and safeguard Publisher Data from unauthorized, unlawful or accidental processing, access, disclosure, loss, alteration or destruction. The parties acknowledge that security requirements are constantly changing

and that effective security requires the frequent evaluation and regular improvement of outdated security measures.

6.2 The security measures are further detailed in **ANNEX II**.

7. SECURITY INCIDENT

7.1 The Company shall notify the Publisher upon becoming aware of any confirmed Security Incident involving the Publisher's Data in the Company's possession or control, as determined by the Company in its sole discretion. The Company shall, in connection with any Security Incident affecting the Publisher Data: (i) take such steps as necessary to contain, remediate, minimize any effects of and investigate any Security Incident and to identify its cause; (ii) co-operate with the Publisher and provide the Publisher with such assistance and information as it may reasonably require in connection with the containment, investigation, remediation or mitigation of the Security Incident; (iii) notify the Publisher in writing of any request, inspection, audit or investigation by a supervisory authority or other authority; (iv) keep the Publisher informed of all material developments in connection with the Security Incident and execute a response plan to address the Security Incident; and (v) cooperate with the Publisher and assist Publisher with the Publisher's obligation to notify affected individuals in the case of a Security Incident.

7.2 The Company's notification regarding or response to a Security Incident under this Section 7 shall not be construed as an acknowledgment by the Company of any fault or liability with respect to the Security Incident.

8. AUDIT RIGHTS

8.1 The Company shall respond promptly and adequately with respect to any inquiries from the Publisher regarding the processing of Personal Data in accordance with this DPA. The Company shall make available to the Publisher all information necessary to demonstrate compliance with the obligations under the EU Data Protection Law.

8.2 The Company shall make available, solely upon prior written notice and no more than once per year (except for in the case of a Security Incident), information necessary to reasonably demonstrate compliance with this DPA to a reputable auditor nominated by the Publisher, and shall allow for audits, including inspections, by such reputable auditor solely in relation to the processing of the Publisher Data ("**Audit**") in accordance with the terms and conditions hereunder. The Audit shall be subject to the terms of this DPA and standard confidentiality obligations (including towards third parties). The Company may object to an auditor appointed by the Publisher in the event the Company reasonably believes that the auditor is not suitably qualified or independent, is a competitor of the Company or otherwise unsuitable ("**Objection Notice**"). The Publisher will appoint a different auditor or conduct the Audit itself upon its receipt of an Objection Notice from the Company. Publisher shall bear all expenses related to the Audit and shall (and ensure that each of its auditors shall) over the course of such Audit, avoid causing any damage, injury or disruption to the Company's premises, equipment, personnel and business. Any and all conclusions of such Audit shall be confidential and reported back to the Company immediately.

9. DATA TRANSFER

9.1 If the processing of Publisher Data includes a transfer (either directly or through an onward transfer) to a third country outside the EEA, the UK and Switzerland, that is not an Adequate Country, such transfer shall be subject to an appropriate safeguard approved by Data Protection Law: the GDPR (Article 46), UK GDPR (Article 46) or Swiss FADP (as applicable).

9.2 if the parties rely on the Standard Contractual Clauses to facilitate a transfer then:

9.2.1 transfer of Personal Data from the EEA the terms set forth in **Annex IV** shall apply.

9.2.2 transfer of Personal Data from the UK, the terms set forth in **Annex V** shall apply; and

9.2.3 transfer of Personal Data from Switzerland, the terms set forth in **Annex VI** shall apply.

10. CONFLICT

In the event of a conflict between the terms and conditions of this DPA and the Agreement, this DPA shall prevail. For the avoidance of doubt, in the event Standard Contractual Clauses have been executed between the parties, the terms of the Standard Contractual Clauses shall prevail over those of this DPA. Except as set forth herein, all of the terms and conditions of the Agreement shall remain in full force and effect.

11. TERM AND TERMINATION

11.1 This DPA shall be effective as of the Effective Date and shall remain in force until the Agreement terminates. The Publisher shall be entitled to suspend the Processing of its Publisher's Data in the event that the Company is in breach of Data Protection Laws, the terms of this DPA all in accordance with a binding decision of a competent court or the competent supervisory authority.

11.2 The Company shall be entitled to terminate this DPA or terminate the Processing of Publisher Data in the event that Processing of Personal Data under the Publisher's instructions or this DPA infringe applicable legal requirements. Such termination shall be subject to informing the Publisher and the Publisher insists on compliance with the instructions.

11.3 Following the termination of this DPA, the Company shall, at the choice of the Publisher, delete all Publisher's Personal Data processed on behalf of the Publisher and certify to the Publisher that it has done so, or otherwise, return all Publisher's Data to the Publisher and delete existing copies unless applicable law or regulatory requirements requires that the Company continue to store the Publisher's Personal Data. Until the Personal Data is deleted or returned, the Company shall continue to ensure compliance with this DPA.

ANNEX I
DETAILS OF PROCESSING

This Annex I include certain details of the processing of the Publisher Data as required by Article 28(3) GDPR.

Categories of Data Subjects:

Publishers' End Users / Data Subject that viewed ads or content which are placed on the Publisher's digital assets, meaning the End Users interacting with the Publisher's app, site, game, etc. and the ads displayed by The Company.

Categories of Personal Data:

IP addresses, IDFA/ AAID or any IDs, Consent logs, cookies data, usage data, approximate location data, behavior data, referred URL, Publisher-uploaded segment data, End User behavior data- meaning, clicked the ad, viewed the ad, which is processed for reporting purposes for Publisher, impression data, optimization data, ad delivery data.

Special Categories of Personal Data:

Not Applicable

Process Frequency:

The Personal Data is transferred on a continuous basis.

Nature of the processing:

Collection, storage, organization, analysis, modification, retrieval, disclosure, communication and other uses in performance of the Services as set out in the Agreement.

Retention Period:

For as long as needed to provide the Service, comply with applicable laws or otherwise requested by the Controller. The logs tracing the event is stored between 7 to 30 days for fraud prevention purposes.

ANNEX II
TECHNICAL AND ORGANISATIONSL MEASURES

Below is a summary of the security measures the Company adheres to:

1. Implement and maintain current and appropriate technical and organizational measures to protect Publisher Data against accidental, unauthorized or unlawful Processing and against accidental loss, destruction, damage, alteration, disclosure or access;
2. Provide third-party attestation of static or dynamic application security testing or penetration testing on all software processing Publisher Data, remediate any identified high vulnerabilities prior to delivery to Publisher, provide written remediation plans for medium and low vulnerabilities, and provide evidence of its remediation of any identified security vulnerabilities at Publisher's request;
3. Maintain a level of security appropriate to the harm that may result from any unauthorized or unlawful Processing or accidental loss, destruction, damage, denial of service, alteration or disclosure, and appropriate to the nature of Publisher Data;
4. Oblige its employees, agents or other persons to whom it provides access to Publisher Data to keep it confidential; take reasonable steps to ensure the integrity of any employees who have access to Publisher Data; provide annual training to staff and subcontractors on the security requirements contained herein;
5. Maintain measures designed to ensure the ongoing confidentiality, integrity, availability and resilience of the Company's systems and services;
6. Maintain a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing of Publisher Data, regularly testing such measures to validate their appropriateness and effectiveness, and implementing corrective action where deficiencies are revealed by such testing;
7. Log all individuals' access to and activities on systems and at facilities containing Company Data. Upon Publisher's request, and subject to applicable laws and the Company retention policy, the Company will provide a report detailing a list of authorized users, their associated privileges, status of accounts, and history of activities;
8. For passwords applicable to the Company's access, adhere to password policies for standard and privileged accounts consistent with industry best practices; protect both the Company's and Publisher's user account with access to Publisher Data using multi-factor authentication (e.g., using at least two different factors to authenticate such as a password and a security token or certificate);
9. Store and transmit Publisher Data using strong cryptography, consistent with industry best practices, and pseudonymize Personal Data where appropriate;
10. Ensure that only those the Company's personnel who need to have access to Publisher Data are granted access, such access is limited to the least amount required, and only granted for the purposes of performing obligations under this DPA. The Company shall conduct access reviews upon each individual's scope of responsibility change, the Company staffing change or other change impacting the Company's personnel access to Publisher Data;

11. Maintain a physical security program that is consistent with industry best practices;
12. Ensure that any storage media (whether magnetic, optical, non-volatile solid state, paper, or otherwise capable of retaining information) that captures Publisher Data is securely erased or destroyed before repurposing or disposal;

Additional Safeguards

Measures and assurances regarding US government surveillance ("**Additional Safeguards**"):

The Company agrees and hereby represents it maintains, and will continue to maintain, the following additional safeguards in connection with any Personal Data transferred under this Annex:

a) The Company maintains industry standard measures to protect the Personal Data from interception (including in transit from Publisher to the Company and between different systems and services). This includes maintaining encryption of Personal Data in transit and at rest.

b) In the event that section 702 of the United States Foreign Intelligence Surveillance Court ("**FISA**") applies the Company, the Company will make reasonable efforts to resist, subject to applicable laws, any request for bulk surveillance relating to the Personal Data protected under the GDPR or the UK GDPR, including (if applicable) under Section 702 of the FISA.

c) If the Company becomes aware of any law enforcement agency or other governmental authority ("**Authority**") attempt or demand to gain access to or a copy of the Personal Data (or part thereof), whether on a voluntary or a mandatory basis, then, unless legally prohibited or under a mandatory legal compulsion that requires otherwise, the Company shall: inform the relevant Authority that the Company is a Processor of the Personal Data and that Publisher, as the Controller has not authorized the Company to disclose the Personal Data to the Authority; inform the relevant Authority that any and all requests or demands for access to the Personal Data should be directed to or served upon Publisher in writing; and use reasonable legal mechanisms to challenge any such demand for access to Personal Data which is under the Company's control.

d) Notwithstanding the above, if, taking into account the nature, scope, context and purposes of the related Authority's intended access to Personal Data, the Company has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual or entity, these subsections shall not apply. In such event, the Company shall notify Publisher, as soon as possible, following the access by the Authority, and provide Publisher with relevant details, unless and to the extent legally prohibited to do so.

The Company will inform Publisher, upon written request (and not more than once a year), of the types of binding legal demands for Personal Data the Company has received and complied with, including demands under national security orders and directives, specifically including any process under Section 702 of FISA.

ANNEX III

LIST OF SUB-PROCESSORS

Name	Address	Description of the processing	DPA/SCC
AWS	EU & US	Hosting, storing	https://aws.amazon.com/blogs/security/aws-gdpr-data-processing-addendum/

ANNEX IV

EU INTERNATIONAL TRANSFERS AND SCC

1. The parties agree that the terms of the Standard Contractual Clauses are hereby incorporated by reference and shall apply to transfer of Personal Data from the EEA to other countries that are not deemed as Adequate Countries.
2. Module Two (Controller to Processor) of the Standard Contractual Clausesshall apply where the transfer is effectuated by Publisher as the data controller of the Personal Data and The Company is the data processor of the Personal Data.
3. The Parties agree that for the purpose of transfer of Personal Data between Publisher (as Data Exporter) and the Company (as Data Importer), the following shall apply:
   a) Clause 7 of the Standard Contractual Clauses shall not be applicable.
   b) In Clause 9, option 2 (general written authorization) shall apply and the method for appointing and time period for prior notice of Sub-processor changes shall be as set forth in the Sub-Processing Section of the DPA.
   c) In Clause 11, the optional language will not apply, and data subjects shall not be able to lodge a complaint with an independent dispute resolution body.
   d) In Clause 17, option 1 shall apply. The parties agree that the Standard Contractual Clauses shall be governed by the laws of the EU Member State in which the Publisher is established (where applicable).
   e) In Clause 18(b) the parties choose the courts of the Republic of Ireland, as their choice of forum and jurisdiction.
4. **Annex I.A** of the Standard Contractual Clauses shall be completed as follows:
   1.a.1."**Data Exporter**": Publisher
   1.a.2."**Data Importer**": The Company
   1.a.3.Roles: (A) With respect to Module Two: (i) Data Exporter is a data controller and (ii) the Data Importer is a data processor.
   1.a.4.Data Exporter and Data Importer Contact details: As detailed in the Agreement.
   1.a.5.Signature and Date: By entering into the Agreement and DPA, Data Exporter and Data Importer are deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.
5. **Annex I.B** of the Standard Contractual Clauses shall be completed as follows:
   a) The purpose of the processing, nature of the processing, categories of data subjects, categories of personal data and the parties' intention with respect to the transfer of special categories are as described in **Annex I** (Details of Processing) of this DPA.
   b) The frequency of the transfer and the retention period of the personal data is as described in **Annex I** (Details of Processing) of this DPA.
   c) The sub-processor which personal data is transferred are listed in **Annex III**.

6. **Annex I.C** of the Standard Contractual Clauses shall be completed as follows: the competent supervisory authority in accordance with Clause 13 is the supervisory authority in the Member State stipulated in Section 3 above.

7. **Annex II** of this DPA (Technical and Organizational Measures) serves as **Annex II** of the Standard Contractual Clauses.

8. **Annex III** of this DPA (List of Sub-processors) serves as **Annex III** of the Standard Contractual Clauses.

9. **Transfers to the US:** Measures and assurances regarding US government surveillance ("**Additional Safeguards**") are further detailed in **Annex II,** as well as:

   The Company agrees and hereby represents it maintains, and will continue to maintain, the following additional safeguards in connection with any Personal Data transferred under this **Annex IV**:

   a. The Company maintains industry standard measures to protect the Personal Data from interception (including in transit from Publisher to The Company and between different systems and services). This includes maintaining encryption of Personal Data in transit and at rest.

   b. The Company will make reasonable efforts to resist, subject to applicable laws, any request for bulk surveillance relating to the Personal Data protected under the GDPR or the UK GDPR, including (if applicable) under section 702 of the United States Foreign Intelligence Surveillance Court ("**FISA**").

   c. If The Company becomes aware of any law enforcement agency or other governmental authority ("**Authority**") attempt or demand to gain access to or a copy of the Personal Data (or part thereof), whether on a voluntary or a mandatory basis, then, unless legally prohibited or under a mandatory legal compulsion that requires otherwise, The Company shall: inform the relevant Authority that The Company is a Processor of the Personal Data and that Publisher, as the Controller has not authorized The Company to disclose the Personal Data to the Authority; inform the relevant Authority that any and all requests or demands for access to the Personal Data should be directed to or served upon Publisher in writing; and use reasonable legal mechanisms to challenge any such demand for access to Personal Data which is under the Company's control.

   d. Notwithstanding the above, if, taking into account the nature, scope, context and purposes of the related Authority's intended access to Personal Data, The Company has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual or entity, these subsections shall not apply. In such event, The Company shall notify Publisher, as soon as possible, following the access by the Authority, and provide Publisher with relevant details, unless and to the extent legally prohibited to do so.

   The Company will inform Publisher, upon written request (and not more than once a year), of the types of binding legal demands for Personal Data The Company has received and complied with, including demands under national security orders and directives, specifically including any process under Section 702 of FISA.

ANNEX V
UK INTERNATIONAL TRANSFERS AND SCC

1. The parties agree that the terms of the Standard Contractual Clauses as amended by the UK Standard Contractual Clauses, and as amended in this **Annex V**, are hereby incorporated by reference and shall apply to transfer of Personal Data from the UK to other countries that are not deemed as Adequate Countries.
2. This **Annex V** is intended to provide appropriate safeguards for the purposes of transfers of Personal Data to a third country in reliance on Article 46 of the UK GDPR and with respect to data transfers from controllers to processors or from the processor to its sub-processors.
3. Terms used in this **Annex V** that are defined in the Standard Contractual Clauses, shall have the same meaning as in the Standard Contractual Clauses.
4. This **Annex V** shall (i) be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that if fulfils the intention for it to provide the appropriate safeguards as required by Article 46 of the UK GDPR, and (ii) not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.
5. Amendments to the UK Standard Contractual Clauses:

5.1. Part 1: Tables

5.1.1. Table 1 Parties: shall be completed as set forth in Section 4 within **Annex IV** above.

5.1.2. Table 2 Selected SCCs, Modules and Selected Clauses: shall be completed as set forth in Section 2 and 3 within **Annex IV** above.

5.1.3. Table 3 Appendix Information:

Annex 1A: List of Parties: shall be completed as set forth in Section 2 within **Annex IV** above.

Annex 1B: Description of Transfer: shall be completed as set forth in **Annex I** above.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: shall be completed as set forth in **Annex II** above.

Annex III: List of Sub processors: shall be completed as set forth in **Annex III** above.

5.1.4. Table 4 Ending this Addendum when the Approved Addendum Changes: shall be completed as “neither party”.

ANNEX VI

SUPPLEMENTARY TERMS FOR SWISS DATA PROTECTION LAW TRANSFERS ONLY

The following terms supplement the Clauses only if and to the extent the Clauses apply with respect to data transfers subject to Swiss Data Protection Law, and specifically the FDPA:

- The term 'Member State' will be interpreted in such a way as to allow data subjects in Switzerland to exercise their rights under the Clauses in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Clauses.

- The clauses in the DPA protect the Personal Data of legal entities until the entry into force of the Revised Swiss FDPA.

- All references in this DPA to the GDPR should be understood as references to the FDPA insofar as the data transfers are subject to the FDPA.

- References to the "competent supervisory authority", "competent courts" and "governing law" shall be interpreted as Swiss Data Protection Laws and Swiss Information Commissioner, the competent courts in Switzerland, and the laws of Switzerland (for Restricted Transfers from Switzerland).

- In respect of data transfers governed by Swiss Data Protection Laws and Regulations, the EU SCCs will also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws and Regulations until such laws are amended to no longer apply to a legal entity.

- The competent supervisory authority is the Swiss Federal Data Protection Information Commissioner.

ANNEX VII

US Privacy Law Addendum

This US Privacy Law Addendum ("**US Addendum**") adds specification applicable to US Data Protection Laws and is in addition to the obligations set forth in the DPA. All terms used but not defined in this CCPA Addendum shall have the meaning set forth in the DPA.

1. **CCPA Specifications:**
    a. For the purpose of the CCPA, Publisher is the Business and Company is the Service Provider.
    b. Company shall process Personal Data on behalf of the Publisher as a Service Provider under the CCPA and shall not: (1) sell or share the Publisher Data; (2) retain, use or disclose the Publisher Data for any purpose other than for Publisher purpose specified in the Agreement; or (3) combine the Publisher Data with other Personal Data that it receives from, or on behalf of, another customer, or collects from its own interaction with California residents, expect as otherwise permitted by the CCPA.
    c. Company shall assist Publisher in respect of consumer request to limit the use of Sensitive Personal Information ("SPI").
    d. Company certifies that it understands the rules, requirements and definitions of the CCPA and agrees to refrain from Selling any Publisher Data.
    e. For the purpose of processing Personal Information made available through the Controller Data Sets, and when the Publisher has chosen the Cross-Contextual Behavior Advertising ("**CCBA**") the following shall apply:
        i. Company shall be the Third Party Business and Publisher is the First Party Business.
        ii. Each party shall independently responsible for complying with the CCPA obligations as a "Business".
        iii. Company requires and relies on the Publisher to provide the End Users with disclosure as applicable under the CCPA regarding Sharing and Selling Personal Information for CCBA with Company.
        iv. Company required that the Publisher will enable the End User to opt-out from Selling and Sharing the Personal Information with Company for CCBA and transfer the opt-out signal to Company.
2. **US Applicable States Specifications:**
    a. For the purpose of this US Addendum "Applicable States" shall mean Virginia, California, Colorado, and Connecticut.
    b. Company agrees to notify the Publisher if Company makes a determination that it can no longer meet its obligations under this Addendum or US Data Protection Laws.
    c. Company shall provide information necessary to enable the Publisher to conduct and document any data protection assessments required by US Data Protection Laws.

Notwithstanding the above, Company is responsible for only the measures allocated to it.

d. Company acknowledges and confirms that it does not receive any monetary goods, payments or discounts in exchange for processing the Publisher Data.

e. Each party shall, taking into account the context of processing, shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and establish a clear allocation of the responsibilities between them to implement the measures. Company technical measures are detailed in the DPA and Annexes above.

f. The processing instructions, including the nature of processing, purpose of processing, the duration of processing, the type of personal data and data subjects, are set forth in **Annex I** above.

g. In addition to the Audit rights under Section 8 of the DPA, under US Data Protection Laws and subject to Publisher's consent, Company my alternately offer, in response to an on premises audit request, initiate a third-party auditor to verify Companys' compliance with its obligations under this US Data Protection Laws. During such an audit, Company will make available to the third-party auditor all information necessary to demonstrate such compliance.

h. Each party will comply with the requirements set forth under US Data Protection Laws with regards to processing de-identified data, as such term defined under the applicable US Data Protection Law.

When processing Publisher Data or Usage Data (as defined in the Agreement) for the permitted purposes under US Data Protection Laws Company shall ensure it complies with applicable laws and shall be liable for such processing.