Vizrt

Customer Data Processing Addendum

This Customer Data Processing Addendum ("**DPA**") applies whenever it is incorporated by reference or attached to an agreement (the "**Agreement**") entered into by and between: (1) the Vizrt entity identified in the Agreement and one or more of its affiliated group companies ("**Vizrt**"); and (2) a customer of Vizrt's products and services, as identified in the Agreement ("**Customer**"). In the event of any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

1. Definitions and interpretation

1.1. *Definitions:* In this DPA, the following terms shall have the following meanings:

"**Applicable Data Protection Law**"	means any and all privacy, data security, and data protection laws applicable to the Processing of Personal Data pursuant to this DPA, including (where applicable) any Jurisdiction-Specific Requirements.
"**Controller**"	means: (a) an entity that alone or jointly with others determines the purposes and means of Processing of Personal Data; and (b) any entity that is defined to be a "controller", "business", or substantially analogous concept under Applicable Data Protection Laws and any Jurisdiction-Specific Requirements.
"**Customer Data**"	means Personal Data for which Customer is the Controller, and which Vizrt will Process pursuant to this DPA and the Agreement, as set out in Annex A.
"**Data Subject**"	means an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
"**Effective Date**"	shall have the same meaning as given in the Agreement.
"**Jurisdiction-Specific Requirements**"	means country- or region-specific privacy and data protection requirements set out in Annex C, if and to the extent applicable to the Processing of Personal Data pursuant to this DPA.

“**Permitted Purpose**”	means the purpose for which Customer appoints Processor to Process Customer Data, as set out in Annex A.
“**Personal Data**”	means: (a) any information relating to a Data Subject; and (b) includes any “personal data”, “personal information”, “personally identifiable information”, “protected health information”, or substantially analogous concept under Applicable Data Protection Laws and any Jurisdiction-Specific Requirements that relates to a Data Subject.
“**Processing**”	means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The terms "**Process**" and "**Processes**" shall be construed accordingly.
“**Processor**”	means: (a) an entity that Processes Personal Data on behalf of, and in accordance with the instructions of, a Controller; and (b) any entity that is defined to be a “processor”, “service provider”, or substantially analogous concept under Applicable Data Protection Laws and any Jurisdiction-Specific Requirements.
“**Restricted Transfer**”	means a transfer of Personal Data from a country in which it is lawfully Processed to a third country, in circumstances where the transfer is either prohibited by Applicable Data Protection Law or permitted to proceed only if certain additional requirements specified by Applicable Data Protection Law are fulfilled. A transfer shall include the provision of remote access to Personal Data from a third country.
“**Security Incident**”	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

1.2. *Interpretation:* Capitalized terms used but not defined in this DPA shall have the meanings given in the Agreement.

2. Data Protection

2.1. *Processor appointment:* With effect from the Effective Date, Customer appoints Vizrt as its Processor to Process the Customer Data for the Permitted Purpose. Customer is the Controller of the Customer Data and is authorised to instruct Vizrt to Process the Personal Data for the Permitted Purpose. Vizrt shall Process the Customer Data only for the Permitted Purpose (or as otherwise instructed in writing by Customer).

2.2. *Compliance with law:* Each party shall comply with its obligations under Applicable Data Protection Law, including any Jurisdiction-Specific Requirements where and to the extent that these apply.

2.3. *Confidentiality of Processing:* Vizrt shall ensure that any person it authorises to Process the Customer Data for the Permitted Purpose (including Vizrt's staff, agents and subcontractors) (each an "**Authorised Person**") shall be subject to a duty of confidentiality (whether contractual or statutory), and shall not permit any person to Process the Customer Data who is not under such a duty of confidentiality. In no event shall Vizrt disclose any Customer Data to a third party except where and to the extent necessary for the Permitted Purpose or in accordance with the Agreement.

2.4. *De-identification:* Where Vizrt is permitted by Applicable Data Protection Law or this DPA to use or disclose Personal Data in a de-identified manner, Vizrt agrees to take reasonable measures designed to ensure that the Personal Data cannot be associated with an individual (or, household, where applicable), publicly commits to maintain and use the information in de-identified form only and make no attempt to re-identify the information except where necessary to test its de-identification processes, and contractually obligates any authorized recipients to comply with these obligations.

2.5. *Security:* Vizrt shall at all times implement and maintain appropriate and reasonable technical, physical and organisational security measures to protect the Customer Data from a Security Incident. Such measures shall take 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 Data Subjects, and shall include as appropriate measures for:

(a) the pseudonymisation and encryption of Personal Data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.]

At a minimum, such measures shall include the measures identified in Annex B.

2.6. *Subcontracting:* Customer agrees that Vizrt may subcontract Processing of the Customer Data to a third-party sub-Processor provided that:

(a) Vizrt provides Customer with prior notice in writing at least fourteen (14) days in advance of any sub-Processor appointment (and, for these purposes, Customer agrees that such notice shall be provided by means of a publicly-accessible webpage where Vizrt provides details of all of its sub-Processor, including proposed sub-Processor appointments);

(b) If Customer objects to the proposed sub-Processor prior to its appointment on reasonable grounds related to data protection, then Vizrt shall discuss with Customer how to resolve the Customer's concerns prior to the sub-Processor's appointment. If Vizrt is unable to resolve the Customer's concerns prior to the sub-Processor's appointment, then either (i) Vizrt will not appoint the proposed sub-Processor, or (ii) if Vizrt intends to proceed with the sub-Processor appointment anyway, it will immediately notify Customer and Customer may terminate this DPA and the Agreement immediately without penalty;

(c) If Customer does not object to the proposed sub-Processor prior to its appointment, then Vizrt may proceed to appoint the sub-Processor provided that: (i) the sub-Processor will Process the Customer Data strictly for the Permitted Purpose or otherwise as expressly permitted by this Agreement; (ii) Vizrt imposes data protection terms on the sub-Processor that protect the Customer Data to substantially the same standard provided for by this DPA; and (iii) Vizrt remains fully liable for any breach of this DPA that is caused by an act, error or omission of the sub-Processor it appoints.

2.7. *Data subjects' rights:* Vizrt shall provide reasonable and timely assistance to Customer (at the Customer's expense) to enable Customer: (i) to fulfil any request from a Data Subject to exercise any of its rights under Applicable Data Protection Law (including, without limitation, rights of access, correction and deletion); and (ii) to respond to any other communication received from a Data Subject, a competent data protection authority or other third party in connection with the Processing of the Customer Data. If any such communication is made directly to Vizrt, Vizrt shall inform Customer providing full details of the same and without responding to the communication (unless instructed to do so by Customer or required by Applicable Data Protection Law).

2.8. *Security incidents:* If Vizrt becomes aware of a Security Incident with respect to the Processing of Personal Data under this DPA, it shall inform Customer without undue delay and shall provide such timely information and cooperation as Customer may reasonably require to ensure that data breach reporting obligations are fulfilled under (and in accordance with the timescales required by) Applicable Data Protection Law. Vizrt shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep Customer informed of all relevant developments in connection with the Security Incident. Vizrt shall not inform any third parties about any Security Incident impacting Customer Data that identifies the Customer or a Data Subject of Customer without Customer's consent, other than: (i) its professional advisors and insurers, subject to a strict duty of confidence; and (ii) where and to the extent necessary to comply with Applicable Data Protection Law.

2.9. *Data Protection Impact Assessments:* Vizrt shall provide all reasonable and timely assistance and information Customer may require (at Customer's expense):

(a) to enable Customer to carry out an assessment of the impact of Vizrt's envisaged Processing operations on the protection of Customer Data (a "**Data Protection Impact Assessment**") where and to the extent this is required by Applicable Data Protection Law; and

(b) for Customer to consult with any competent data protection authority where this is required by Applicable Data Protection Law in connection with any Data Protection Impact Assessment Customer has carried out in accordance with this Clause.

2.10. *Deletion or return of Data:* The DPA shall terminate immediately upon termination or expiry of the Agreement. Vizrt shall delete all Customer Data in its possession or control (including any Customer Data subcontracted to a third-party sub-Processor for Processing). This requirement shall not apply to the extent that Vizrt is permitted to retain some or all of the Customer Data pursuant to the Applicable Data Protection Law.

2.11. *Audit:* Vizrt shall make available to Customer all information necessary to demonstrate compliance with the obligations laid down in this DPA and allow for and contribute to audits, including inspections, conducted by Customer or another auditor chosen by Customer. In addition, Vizrt shall also respond to any reasonable, written audit questions submitted to it by Customer, provided that Customer shall not exercise this right more than once per year.

3. Restricted Transfers

3.1. If a party intends to make a Restricted Transfer of Customer Data (whether to the other party or to any third-party) it shall do all such acts and things necessary to ensure that the Restricted Transfer will comply with Applicable Data Protection Law and any Jurisdiction-Specific Requirements prior to making the Restricted Transfer.

4. Miscellaneous

4.1. *Governing law and jurisdiction:* This DPA shall be subject to any dispute resolution procedure(s) specified in, and the governing law and jurisdiction of, the Agreement.

4.2. Limitation of liability: Breaches of the DPA will be subject to the same limitation of liability as under the Agreement.

Annex A

Description of the Processing

A. LIST OF PARTIES

Controller / Data exporter(s)

Name:	See Customer's details as set out in the Agreement.
Address:	See Customer's details as set out in the Agreement.
Contact person's name, position and contact details:	See Customer's details as set out in the Agreement.
Activities relevant to the data transferred under these Clauses:	The receipt of data processing services as described in this DPA and the Agreement.
Signature and date:	This DPA shall be deemed executed upon acceptance or execution of the Agreement by the parties.
Role (Controller/Processor):	Controller

Processor / Data importer(s):

Name:	See Vizrt's details as set out in the Agreement.
Address:	See Vizrt's details as set out in the Agreement.
Contact person's name, position and contact details:	See Vizrt's details as set out in the Agreement.
Activities relevant to the data transferred under these Clauses:	The provision of data processing services as described in this DPA and the Agreement.
Signature and date:	This DPA shall be deemed executed upon acceptance or execution of the Agreement by the parties.
Role (Controller/Processor):	Processor

B. DESCRIPTION OF PROCESSING AND TRANSFER

Categories of Data Subjects whose Personal Data is Processed and transferred	End users of the Flowics platform (e.g., customers' employees, contractors) Viewers or audience members interacting with Flowics-powered features (e.g., social polls, forms, second-screen modules) Social media users whose publicly available content is processed
Categories of Personal Data Processed and transferred	Account and authentication data (e.g., name, email address, login activity, IP address)

	Usage and telemetry data (e.g., interaction logs, analytics) Content-related data (e.g., user-generated forms, poll interactions, curated social media content) Contact/support data (e.g., support messages, in-app feedback)
Sensitive data Processed and 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	Flowics is not intended for processing special categories of data. However, if customers configure features to collect such data, appropriate security, access control, and data minimization safeguards are applied. Customers remain responsible for ensuring that such use is lawful and appropriate.
The frequency of the Processing and transfers (e.g. whether the data is Processed and transferred on a one-off or continuous basis)	Continuous for the duration of the Agreement.
Nature of the Processing	Collecting, storing, analyzing, curating, and displaying data as necessary for the delivery of Flowics cloud-based broadcast graphics services to the Customer, as described in the Agreement and this DPA, including customer-facing content rendering and analytics..
Purpose(s) of the data transfer and further Processing	To operate and support the Flowics platform in accordance with the Agreement and the DPA, including account management, feature delivery, support, analytics, and performance optimization.
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 and for no longer than 12 months after termination or expiration of the Agreement, unless applicable data protection law requires retention.
For transfers to (sub-) Processors, also specify subject matter, nature and duration of the Processing	□ Vizrt uses subprocessors to provide infrastructure (AWS, Azure, GCP), authentication (Auth0), observability/logging (New Relic, Rapid7), and communication (Intercom). □ All subprocessors process data for the same purpose and duration as Vizrt, limited to their functional roles, as documented in Flowics' vendor list https://www.flowics.com/legal/sub-processors/?

Annex B

Security Measures

Except as may otherwise be set out in the Agreement, Vizrt shall apply the security measures described at https://www.vizrt.com/product-security/.

1. Organisational Measures

- Data Protection Governance: Vizrt maintains a dedicated Legal and Security team responsible for privacy and information security oversight, including compliance with applicable data protection laws.

- Access Control and Role-Based Permissions
  - Access to production systems is limited to authorized personnel based on job function.
  - Role-based access controls are enforced across services (e.g., CRM, Intercom, analytics).
  - Contractors and employees undergo access reviews and have unique credentials.

- Employee Confidentiality and Training
  - All personnel are subject to confidentiality obligations via employment or contractual agreements.
  - Privacy and security awareness is embedded through onboarding and ongoing training.
  - All developers are required to complete specialized secure development training to ensure adherence to secure coding practices and organizational standards.

- Vendor and Subprocessor Management
  - Subprocessors undergo due diligence and are bound by contractual obligations including equivalent TOMs.
  - A list of subprocessors is maintained and updated publicly.

- Policy and change management
  - Vizrt maintains a comprehensive set of information security and data protection policies, reviewed at least annually.
  - System and application changes follow a documented change management process, including testing, approvals, and rollback procedures.

2. Technical Measures

- Encryption
  - Data in transit is encrypted using TLS 1.2 or higher.
  - Data at rest is encrypted using industry-standard protocols (e.g., AES-256).

- Authentication and Access Security
  - Authentication is implemented following industry standards, using Auth0 with support for SSO and MFA.
  - Passwords are securely stored using salting and hashing. Strong password policies are enforced through complexity rules, and any weak or commonly used passwords are automatically detected and rejected.

- Infrastructure Security
  - Core infrastructure is hosted in cloud environments (AWS, Azure, GCP) in the United States.

- Application and Product Security
  - Application-level logging and telemetry via New Relic and Rapid7 InsightOps.
  - Secure coding practices and periodic penetration tests are applied.
  - Web Application Firewall (WAF) and DDoS protections are provided via Cloudflare.

- Data Minimization and Segregation
    - Customers control the amount and type of personal data collected (e.g., via forms).
    - Data is logically segregated by customer account.

3. Availability, Backup and Business Continuity

- Redundancy and Failover
    - Flowics leverages redundant infrastructure and cloud-native architecture for high availability.

- Backup and Recovery
- Automated backups are in place for core systems.
    - Backup data is encrypted and retained in accordance with retention policies.

- Incident Response
    - Security incidents are escalated through an internal response protocol.
    - Customers are notified without undue delay in the event of a breach affecting their data.

4. Audit, Monitoring and Risk Management

- Logging and Monitoring
    - Audit trails, user activity logs, and system logs are maintained across services.
    - Logs are retained (e.g., 30 days for access logs, 2 years for deep storage) for troubleshooting and accountability.

- Security Reviews and Testing
    - Regular vulnerability scanning and targeted testing are conducted.

- Data Protection Impact Assessments (DPIAs)
    - DPIAs are supported where required, in collaboration with Vizrt's legal team.

Annex C

Jurisdiction-Specific Requirements

Part A: EU, UK and Switzerland

1. **Application of this Part A**

1.1. This Part A (EU, UK and Switzerland) to Annex C (Jurisdiction-Specific Requirements) applies where and to the extent that the Processing of Personal Data pursuant to this DPA is subject to EU Data Protection Law, Swiss Data Protection Law and/or UK Data Protection Law.

1.2. In the event of any conflict between this Part A (EU, UK and Switzerland) of Annex C (Jurisdiction-Specific Requirements) and the body of the DPA, this Part A shall prevail to the extent of that conflict.

2. **Definitions and interpretation**

2.1. Where this Part A (EU, UK and Switzerland) to Annex C (Jurisdiction-Specific Requirements) applies, the following terms shall have the following meanings:

"**Data Privacy Framework**" or "**DPF**"	means the EU-U.S. Data Privacy Framework ("**EU-US DPF**"), the UK Extension to the EU-U.S. DPF ("**UK-US Extension**"), and the Swiss-U.S. Data Privacy Framework ("**Swiss-US DPF**") as set forth by the U.S. Department of Commerce.
"**EU Data Protection Law**"	means: (i) EU Regulation 2016/679 (the "**EU GDPR**"); (ii) EU Directive 2002/58/EC; and (iii) the national laws of each EEA member state made under, pursuant to, or that implement (i) or (ii), or which otherwise relate to the Processing of Personal Data; in each case, as amended or superseded from time to time.
"**EU/UK/Swiss Restricted Transfer**"	means: (i) where the EU GDPR applies, a transfer of Personal Data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission (an "**EU Restricted Transfer**"); (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not subject to or based on adequacy regulations

pursuant to Section 17A of the United Kingdom Data Protection Act 2018 (a "**UK Restricted Transfer**"); and

(iii) where the Swiss DPA applies, a transfer of Personal Data from Switzerland to any other country which is not subject to an adequacy determination by the Swiss Federal Data Protection and Information Commissioner or Federal Council (as applicable) (a "**Swiss Restricted Transfer**").

For the avoidance of doubt, a transfer of Personal Data to the United States pursuant to the Data Privacy Framework shall not be a Restricted Transfer.

"**Standard Contractual Clauses**" means:

(i) where the EU GDPR or the Swiss DPA applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and

(ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the DPA 2018 ("**UK Addendum**").

"**Swiss Data Protection Law**" means:

(i) the Swiss Federal Act on Data Protection of 25 September 2020 and its corresponding ordinances ("**Swiss DPA**"); and

(ii) any other national laws in Switzerland applicable (in whole or in part) to the Processing of Personal Data;

in each case, as amended or superseded from time to time.

"**UK Data Protection Law**" means:

(i) the EU GDPR as it forms part of UK law by virtue of section 3 of the European

Union (Withdrawal) Act 2018 (the "**UK GDPR**");

(ii) the Privacy and Electronic Communications (EC Directive) Regulations 2003 as it continues to have effect under section 2 of the European Union (Withdrawal) Act 2018;

(iii) the Data Protection Act 2018 (the "**DPA 2018**"); and

(iv) any other laws in the UK made under, pursuant to, or that implement (i), (ii) or (ii), or which otherwise relate to the Processing of Personal Data;

in each case, as amended or superseded from time to time.

2.2. Where this Part A (EU, UK and Switzerland) to Annex C (Jurisdiction-Specific Requirements) applies, the term "**Applicable Data Protection Law**" shall be deemed to include EU Data Protection Law, Swiss Data Protection Law and UK Data Protection Law.

3. **Restricted Transfers**

3.1. *Restricted transfers to Vizrt:* To the extent that any transfer of Customer Data from Customer to Vizrt is a Restricted Transfer, the Standard Contractual Clauses shall be incorporated into this DPA and apply as follows:

(a) where the Restricted Transfer is an EU Restricted Transfer, the EU SCCs will apply between Customer and Vizrt as follows:

(i) Module Two will apply;

(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 clause 2.5 of this DPA;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Sweden law;

(vi) in Clause 18(b), disputes shall be resolved before the courts of Sweden;

(vii) in Annex I:

(A) Parts A and B shall be deemed completed with the information set out in Annex A to this DPA;

(B) Part C shall be deemed completed in accordance with the criteria set out in Clause 13(a) of the EU SCCs;

(vii) Annex II shall be deemed completed with the security measures set out in Annex B to this DPA;

(b) where the Restricted Transfer is a UK Restricted Transfer, the UK Addendum will apply between Customer and Vizrt as follows:

(i) the EU SCCs, completed as set out above shall apply between Customer and Vizrt, and shall be modified by the UK Addendum (completed as set out in sub-clause (ii) below); and

(ii) tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from the EU SCCs, completed as set out above, and the options "Exporter" and "Importer" shall be deemed checked in table 4. The start date of the UK Addendum (as set out in table 1) shall be the Effective Date; and

(c) where the Restricted Transfer is a Swiss Restricted Transfer, the EU SCCs will apply between Customer and Vizrt with the following modifications:

(i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;

(ii) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss DPA;

(iii) references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" or "Swiss law" (as applicable);

(iv) the term "member state" shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland);

(v) Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the Swiss Federal Data Protection and Information Commissioner;

(vi) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection and Information Commissioner" and "applicable courts of Switzerland";

(vii) in Clause 17, the EU SCCs shall be governed by the laws of Switzerland.

1.2. *Restricted transfers by Vizrt:* Vizrt will not make a Restricted Transfer of Customer Data to a third party unless it has done all such acts and things as are necessary to ensure that the Restricted Transfer is compliant with Applicable Data Protection Law and any Standard Contractual Clauses it has executed with Customer.

Part B: California

1. **Application of this Part C**

1.1. This Part C (California) to Annex C (Jurisdiction-Specific Requirements) applies where and to the extent that the Processing of Personal Data pursuant to this DPA is subject to California's Data Protection Law.

1.2. In this event of any conflict between this Part C (California) of Annex C (Jurisdiction-Specific Requirements) and the body of the DPA, this Part C shall prevail to the extent of that conflict.

2. **Definitions and interpretation**

2.1. Where this Part C (California) to Annex C (Jurisdiction-Specific Requirements) applies, the following terms shall have the following meanings:

"**California Data Protection Law**" means:

(i) the California Consumer Privacy Act of 2018, Civil Code section 1798.100 et seq, as amended (including as amended by the California Privacy Rights Act of 2020) ("**CCPA**") and its implementing regulations; and

(ii) any other laws and regulations in California applicable (in whole or in part) to the Processing of Personal Data;

in each case, as amended or superseded from time to time.

2.2 The terms "**Business**", "**Business Purpose**", "**Commercial Purpose**", "**Contractor**", "**Sell**", "**Service Provider**", "**Share**", and "**Third Party**" shall have the same meaning as in the California Data Protection Law and construed accordingly.

2.3 Where this Part C (California) to Annex C (Jurisdiction-Specific Requirements) applies, the term "Applicable Data Protection Law" shall be deemed to include California Data Protection Law.

3. **Role of the Parties**

3.1 Vizrt is Processing Personal Data in connection with the Services in the capacity as a Service Provider under California Data Protection Law and Customer is a Business under such law. If Customer is also a Service Provider of Personal Data, Customer represents and warrants that its instructions and Processing of Personal Data, including its appointment of Vizrt as a subcontractor, have been authorized by the Customer's customer (as the respective Business instructed Customer as a service provider) its instructions to Vizrt comply with California Data Protection Law.

4. **Customer Instructions and Restrictions on Processing**.

4.1 *Instruction and Direction*. Vizrt shall use, retain, disclose, or otherwise Process Personal Data only on behalf of Customer and for the specific Business Purposes described in this Part C to provide the Services and in accordance with Customer's instructions, including as described

in the Agreement. Vizrt shall not Sell or Share Personal Data. Vizrt shall not use, retain, disclose, or otherwise Process Personal Data outside of its business relationship with Customer or for any other purpose (including Vizrt's Commercial Purpose) except as required or permitted by law. Vizrt will inform Customer if, Vizrt determines that it is no longer able to meet its obligations under California Data Protection Laws. Customer reserves the right to take reasonable and appropriate steps to (i) ensure Vizrt's Processing of Personal Data is consistent with Customer's obligations under California Data Protection Law and (ii) discontinue and remediate unauthorized use of Personal Data.

4.2. *No Combination of Personal Data*. Vizrt will not combine Personal Data which Vizrt Processes on Customer's behalf, with Personal Data which it receives from or on behalf of another person or persons, or collects from its own interaction with individual, provided that Vizrt may combine Personal Data to perform any Business Purpose permitted or required under the Agreement to perform the Services.

4.3 *Business Purposes*. Vizrt is permitted to Process Personal Data for the following and limited Business Purposes:

(a) Auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards;

(b) Helping to ensure security and integrity to the extent the use of the Data Subject's Personal Data is reasonably necessary and proportionate for these purposes;

(c) Debugging to identify and repair errors that impair existing intended functionality;

(d) Short-term, transient use, including, but not limited to, non-personalized advertising shown as part of a Data Subject's current interaction with the Business, provided that the Data Subject's Personal Data is not disclosed to another Third Party and is not used to build a profile about the Data Subject or otherwise alter the Data Subject's experience outside the current interaction with the Business;

(e) Performing services on behalf of the Business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the Business;

(f) Providing advertising and marketing services, except for cross-context behavioural advertising, to the Data Subject provided that, for the purpose of advertising and marketing, Vizrt shall not combine the Personal Data of opted-out consumers that Vizrt receives from, or on behalf of, the Business with Personal Data that Vizrt receives from, or on behalf of, another person or persons or collects from its own interaction with Data Subjects;

(g) Undertaking internal research for technological development and demonstration;

(h) Undertaking activities to verify or maintain the quality or safety of a Service or device that is owned, manufactured, manufactured for, or controlled by the Business, and to improve, upgrade, or enhance the Service or device that is owned, manufactured, manufactured for, or controlled by the Business;

(i) To retain and employ another Service Provider or Contractor as a subcontractor where the subcontractor meets the requirements for a Service Provider or Contractor under California Data Protection Law;

(j) To build or improve the quality of the Services it is providing to the Business provided that Vizrt does not use the Personal Data to perform Services on behalf of another person.

(k) To prevent, detect, or investigate data security incidents or protect against malicious, deceptive, fraudulent, or illegal activity.

4.4 *Third Parties*. To the extent Vizrt Processes Personal Data as a Third Party under the California Data Protection Laws, the following provisions shall apply instead of Sections 4.1-4.3 for such Processing conducted as a Third Party: Vizrt may process Personal Data only for the limited and specified purposes described in the Agreement and this DPA. Vizrt must comply with all applicable California Data Protection Laws, including all applicable sections of the CCPA and provide the same level of privacy protection as required of businesses by the CCPA. Vizrt will promptly inform Customer if Vizrt determines that it is no longer able to meet its obligations under California Data Protection Laws. Customer reserves the right to take reasonable and appropriate steps to ensure that Vizrt as a Third Party Processes Personal Data it in a manner consistent with the Business's obligations under the applicable California Data Protection Laws and these regulations and discontinue and remediate unauthorized use of Personal Data.