# Vizrt

## Supplier Data Processing Addendum

This Supplier 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 provider of the Vizrt products and services, as identified in the Agreement (**"Supplier"**). 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:<br>(a) an entity that alone or jointly with others determines the purposes and means of Processing of Personal Data; and<br>(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 Vizrt is the Controller, and which Supplier 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 Vizrt appoints Processor to Process Customer Data, as set out in Annex A. |
| "**Personal Data**" | means:<br>(a) any information relating to a Data Subject; and<br>(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:<br>(a) an entity that Processes Personal Data on<br>(b) behalf of, and in accordance with the instructions of, a Controller; and<br>(c) 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:* Capitalised 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, Vizrt appoints Supplier as its Processor to Process the Customer Data for the Permitted Purpose. Vizrt is the Controller of the Customer Data and is authorised to instruct Supplier to Process the Personal Data for the Permitted Purpose. Supplier shall Process the Customer Data only for the Permitted Purpose (or as otherwise instructed in writing by Vizrt).

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:* Supplier shall ensure that any person it authorises to Process the Customer Data for the Permitted Purpose (including Supplier's staff, agents and subcontractors) (each an "**Authorised Person**") shall be subject to a duty of confidentiality (whether contractual or

statutory) and Supplier shall not permit any person to Process the Customer Data who is not under such a duty of confidentiality. In no event shall Supplier 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 Supplier is permitted by Applicable Data Protection Law or this DPA to use or disclose Personal Data in a de-identified manner, Supplier 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 deidentified form only and make no attempt to re-identify the information except where necessary to test its de-identification processes, and contractually obligates any authorised recipients to comply with these obligations.

2.5. *Security:* Supplier 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 security measures identified in Annex B.

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

(a) Supplier conducts appropriate due diligence to ensure it retains sub-Processors which present sufficient guarantees in terms of confidentiality, security and data protection in accordance with Applicable Data Protection Law;

(b) Supplier provides Vizrt with prior notice in writing at least thirty (30) days in advance of any sub-Processor appointment (and, for these purposes, Vizrt agrees that such notice shall be provided by means of a publicly-accessible webpage where Supplier provides details of all of its sub-Processor, including proposed sub-Processor appointments);

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

(d) If Vizrt does not object to the proposed sub-Processor prior to its appointment, then Supplier 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) Supplier 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) Supplier 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:* Supplier shall provide reasonable and timely assistance to Vizrt to enable Vizrt: (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 Supplier, Supplier shall inform Vizrt providing full details of the same and without responding to the communication (unless instructed to do so by Vizrt or required by Applicable Data Protection Law).

2.8. *Security incidents:* If Supplier becomes aware of a Security Incident with respect to the Processing of Customer Data under this DPA, it shall inform Vizrt promptly, and in any event within twenty-four (24) hours, and shall provide such timely information and cooperation as Vizrt 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. Supplier shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep Vizrt informed of all relevant developments in connection with the Security Incident. Supplier shall not inform any third parties about any Security Incident impacting Customer Data that identifies Vizrt or a Data Subject of Vizrt without Vizrt'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:* Supplier shall provide all reasonable and timely assistance and information Vizrt may require:

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

(b) for Vizrt 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 Vizrt 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. Supplier shall permanently delete all copies of 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 the Supplier is permitted to retain some or all of the Customer Data pursuant to the Applicable Data Protection Law, in which case Supplier shall isolate and protect the Customer Data from any further Processing except to the extent required by such Applicable Data Protection Law. Supplier shall permanently delete such retained data without undue delay when technically feasible and/or allowed by the Applicable Data Protection Law.

2.11. *Audit:* Supplier shall maintain and make available to Vizrt 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 Vizrt or another auditor chosen by Vizrt. In addition, Supplier shall also respond to any reasonable, written audit questions submitted to it by Vizrt.

## 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 (set out in Annex C) 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 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 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 Supplier's details as set out in the Agreement. |
| **Address:** | See Supplier's details as set out in the Agreement. |
| **Contact person's name, position and contact details:** | See Supplier'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** | The categories of Personal Data processed by Supplier on behalf of Vizrt shall be as specified in the Agreement or the accompanying product documentation for the product or service to be delivered by Supplier. . |

| | |
|---|---|
| **Categories of Personal Data Processed and transferred** | The categories of Personal Data Processed by Supplier on behalf of Vizrt shall be as specified in the Agreement or the accompanying product documentation for the product or service to be delivered by Supplier. |
| **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** | The sensitive data (if any) Processed by Supplier on behalf of Vizrt shall be as specified in the Agreement or the accompanying product documentation for the product or service to be delivered by Supplier. |
| **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** | Processing as necessary for the delivery of Supplier's products and services to Vizrt, as described in the Agreement and this DPA. |
| **Purpose(s) of the data transfer and further Processing** | Processing as necessary for the delivery of Supplier's products and services to Vizrt, as described in the Agreement and this DPA. |
| **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. |
| **For transfers to (sub-) Processors, also specify subject matter, nature and duration of the Processing** | The subject matter, nature and duration of the Processing shall be as specified in the Agreement. |

## Annex B

## Security Measures

Except as may otherwise be set out in the Agreement, Supplier shall implement and maintain, as a minimum, the following technical and organisational security measures for all systems, networks, applications and services that Process Customer Data.

Supplier documentation may supplement, but shall not reduce or qualify, the measures set out in this Annex B. Supplier shall maintain documented evidence of the implementation of these measures and shall make it available to Vizrt upon reasonable request. Where this Annex B refers to a defined frequency, timeframe, period or objective, Supplier shall document the value it applies and shall provide it to Vizrt upon request.

### 1. Security Governance and Risk Management

1.1 Supplier shall maintain a documented information security program, including security policies based on a recognised framework (such as ISO/IEC 27001, the NIST Cybersecurity Framework or the CIS Controls) that are approved by management and reviewed at a defined frequency, and shall designate a person or team responsible for information security.

1.2 Supplier shall maintain a risk management program under which information security risks to the services and to Customer Data are assessed at a defined frequency and upon significant change, and identified risks are treated, tracked and formally accepted where not remediated.

1.3 Supplier shall maintain a third-party risk management process under which its suppliers and sub-Processors with access to Customer Data, or to systems that Process Customer Data, are assessed for security before engagement and at a defined frequency thereafter, and are bound by security obligations no less protective than those in this Annex B.

### 2. Security Awareness and Training

2.1 Supplier shall provide security awareness training to all personnel with access to Customer Data before access is granted and at a defined frequency thereafter.

### 3. Identity and Access Management

3.1 Supplier shall grant access to Customer Data, and to systems that Process Customer Data, on a role-based, least-privilege and need-to-know basis, using unique, individually attributable accounts. Shared or generic user accounts shall not be used; technical service accounts shall be documented, assigned an owner and secured.

3.2 Supplier shall enforce multi-factor authentication for all remote access, all administrative and privileged access, and all access to cloud management consoles and administrative interfaces of services used to Process Customer Data. For privileged access, Supplier shall use phishing-resistant authentication methods where technically supported.

### 4. Vulnerability and Patch Management

4.1 Supplier shall maintain a documented vulnerability management process covering all systems, applications and infrastructure that Process Customer Data, including vulnerability scanning at a defined frequency.

4.2 Supplier shall define remediation timeframes based on vulnerability severity, shall remediate vulnerabilities within those timeframes, and shall prioritise vulnerabilities that are known to be actively exploited.

4.3 Supplier shall maintain a documented patch management process for operating systems, applications, and third-party libraries and dependencies, including a procedure for emergency patching, and shall apply security patches within the remediation timeframes defined under paragraph 4.2 of this Annex B.

## 5. Cryptography

5.1 Supplier shall encrypt Customer Data in transit over public and internal networks using current, industry-standard protocols, and shall disable deprecated protocol versions and weak cipher suites.

5.2 Supplier shall encrypt Customer Data at rest using industry-standard encryption algorithms, including in databases, file storage and backups, and shall apply full-disk encryption to laptops and other portable devices and media that store Customer Data.

## 6. Logging and Monitoring

6.1 Supplier shall log and monitor security-relevant events on systems that Process Customer Data, including authentication events, privileged activity, and access to Customer Data by Supplier personnel and third parties, using synchronised time sources. Supplier shall protect logs against unauthorised modification and deletion and retain them for a defined period.

## 7. Network and Infrastructure Security

7.1 Supplier shall protect networks that carry Customer Data with firewalls or equivalent controls configured to deny traffic by default, and with intrusion detection or prevention capabilities.

7.2 Supplier shall segregate production environments that Process Customer Data from corporate and non-production environments. Customer Data shall not be used in non-production environments unless it has been masked or anonymised.

## 8. Endpoint Security

8.1 Supplier shall ensure that endpoints and servers that access or Process Customer Data are centrally managed, run vendor-supported operating systems, and are protected by endpoint detection and response or equivalent anti-malware controls that are kept up to date.

## 10. Secure Software Development

10.1 Supplier shall develop and maintain software that Processes Customer Data under a documented secure software development lifecycle that includes controls to protect against the vulnerability classes in the OWASP Top 10 and the CWE/SANS Top 25 Most Dangerous Software Weaknesses.

## 11. Security Testing

11.1 Supplier shall have systems and applications that Process Customer Data penetration tested by an independent, qualified third party. Testing shall take place at a defined frequency and after significant changes. Upon request, Supplier shall provide Vizrt with a summary of the latest test results and the remediation status of findings.

## 12. Backup and Recovery

12.1 Supplier shall back up Customer Data and the systems required to Process it at a defined frequency consistent with documented recovery point objectives.

12.2 Supplier shall encrypt backups, protect them against unauthorised access, and maintain at least one backup copy that is logically or physically separated, or immutable, to protect against ransomware and destructive attacks.

12.3 Supplier shall maintain documented disaster recovery procedures with recovery point and recovery time objectives for systems that Process Customer Data, and shall test them, including the restoration of backups, at a defined frequency.

## 13. Incident Response

13.1 Supplier shall maintain a documented incident response plan that defines roles, responsibilities and escalation paths, and procedures for detection, containment, eradication, recovery and preservation of evidence, and shall test the plan at a defined frequency.

13.2 Supplier shall designate a security contact for Vizrt and shall notify Vizrt of Security Incidents in accordance with this DPA. During a Security Incident, Supplier shall provide Vizrt with regular updates and, upon closure, a written report describing the root cause, impact and remediation actions taken.

## 14. Software and Components Supplied to Vizrt

14.1 Where the Supplier delivers software, components or libraries that are incorporated into Vizrt products or deployed in Vizrt environments, the supplier shall provide a software bill of materials in an industry-standard, machine-readable format (such as SPDX or CycloneDX) upon request.

14.3 Supplier shall notify Vizrt within two (2) calendar days of becoming aware of a vulnerability affecting supplied software, giving priority to vulnerabilities known to be actively exploited, and shall provide remediation or mitigation.

**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:<br>(i) EU Regulation 2016/679 (the "**EU GDPR**");<br>(ii) EU Directive 2002/58/EC; and<br>(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;<br>in each case, as amended or superseded from time to time. |
| "**EU/UK/Swiss Restricted Transfer"** | means:<br>(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**");<br>(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<br>(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:<br>(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<br>(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:<br>(i) the Swiss Federal Act on Data Protection of 25 September 2020 and its corresponding ordinances ("**Swiss DPA**"); and<br>(ii) any other national laws in Switzerland applicable (in whole or in part) to the Processing of Personal Data;<br><br>in each case, as amended or superseded from time to time. |
| "**UK Data Protection Law**" | means:<br>(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**");<br>(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;<br>(iii) the Data Protection Act 2018 (the "**DPA 2018**"); and<br>(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;<br><br>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 Vizrt to Supplier 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 Vizrt and Supplier 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 Vizrt and Supplier as follows:

(i) the EU SCCs, completed as set out above shall apply between Vizrt and Supplier, and shall be modified by the UK Addendum (completed as set out in subclause (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 Vizrt and Supplier 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.

3.2. *Restricted transfers by Supplier:* Supplier 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 Vizrt.

## Part B: California

### 1. Application of this Part B

1.1. This Part B (California) to Annex B (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 B (California) of Annex C (Jurisdiction-Specific Requirements) and the body of the DPA, this Part B shall prevail to the extent of that conflict.

### 2. Definitions and interpretation

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

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

4.1. *Instruction and Direction*. Supplier shall use, retain, disclose, or otherwise Process Personal Data only on behalf of Vizrt and for the specific Business Purposes described in this Part B to provide the Services and in accordance with Vizrt's instructions, including as described in the Agreement. Supplier shall not Sell or Share Personal Data. Supplier shall not use, retain, disclose, or otherwise Process Personal Data outside of its business relationship with Vizrt or for any other purpose (including Supplier's Commercial Purpose) except as required or permitted by law. Supplier will inform Vizrt if, Supplier determines that it is no longer able to meet its obligations under California Data Protection Laws. Vizrt reserves the right to take reasonable and appropriate steps to (i) ensure Vizrt's Processing of Personal Data is consistent with Vizrt's obligations under California Data Protection Law and (ii) discontinue and remediate unauthorised use of Personal Data.

4.2. *No Combination of Personal Data*. Supplier will not combine Personal Data which Supplier Processes on Vizrt'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 Supplier may combine Personal Data to perform any Business Purpose permitted or required under the Agreement to perform the Services.

4.3. *Business Purposes*. Supplier 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, Supplier shall not combine the Personal Data of opted-out consumers that Supplier receives from, or on behalf of, the Business with Personal Data that Supplier 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 Supplier 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 Supplier Processes Personal Data as a Third Party under the California Data Protection Laws, the following provisions shall apply instead of Sections 4.14.3 for such Processing conducted as a Third Party: Supplier may process Personal Data only for the limited and specified purposes described in the Agreement and this DPA. Supplier 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. Supplier will promptly inform Vizrt if Supplier determines that it is no longer able to meet its obligations under California Data Protection Laws. Vizrt reserves the right to take reasonable and appropriate steps to ensure that Supplier 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.