Data Privacy and Security Addendum to Agreement

This Data Privacy and Security Addendum ("Data Protection Addendum") is entered into as of _____, 2019, between _____ ("Controller") and _____ ("Processor") (collectively, the "Parties"). This Data Protection Addendum IS PART OF THE CONTRACT DOCUMENT THAT FORMS THE CONTRACTUAL RELATIONSHIP BETWEEN CONTROLLER AND PROCESSOR, including the _____[Agreement] dated _____ and Order Form(s) and any amendments thereto (collectively, the "Agreement"), for the provision of services (the "Services") by Processor as more particularly described in the Agreement, including the Parties' agreement related to Processing of Controller Data, including Personal Data (as hereinafter defined), in accordance with the requirements of applicable Data Protection Requirements (as hereinafter defined).

This Data Protection Addendum shall not replace any rights or obligations related to Processing of Controller Data or Personal Data previously agreed to by Controller and Processor in the Agreement, but shall replace any existing data processing addendum to the Agreement unless otherwise explicitly stated herein. Capitalized terms not defined herein shall have the meanings set forth elsewhere in the Agreement. In the event of a conflict between this Data Protection Addendum and any other provision of the Agreement, this Data Protection Addendum shall control.

DATA PROTECTION ADDENDUM TERMS

In the course of providing Services to Controller pursuant to the Agreement, Processor may Process Personal Data on behalf of Controller. Processor agrees to comply with the following provisions with respect to any Personal Data submitted to Processor by or for Controller or collected and processed by or for Controller in connection with the Services.

1. DEFINITIONS

1.1. "Affiliate" means, in relation to Controller its subsidiary or holding company or any subsidiary of any such holding company, the terms "subsidiary" and "holding company" having the meanings given to them under the applicable law.

1.2. "Controller" means the natural or legal person, public authority, agency, or entity, identified in the first paragraph of this Data Protection Addendum, that determines the purposes and means of the Processing of Personal Data.

1.3. "Controller Data" means any data and information the Controller provides, generates, transfers, or makes available to Processor under the Agreement, whether in printed, electronic, or other format.

1.4. "Cybersecurity Incident" means any Indicator or combination/sequence of related Indicators that threatens or compromises the confidentiality, integrity, or availability of Controller Data or Controller information systems. This includes any potential leak, destruction, loss, alteration, unauthorized disclosure, or access to Controller Data or Controller information systems.

1.5. "Data Breach" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Controller Data or any Personal Data.

1.6. "Data Protection Requirements" means all applicable laws and regulations protecting the fundamental rights and freedoms of natural persons and their right to privacy with regard to the processing of Personal Data including, without limitation and only as applicable to Processor: (i) the Federal Trade Commission Act (15 U.S.C. §§ 41-58, as amended), (ii) the General Data Protection Regulation (GDPR); (iii) the California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 -1798.199); and any other international, national, local or regional data protection, data privacy or data security laws. It also includes, where applicable to Processor's business, in its delivery of the Services, or as otherwise required in this Data Protection Addendum, application of certain certification requirements, including but not limited to the EU-U.S. and Swiss-U.S. Privacy Shield Principles, as further described in this Data Protection Addendum.

1.7. "Data Subject" means an identified or identifiable natural person whose Personal Data is collected and hosted by Processor on behalf of Controller, as may be more fully set forth in the Data Protection Requirements, and shall be meant to include any different but similar term used in the Data Protection Requirements.

1.8. "Data Subject Right" means a Data Subject's right to access, delete, edit, export, restrict or object to Processing of the Personal Data of that Data Subject if required by Law.

1.9. “Destroy” means, with respect to Personal Data, destruction of such information through shredding, pulverizing, burning, erasure (in the case of electronic media), or other methods such that it cannot practicably be read or reconstructed.
1.10. "European Economic Area" means the member states of the European Union as well as Iceland, Liechtenstein and Norway.
1.11. “General Data Protection Regulation” or “GDPR” means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
1.12. “Indicator” means any observable, logical occurrence involving Processor’s information system or computerized operational systems that signals a possibility that a Cybersecurity Incident has occurred or is ongoing.
1.13. “Joint Controller” means a joint controller as defined by the GDPR, Article 26.
1.14. “Law” means all applicable laws, rules, statutes, decrees, decisions, orders, regulations, judgments, codes, enactments, resolutions and requirements of any government authority (federal, state, local or international) having jurisdiction.
1.15. “Order Form” means an order form, statement of work or any other documentation that reflects the work undertaken by Processor at Controller’s request and which forms a part of the Agreement.
1.16. “Personal Data” means any information, including Special Personal Data, relating to an identified or identifiable natural person (“Data Subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or society of that natural person. It may include a term similar to Personal Data but which shall have the same general meaning (for example “personal information”), where such data is submitted to the Processor as Personal Data. This information may be in paper, electronic or other form received by Processor in connection with performance of its Services and as described in the Vendor pre-screening process and related forms completed by Processor, which may be attached to this Data Protection Addendum. Personal Data includes but is not limited to a Data Subject’s name, address, contact information, credit or debit card numbers, bank account numbers or financial information, social security number, driver’s license, passport or visa information, e-mail address, user name, password, IP address, transactional information, health or disability information, image, consumer preferences, marital status, salary, occupation demographic information, information provided by the Data Subject in connection with his or her relationship with Controller. In addition, for purposes of this Data Protection Addendum, Personal Data also includes Personal Data provided by a Data Subject directly to Processor if (i) Processor was collecting such information on behalf of Controller, (ii) Data Subject provides Personal Data to a Controller-designated Processor in order to obtain the requested goods or services, but excludes all other Personal Data provided by a Data Subject directly to Controller, or (iii) such Personal Data is combined with Personal Data provided by Controller for Processing.
1.17. “Privacy Requirements” means the requirements regarding the Processing of Personal Data by Processor in connection with delivering the Services, as more fully set out in Appendix 1 hereto.
1.18. "Privacy Shield" means the EU-U.S. Privacy Shield and the Swiss-U.S. Privacy Shield self-certification programs, both operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 of July 12, 2016 (and as may be amended from time to time) and pursuant to the Swiss Federal Council pronouncement on 11 January 2017.
1.19. "Privacy Shield Principles" means the Privacy Shield Framework Principles (as supplemented by any Supplemental Principles) which may be found on the U.S. Department of Commerce website, and as may be amended, superseded or replaced from time to time.
1.20. “”Process” or “Processing” means any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as, but not limited to, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, and shall be meant to include any different but similar term used in the Data Protection Requirements and as may be more fully set out in Appendix 2 hereto.
1.21. “Processor” means a natural or legal person, public authority, agency or other body, including the entity identified in the first paragraph of this Data Protection Addendum, that Processes Personal Data on behalf of the Controller. Processor includes Joint Controllers who Process Controller Data.
1.22. “Security Specifications” means the security measures employed by Processor to protect the Personal Data in its possession in connection with delivering the Services and as more fully set out in Appendix 1 hereto.

1.23. "Special Personal Data" means any information revealing a Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, unique genetic or biometric data, health condition, sex life or sexual orientation.

1.24. "Standard Contractual Clauses" means the Standard Contractual Clauses (processors) approved by the European Commission's decision of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection. A copy of the Standard Contractual Clauses is set forth in Appendix 4 hereto.

1.25. "Sub-processor" means any processor engaged by Processor for carrying out specific processing activities on behalf of the Controller.

1.26. "Unlawful" means any violation of Law.

2. PROCESSING OF PERSONAL DATA

2.1. **Roles of the Parties**. The Parties acknowledge and agree that with regard to the Processing of Personal Data, Controller is the Controller, Processor is the Processor and that, to the extent permitted by the Data Protection Requirements, the Agreement and this Data Protection Addendum, Processor may engage Sub-processors pursuant to the requirements set forth in section 6 "Sub-processors" below. Further, each Party agrees to comply with its respective obligations under the Data Protection Requirements in relation to its Processing of the Personal Data and Processor agrees to provide all assistance reasonably required by Controller to enable Controller to take reasonable and appropriate steps to ensure that Processor effectively Processes Personal Data in a manner consistent with Controller's obligations under all the Data Protection Requirements.

2.2. **Controller's Processing of Personal Data**. Controller shall, in its use of the Services, Process Personal Data in accordance with the requirements of the Data Protection Requirements. Controller's instructions to Processor for the Processing of Personal Data shall comply with the Data Protection Requirements. Controller shall have sole responsibility for the quality, ongoing accuracy, legality and scope of Personal Data collected by Processor on Controller's behalf.

2.3. **Processor's Processing of Personal Data**. Processor shall only Process Personal Data to the extent necessary to perform the Services specified in the Agreement and only in accordance with Controller's written instructions and shall treat Personal Data as Confidential Information. In Processing Personal Data, Processor shall at all times comply with the Privacy Requirements. Controller hereby instructs Processor to Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by users in their use of the Services; and (iii) Processing to comply with other reasonable written instructions by Controller that are consistent with the terms of the Agreement. Processor acknowledges and agrees that it does not own or control the Personal Data. Further, Processor agrees that it shall, in its capacity as Processor:

2.3.1. Only carry out Processing of Personal Data on Controller's instructions, as set forth in the Agreement;

2.3.2. Provide at least the same level of protection to Personal Data as is required by this Data Protection Addendum and the Data Protection Requirements;

2.3.3. Promptly notify Controller if it determines that it can no longer meet its obligation to provide the same level of protection as is required by the Data Protection Requirements and this Data Protection Addendum, and in such event, to work with Controller to take prompt, reasonable and appropriate steps to stop and remediate any Processing until such time as the Processing meets the level of protection as is required by the Data Protection Requirements and this Data Protection Addendum;

2.3.4. Implement and maintain throughout the term of this Data Protection Addendum appropriate technical and organizational measures to protect Personal Data against unauthorized or unlawful Processing and accidental destruction or loss (including ensuring the reliability of employees), so as to allow Controller to comply with the requirement to implement appropriate technical and organizational security measures, in accordance with the Security Specifications and other applicable provisions of the Data Protection Requirements;

2.3.5. At Controller's sole election, to cease Processing Personal Data promptly if in Controller's reasonable determination, Processor is not providing the same level of protection to Personal Data as is required by the Data Protection Requirements or this Data Protection Addendum.

2.3.6. Keep or cause to be kept full and accurate records relating to all Processing of Personal Data on behalf of Controller as part of the Services ("Records");

2.3.7. Promptly refer to Controller any requests, notices or other communication from Data Subjects, any national data protection authority established in the jurisdiction of Controller, or any other law enforcement authority, for Controller to resolve;

2.3.8. Promptly inform the Controller about every inquiry, action, investigation, inspection by any data protection authorities or by judicial authorities;

2.3.9. Comply with the orders of any data protection authorities or the judicial authorities, unless Controller has promptly informed Processor of the intention of filing opposition to the orders;

2.3.10. Provide all assistance reasonably required by Controller to enable Controller to respond to, comply with or otherwise resolve any request, question or complaint made to it by a Data Subject in relation to the Processing of Personal Data associated with such Data Subject;

2.3.11. If required by the Data Protection Requirements, provide reasonable assistance to Controller with any data protection impact assessments and with any prior consultations to any supervisory authority of Controller, in each case solely in relation to processing of Personal Data, and taking into account the nature of the Processing and information available to Processor.

2.3.12. Provide all assistance reasonably required by Controller to enable Controller to respond to, comply with or otherwise resolve any request, question or complaint made to it that is received from any regulatory or data protection authority including, but not limited to, any applicable U.S., EU or Swiss regulator or data protection authorities.

2.3.13. Take all reasonable steps to ensure the reliability of any of its employees who have access to the Personal Data.

2.3.14. Appoint a Data Protection Officer, if this is legally required by the Data Protection Requirements. The Processor shall promptly notify the Controller of the appointment and the contact information of the Data Protection Officer. If not legally required, assign responsibility for compliance with this Data Protection Addendum to a designated person or group within the company. The authority and accountability of this person or group that demonstrates a privacy and/or security role must be made available to Controller on request.

2.3.15. To the extent Controller, in its use of the Processor's services, does not have the ability to correct, amend, block, or delete Personal Data, as required by the Data Protection Requirements, Processor shall comply with any commercially reasonable request by Controller to facilitate such actions to the extent Processor is legally permitted to do so. To the extent legally permitted, Controller shall be responsible for any reasonable costs arising from Processor's provision of such assistance.

2.3.16. Processor shall not direct any of its own marketing materials to any of Controller's customers without first obtaining all necessary consents to do so from the Controller in accordance with the Data Protection Requirements.

2.3.17. Processor agrees it shall not, in its capacity as Processor:

2.3.17.1. Disclose Personal Data to any third party other than i) for the purposes of complying with Data Subject access requests and Data Subject Rights in accordance with the Data Protection Requirements, as may be required by local laws and regulations, and ii) in accordance with Sections 2.3.8 to 2.3.13, as applicable, unless required by applicable law to which Processor is subject; in such a case, Processor shall notify Controller of that legal requirement before disclosing the Personal Data, unless that law prohibits such notification on important grounds of public interest; this Clause 2.3.16.1 shall be without prejudice to clause 2.3.17.2;

2.3.17.2. Notwithstanding clause 2.3.17.1 or anything else to the contrary in this Data Protection Addendum or the Agreement, Process Personal Information that is subject to the GDPR in any other way than on documented instructions from Controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by European Union or EU Member State law to which Processor is subject; in such a case, Processor shall notify Controller of that legal requirement before Processing, unless that law prohibits such notification on important grounds of public interest;

2.3.17.3. Include Personal Data in any product or service offered by Processor to third parties;

2.3.17.4. With the exception of those pre-approved subcontractors listed in Appendix 3 hereto who are engaged in the performance of the Services, share or allow access to files containing Personal Data to any third party for further Processing by that third party or its agents (except for the purposes of mere routing of Personal Data through a third party telecommunications carrier).

It is expressly agreed and understood that Processor's obligations as set forth in Sections 2.3.4, and 2.3.6 through 2.3.16.4 shall survive termination of the Agreement and shall continue in effect until such time Processor no longer has access to, hosts or retains Personal Data.

3. RIGHTS OF DATA SUBJECTS

3.1. **Data Subject Requests.** Processor shall, to the extent legally permitted, notify Controller within five (5) business days of any request received by Processor from a Data Subject for access to, correction, amendment or deletion of that individual's Personal Data. Processor shall not respond to any such Data Subject request without Controller's prior written consent except to confirm that the request has been received and relates to Controller. Processor shall provide Controller with commercially reasonable cooperation and assistance in relation to a Data Subject's request for access to that individual's Personal Data and in complying with the Data Protection Requirements for responding to Data Subject's requests, to the extent legally permitted and to the extent Controller does not have access to such Personal Data through its use of the Services. Upon receipt of written instructions from Controller, Processor shall promptly delete from its records the Personal Data of any Data Subject who has requested deletion of Personal Data and confirm the deletion in writing to Controller within two (2) business days. If legally permitted, Controller shall be responsible for any reasonable costs arising from Processor's provision of such assistance.

4. GOVERNMENT DISCLOSURE

4.1 Processor shall promptly notify Controller of any request for disclosure of Personal Data by a governmental or regulatory body or law enforcement authority (including any data protection supervisory authority) unless otherwise prohibited by law or a legally binding order of such body or authority.

5. PROCESSOR'S PERSONNEL

5.1. **Confidentiality**. Processor shall ensure that the personnel it has engaged or employed for Processing Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities with respect to its confidentiality and have executed written confidentiality agreements. Processor shall ensure that such confidentiality obligations survive the termination of the personnel engagement or employment.

5.2. **Reliability**. Processor shall take commercially reasonable steps to ensure the reliability for maintaining confidentiality of any Processor personnel engaged or employed in the Processing of Personal Data and give them the necessary operational instructions.

5.3. **Limitation of Access**. Processor shall ensure that Processor's access to Personal Data is limited to those personnel or employees who require such access to perform the Services under the Agreement.

5.4. **Data Protection Officer**. Pursuant to Section 2.3.14, as of the date of this Data Protection Addendum, the name and contact information for the appointed data protection officer is _____. Processor shall promptly notify Controller in writing if a different data protection office has been or is appointed during the term of the Agreement or this Data Protection Addendum.

6. SUB-PROCESSORS

6.1. **Appointment of Sub-processors**. Controller acknowledges and agrees that (a) Processor's affiliates and other third parties, as listed in Appendix 3 hereto, may be retained as Sub-processors; and (b) Processor may engage third-party Sub-processors in connection with the provision of the Services subject to section 6.3 below.

6.2. **Due Diligence**. Before the Sub-processor first processes Personal Data, Processor shall carry out adequate due diligence to ensure that the Sub-processor is capable of providing the level of protection for Personal Data required by this Data Protection Addendum.

6.3. **Liability**. Where a Sub-processor fails to fulfill its data protection obligations, Processor shall remain fully liable to Controller for the performance of that Sub-processor's obligations.

6.4. **Prior Information; Right to Object.** Any approved Sub-Processors as of the time of the execution of this Data Protection Addendum are listed in Appendix 3 hereto. Processor shall inform Controller in writing prior to any intended changes concerning the addition or replacement of Sub-Processors, thereby giving Controller a reasonable opportunity to object to such changes.

6.5. **Obligations to be imposed on Sub-Processors.** Where Processor engages a Sub-Processor for carrying out specific Processing activities on behalf of Controller, the same data protection obligations as set out in this Data Protection Addendum between Controller and Processor shall be imposed on that Sub-Processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organizational measures, including those Security Specifications set forth in Appendix 1 hereto, in such a manner that the Processing will meet the Data Protection Requirements.

6.6. **Right of Controller.** The Controller has the right to obtain information from the Processor, upon written request, on the substance of the contract and the implementation of the Data Protection Requirements within the sub-process relationship, where necessary by inspecting the relevant contract documents.

6.7. **Sub-processor in third country.** The provisions of this section 6 will apply as well if a Sub-processor in a third country Processes or uses the Personal Information of the Controller outside the European Economic Area. In this case the Sub-processor will enter into EU Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries approved by the European Commission.

7. SECURITY

7.1. **Controls for the Protection of Personal Data**. Processor shall maintain administrative, physical, organizational and technical safeguards for protection of the security, confidentiality and integrity of Personal Data. These safeguards may include, in accordance with Processor's certification as required by Section 7.2 below, (i) the pseudonymization or encryption of Personal Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services (iii) 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 (iv) a process of regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of Processing. Without limiting the generality of the foregoing, Processor shall implement and maintain each of the technical and organizational measures set forth in the Security Specifications in Appendix 1 hereto. Processor shall regularly monitor compliance with these safeguards. Processor shall not materially decrease the overall security of the Services during the term of the Agreement.

7.2. **Vendor Pre-Screening.** Processor shall have completed Controller's Vendor pre-screening, pre-qualification, or such other process as Controller may require, including completion of all forms requested by Controller, and shall have certified that the information provided therein is true, accurate and complete. Processor shall promptly notify Controller in writing should it determine that any information it provided in the pre-screening process is inaccurate or incomplete in any material respect.

7.3. **Network Security.** In the event that access to Controller systems is required in order to fulfill its services, Processor is responsible for all use of and access to the Controller network system by its employees and permitted subcontractors, and Controller maintains the right to monitor all user activity and revoke access due to noncompliance to its security policies. It is agreed by Processor that the Processor network security policy will only allow authorized users access, and will deny all unauthorized access.

7.4. **Third-Party Certifications and Audits**. With respect to third-party certifications and audits obtained by Processor as set forth hereinabove and in the Security Specifications, upon Controller's written request, at reasonable intervals, Processor shall provide a copy of Processor's then most recent third-party audit or certification, as applicable, or any summaries thereof, that Processor generally makes available to its clients at the time of such request.

7.5. **Controller's Right to Audit.** Processor shall allow for and cooperate in audits by Controller or Controller's designated third party with respect to Processor's compliance with this Data Protection Addendum, including audits of Processor's processing facilities at least once annually and upon the occurrence of any Security Incident or Data Breach. Controller shall provide at least thirty (30) days' advance notice for any scheduled audit and as much advance notice as Controller in its sole discretion deems reasonably appropriate with respect to audits arising out of a Cybersecurity Incident or Data Breach. Processor shall make available to Controller or its designee all information necessary to demonstrate compliance with the Data Protection Requirements.

8. SECURITY INCIDENT OR DATA BREACH MANAGEMENT AND NOTIFICATION

8.1. **Cybersecurity Incident or Data Breach Notification**. If Processor becomes aware of, or has reason to believe or suspect, that there has been a Cybersecurity Incident or Data Breach, Processor shall, promptly, and in any event within twenty-four (24) hours, notify Controller in writing directed to privacy@carnival.com [*brand to insert brand-specific email address*] with sufficient information to allow Controller to meet any obligations to report such a Cybersecurity Incident or Data Breach under the Data Protection Requirements. Such notification shall at a minimum (i) describe the nature of the Cybersecurity Incident or Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned; (ii) identify the name of the Processor's data protection officer or other relevant contact person(s) from whom more information about the Cybersecurity Incident or Data Breach may be obtained; (iii) describe the likely consequences of the Cybersecurity Incident or Data Breach; and (iv) describe the measures taken or proposed to be taken to address the Cybersecurity Incident or Data Breach. If a Cybersecurity Incident Data Breach occurs, Processor shall not inform any third party without first obtaining Controller's express consent, unless notification is required by the Data Protection Requirements to which Processor is subject, in which case Processor shall to the extent permitted by the Data Protection

Requirements, inform Controller of that requirement, provide a copy of the proposed notification and consider any comments made by Controller before notifying of the Cybersecurity Incident or Data Breach.

8.2. **Cybersecurity Incident or Data Breach Response**. To the extent such Cybersecurity Incident or Data Breach is contributed to, or caused by, a violation of the requirements of this Data Protection Addendum by Processor, Processor shall: (i) fully cooperate with Controller or anyone acting on its behalf (and with any law enforcement or regulatory official) to investigate and resolve the Cybersecurity Incident or Data Breach; (ii) make reasonable efforts to identify and remediate the cause of such Cybersecurity Incident or Data Breach; and (iii) keep Controller up-to-date about developments in connection with the Cybersecurity Incident or Data Breach.

8.3. **Option to Terminate the Agreement**. Controller may terminate the Agreement immediately and without recourse to the courts, and without further liability or obligation on its part under the Agreement, if any Personal Data is lost, corrupted or stolen as a consequence of a Cybersecurity Incident or Data Breach arising out of any action or inaction of the Processor.

9. RETURN AND DELETION OF PERSONAL DATA

9.1. Upon the termination of the Agreement or earlier if demanded by Controller, Processor shall immediately return to Controller all Personal Data in its possession or constructive possession, custody or control, including any copies or reproductions thereof. Notwithstanding the foregoing, Controller may provide written notice to Processor that it is required to Destroy such Personal Data, in which case Processor shall do so immediately at its sole cost and expense. Processor shall promptly thereafter certify in writing to Controller that it has returned or Destroyed (as the case may be) the Personal Data and has not retained copies of any Personal Data. In any event, during the term of the Agreement, Controller shall notify Processor of all Personal Data that is no longer in use or required by the Processor and obtain from Processor written confirmation of the personal data being deleted and purged from the Processors online systems, including backup and recovery systems and all archival storage media.

10. OBJECTIVE AND ADDITIONAL TERMS

10.1. **Objective and Duration**. The objective of Processing of Personal Data by Processor is the performance of the Services pursuant to the Agreement.

10.2. **Instructions**. This Data Protection Addendum and the Agreement are Controller's complete and final instructions to Processor for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately, always in accordance with the Data Protection Requirements.

10.3. **Cross Border Transfers.** The Standard Contractual Clauses will apply to the processing of Personal Information subject to the GDPR if the Processing carried out by Processor under the Agreement occurs outside the European Union. In the event of any conflict or inconsistency between this Data Protection Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

11. PRIVACY SHIELD *[Check here ____if applicable]*

11.1. **Self-certification**. Processor has self-certified under the Privacy Shield so as to ensure that adequate safeguards are adduced with respect to the protection of privacy and fundamental rights and freedoms of individuals located in the European Economic Area and Switzerland for the transfer of any Personal Data by Controller to Processor. Accordingly, Processor agrees to process any such Personal Data in compliance with the Privacy Shield Principles.

11.2. **Sub-processing**. Processor agrees to remain responsible for any Personal Data received from Controller under Privacy Shield which is subsequently transferred to Sub-processor.

11.3. **Conflict**. In the event of any conflict or inconsistency between this Data Protection Addendum and the Privacy Shield Principles, the Privacy Shield Principles shall prevail.

11.4 **Adequacy**. In the event that during the term of the Agreement Processor is no longer self-certified under Privacy Shield, Processor shall promptly notify Controller and continue to process any Personal Data previously transferred under the Privacy Shield in accordance with the Privacy Shield Principles. In addition, Processor shall do all such things as are required to ensure adequate protection for Personal Data in accordance with the Data Protection Requirements. Such measures may include ensuring that Processor and Controller enter into the Standard Contractual Clauses approved by the European Commission or implement any other data export adequacy measure permitted by the Data Protection Requirements.

12. INDEMNITY AND INJUNCTIVE RELIEF

12.1. Processor shall indemnify, defend and hold harmless Controller and its affiliates and their shareholders, officers, directors, and employees, from, against and in respect of any and all losses, liabilities, damages, claims, causes of action, penalties, fines, charges, liens, costs and expenses (including, without limitation, attorneys' fees and paraprofessionals' fees) arising out of or related to a Cybersecurity Incident or Data Breach, including, but not limited to, the misuse, unauthorized access, mishandling, theft by or theft from the Processor or its employees, independent vendors and/or agents (or any person conspiring with the any of the foregoing) of any Personal Data. Processor agrees that any Cybersecurity Incident or Data Breach, including, but not limited to, unauthorized use or disclosure of Personal Data may cause immediate and irreparable harm to Controller for which money damages may not constitute an adequate remedy. In that event, Processor agrees that injunctive relief may be warranted in addition to any other remedies Controller may have. In addition, Processor agrees to take all steps at its own expense reasonably requested by Controller to limit, stop or otherwise remedy a Cybersecurity Incident or Data Breach such as the actual or suspected misappropriation, disclosure or use of Personal Data.

13. CONFLICT IN TERMS

13.1 In the event that a conflict exists between and term or provision of this Data Protection Addendum and the Agreement, the terms and provisions of this Data Protection Addendum shall control unless specifically provided otherwise in a written documents signed by Controller and Processor.

14. SURVIVAL OF OBLIGATIONS

14.1 Processor's responsibilities under this Data Protection Addendum shall continue beyond the length or term of the Agreement until the later of (i) such time that all Personal Data is satisfactorily deleted from all systems including backup tapes owned or under control of the Processor and Destroyed, or (ii) completion of any audits, investigations or other matters that continue beyond the expiration or termination of the underlying Agreement, it being understood that the obligations under Section 12 hereof shall continue indefinitely.

15. LEGAL EFFECT

15.1 This Data Protection Addendum shall only become legally binding between Controller and Processor when executed in full.

CONTROLLER		**PROCESSOR**	
BY:	_____	BY:	_____
NAME:	_____	NAME:	_____
TITLE:	_____	TITLE:	_____
DATE:	_____	DATE:	_____

APPENDIX 1 TO THE DATA PRIVACY AND SECURITY ADDENDUM

In addition to Processor's information security and privacy policy, Processor employs those of the following technical and organizational measures (Security Specifications) necessary to safeguard Controller Data and Personal Data within the Services, as determined by Controller based on Processor's responses to Controller's Vendor pre-screening process.

Security Specifications

1.	Governance and Policies	• Maintain written information security policies and procedures and incident response programs required to comply at a minimum with (i) all applicable Data Protection Laws and (ii) generally accepted industry standards for data protection including ISO 27001/2. • Test its information security procedures and incident response programs at least annually and retain written reports of the test results • Assign personnel with responsibility for the determination, review and implementation of security policies and measures.
2.	Network level security	Measures employed to prevent unauthorized access to the processing environment and thwart attackers from breaching the Processor's network. Security measures may include technology in the following categories • Perimeter next generation firewalls • Denial of Service protection • Data loss prevention • Advanced Persistent Threat detection/prevention • Mobile device management • Web application security
3.	Intrusion, anti-virus and anti-malware	Defenses deployed on systems used to process personal data. • Implement patch management procedures that prioritize security patches for systems used to process Carnival personal or confidential information. • Maintain logs of all auditing, monitoring and security activity for a period of 120 days in a secure environment • Employ anti-virus, endpoint protection and response capabilities
4.	**Cloud hosting**	Where any part of the Services is supported by cloud hosting, Counterparty will comply with the latest version of the Cloud Security Alliance Cloud Controls Matrix (available here: https://cloudsecurityalliance.org/) or other substantially similar assurance agreed with CARNIVAL. Counterparty must be able to demonstrate the established commonly accepted data protection and privacy control objectives.

5.	**Physical Site Security** **and** **Device hardening**	• Electronic access card reading system • Management of keys/documentation of key holders • Palisade fencing • Solid reinforced concrete exterior to building with no windows. • 24x7x365 staffed security guards • Security service, front desk with required sign in for all visitors • Burglar alarm system • Internal and external infrared pan, tilt, zoom CCTV Monitored building management system • Biometric scanners • Man traps • Remove unused software and services from devices used to Process Personal Information. • Default passwords that are provided by hardware and software producers shall not be used. • Mandate and ensure the use of system enforced strong passwords in accordance with leading industry practices on all systems hosting, storing, processing, or that have or control access to CARNIVAL's information and • Passwords and access credentials are kept confidential and not shared among personnel.
6.	**Access control**	Measures taken for preventing data processing systems from being used without authorization. • Personal and individual user log-in when entering the system and/or the corporate network • Password procedures minimum of 8 characters, with one upper case, lower case, and digit. If the user account has five invalid logon attempts, the account will be locked out. All passwords expire after 90 days. Upon verification of the username and password, the application uses session-based token authentication. • Remote access for maintenance requires two-factor authentication • Automated screen locks after a defined period of inactivity • Password protected screen savers • All passwords are electronically documented and protected against unauthorized access through encryption • User accounts are audited twice per year.
7.	Virtual access control.	Measures taken to ensure that persons entitled to use a data processing system have access only to Confidential or Personal Data to which they have a right of access, and that Personal Data cannot be read, copied, modified or removed without authorizations in the course of processing or use and after storage • User authentication is based on username and strong password • Data are stored encrypted at rest • All transactional records contain identifiers to distinguish client records • System processing uses a role-based mechanism to tailor data access to specific users and roles • Data access, insert, and modification are logged • ISO certifications and/or Third Party Independent audit reports are maintained at the primary data center

8.	Cardholder data processing	When processing or accessing cardholder data on Controller's behalf, processor must adhere to the applicable credit card handling standards per card issuer. Processor must be compliant with Payment Card Industry Data Services Standard ("PCI-DSS") and will provide proof of compliance annually.
9.	Transmission control	Measures taken to ensure that Personal Data cannot be read, copied, modified or removed without authorization dui having electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities is envisaged. • All data are encrypted in flight using the latest secured transmission protocols Transport Layer Security (TLS) 1.1 or above • Access to reports is logged • Backup media are encrypted • Removable storage is not used
10.	Input control measures	Taken to ensure that it is possible to check and establish whether and by whom Personal Data have been entered into data processing systems, modified or removed. • Record entry is restricted to a defined set of roles • All entry is date/time stamped and includes identifiers for entering party • Firewalls and intrusion prevention systems are in place to prevent unauthorized access
11.	Assignment control	Employed to ensure that, in the case of commissioned processing of Personal Data, the data are processed strictly in accordance with the instructions of the principal. • Confidentiality agreements are in place for all individuals with data access • Training is conducted during onboarding and on a regular basis • No third parties used for the processing of data other than as described in this Agreement • Privacy policy describes rights and obligations of agent and principal
12.	Availability control	Measures taken to ensure that Personal Data are protected from accidental destruction or loss. • Systems employ redundancies such as RAID arrays and redundant equipment • Backups are stored in alternate location from primary processing • Multiple air conditioning units are installed to provide redundant capacity in an N+1 configuration. • High sensitivity smoke detection, and Argonite gas suppression • Multiple firewall layers and virus protection on all servers • UPS backed by N+1 generators • Diverse fiber routing and multiple carriers
13.	Separation control	Measures taken to ensure that Personal Data collected for different purposes can be processed separately. • Three-tier systems are used to physically separate presentation, business processing and storage • Controller data are stored in separate databases or in logically separate architectures • Separation of duties is used internally to ensure functions pass through change control processes • Discrete development, staging and production environments are maintained. • All routing of data for processing is controlled through automated rules engines. • Computing and storage is on equipment owned by Processor

14.	Communications	Promptly communicate Investigation results from incident response to Carnival. • Systems and processes are in place to communicate incident and response investigation results • *Contact privacy@carnival.com [brand to replace with brand-specific email address] to inform Carnival.*

Processor also maintains the following procedures and documentation (Privacy and Evidence of Compliance Requirements):

Privacy and Evidence of Compliance Requirements

	Privacy Requirement	**Evidence of Compliance**
1.	Process Personal Data only in accordance with Controller's documented instructions, including with regard to transfers of Personal Data to a third country or an international organization, unless required to do so by Law; in such a case, the Processor shall inform the Controller of that legal requirement before Processing, unless that Law prohibits such information on important grounds of public interest.	Documented evidence of instructions as set out in the Agreement (e.g. contract, statement of work or purchase order), or captured as part of an electronic system used in performing the services required under the Agreement.
2.	Processor must use the appropriate Carnival brand Privacy Statement when collecting Personal Data on Controller's behalf. The privacy notice must be obvious and available to Data Subjects to help them decide whether to submit their Personal Data to Processor. Contact Privacy@carnival.com [*brand to replace with brand-specific email address]* for access to the correct notices.	Processor uses a fwdlink to the current, published Carnival brand Privacy Statement. The Privacy Statement is posted in any context where a user's Personal Data will be collected. If applicable, an offline version is available and is provided prior to data collection. Any offline Privacy Statements used are the latest, published version and are dated properly. For employee services, the appropriate employee notice is used.
3.	When collecting Personal Data via a live or recorded voice call, Processor must be prepared to discuss the applicable data collection, handling, use, and retention practices with Data Subjects.	Documented evidence of a script for voice recordings that includes how Personal Data is Processed, and includes collection, use and retention.
4.	Processors that create and manage Controller websites and/or applications must provide Data Subjects with transparent notice and choice regarding the use of cookies. Processors that create and manage Controller websites and/or applications must ensure that cookie use aligns with commitments in the Controller's Privacy Statement and local legal requirements such as rules established by the EU. For purposes of these Privacy Requirements, cookies are small text files stored on devices by websites and/or applications that contain information used to recognize a Data Subject or a device.	The purpose of each cookie must be documented and must inform as to the type of cookie implemented. ▪ Documented evidence that persistent cookies are not used when session cookies will suffice. ▪ Documented evidence that when persistent cookies are used, they do not have an expiration date that exceeds 2 years after a user has visited the site. For EU users, the expiration date for a persistent cookie must not exceed 13 months. Validate compliance with EU Laws as applicable, such as, use of the labelling convention, "Privacy & Cookies" for the privacy statement, and secure affirmative user consent before use of cookies for "non-essential" purposes such as advertising.
5.	Processor must monitor the collection of Carnival Personal	Processor can provide documentation

	Data to ensure that the only data collected is that required to perform the services required under the Agreement.	that shows the Carnival Personal and/or Confidential Data collected is needed to perform the services required under the Agreement.
6.	If Processor collects Personal Data from third parties on behalf of the Controller, Processor must validate that the third-party data protection policies and practices are consistent with Processor's Agreement with Controller.	Processor can provide documentation of due diligence performed regarding the third party's data protection policies and practices.
7.	Where Processor relies on consent as its legal basis for Processing data, Processor must obtain and record a Data Subject's consent for all of its Processing activities (including any new and updated Processing activities) prior to collecting that Data Subject's Personal Data.	Processor can demonstrate how a Data Subject provides consent for a Processing activity and that the scope of the consent covers all of Processor's Processing activities with respect to that Data Subject's Personal Data. Processor can demonstrate how a Data Subject withdraws consent for a Processing activity. Processor can demonstrate how preferences are checked prior to launch of a new Processing activity. Processor monitors effectiveness of preference management to ensure the timeframe to honor a preference change is the most restrictive local legal requirement that applies. Note: Evidence can be user interaction screenshots; experimentation with the service or an opportunity to view technical documentation.
8.	Before collecting sensitive Personal Data (data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation) the necessity for collecting that Personal Data must be documented in an executed Processing Agreement with Controller.	The necessity of collecting sensitive Personal Data is noted in the executed Agreement with Controller.
9.	Ensure that Personal Data is retained for no longer than necessary to Perform the services required under the Agreement, unless continued retention of the Personal Data is required by Law.	Processor supplies Controller with a certificate of compliance signed by an officer of the Processor that it complies with documented retention policies or retention requirements specified by Controller in the Agreement (e.g., statement of work, purchase order).
10.	Ensure that, at Controller's sole discretion, Personal Data in Processor's possession or under its control is returned to Controller or Destroyed upon completion of performance of the Agreement or upon Controller's request.	Processor maintains a record of disposition of Personal Data (this can include returning Data to Controller for destruction). If Controller requests Processor Destroy Personal Data, Processor provides a certificate of destruction signed by an officer of the Processor certifying that the Personal Data has been Destroyed.
11.	Assist Controller, through appropriate technical and	Documented evidences that processes

	organizational measures, insofar as possible, to fulfill its obligations to respond to requests for Data Subjects seeking to exercise their Data Subject Rights.	and procedures are in place to support execution of Data Subject Rights.
12.	Respond to all Data Subject Rights requests without undue delay.	Documented evidence that Processor conducts periodic tests to ensure it can support Data Subject Rights.
13.	Unless otherwise directed, Processor will refer all Data Subjects who contact Processor directly to Controller using Privacy@carnival.com [*brand to replace with brand-specific email address]* to exercise their Data Subject Rights. Processor will communicate to the Data Subject the steps that person must take to gain access to or otherwise exercise their rights vis-à-vis their Personal Data.	Documented evidence that Processor communicates the steps to be taken to access the Personal Data, as well the methods available to update that data including referring the Data Subject to Privacy@carnival.com [*brand to replace with brand-specific email address]*.
14.	When responding directly to the Data Subject, validate the identity of the Data Subject making the request.	Processor has documented the method used to identify Data Subjects.
15.	Once a Data Subject has been authenticated, the Processor must: Determine whether it holds or controls Personal Data, including Carnival Personal Data, about that Data Subject; • Make a reasonable effort to locate the Personal Data and Carnival Personal Data requested and keep sufficient records to demonstrate that a reasonable search was made; • Record the date and time of Data Subject Rights requests and the actions taken by Processor in response to such requests. Provide records of Data Subject requests to Controller upon request. • For requests to obtain a copy of Personal Data, provide the Personal Data to the Data Subject in an appropriate printed, electronic or verbal format. • If their request is denied, at Controller's direction, provide the Data Subject with a written explanation that is consistent with any relevant instructions previously provided by Controller. • Processor must take reasonable precautions to ensure that Personal Data released to a Data Subject cannot be used to identify another person. • If a Data Subject and Processor disagree about whether Personal Data is complete and accurate, Processor must escalate the issue to Controller at Privacy@carnival.com[*brand to replace with brand-specific email address]* and cooperate with Controller as necessary to resolve the issue	• Processor has procedures in place to establish whether Personal Data is being held. • Processor maintains a record demonstrating the steps taken to meet Data Subject Right requests. The documentation includes date and time of the request, actions taken to respond to the request, and record of when Controller was informed. • _Processor maintains records of requests for access and documents changes made to Personal Data. • Processor supplies Personal Data to the Data Subject in a format that is understandable and in a form convenient to the Data Subject and Processor. • Document instances where requests are denied and retain evidence of Controller review and approval • Controller must demonstrate that reasonable precautions are taken so that another person cannot be identified from the information released (e.g., cannot photocopy the entire page of data when requested Personal Data for a Data Subject only appears on one line). • Processor documents instances of disagreement and escalates issue to Controller.
16.	If Processor intends to use a Sub-processor to Process Personal Data, including Carnival Personal Data, Processor must: • Obtain Controller's express written consent prior to subcontracting services or making any changes concerning the addition or replacement of Sub-processors; • Document the nature and extent of Personal Data, sub-Processed by Sub-processors, ensuring that the information collected is required to perform services	• Validate that Personal Data is Processed only by companies known to Controller as required in the Agreement with Controller (e.g., statement of work, addendum, purchase order); • Controller maintains documentation concerning the Personal Data disclosed or transferred to Sub-processors. • Demonstrate how a Data Subject preference is utilized by Sub-processors.

	required under the Agreement; • Ensure Sub-processor uses Personal Data, in accordance with a Data Subject's stated contact preferences; • Limit the Sub-processor's Processing of Personal Data to those purposes necessary to fulfill the Processor's services required under the Agreement; • Review complaints for indications of any unauthorized or Unlawful Processing of Personal Data; • Notify Controller promptly upon learning that a Sub-processor has Processed Personal Data for any purpose other than those related to the services required to be performed under the Agreement; • Promptly take actions to mitigate any actual or potential harm caused by a Sub-processor's unauthorized or Unlawful Processing of Personal Data.	Provide supporting documentation that includes the timeframe for a Sub-processor to honor a preference change. • Processor can provide documentation that shows the Personal Data, provided to a Sub-processor is needed to perform the services required under the Agreement. • Processor can demonstrate systems and processes are in place to address complaints concerning unauthorized use or disclosure of Personal Data, by a Sub-processor. • Processor has provided the instruction and means for a Sub-processor to report the misuse of Personal Data. • Processor can demonstrate it has a plan and procedures in place should the misuse of Personal Data, by a Sub-processor occurs.

APPENDIX 2 DATA PRIVACY AND SECURITY ADDENDUM

Controller
Controller is the legal entity that has executed this Data Protection Addendum.

Processor
Processor is a _____.

Data subjects
Controller has instructed Processor to collect and host certain information as may be submitted in the course of _____.

Categories of data
The Personal Data processed concern the following categories of data as well as any other data and data categories that match the definition of "Personal Data" as set forth in this Data Protection Addendum incorporating this Appendix 2: _____

Special categories of data (if appropriate) as well as any other data and data categories that match the definition of "Personal Data" as set forth in this Data Protection Addendum incorporating this Appendix 2:
_____

Processing operations
The Personal Data transferred will be processed by Data Processor as more fully set forth in the Agreement.

APPENDIX 3 TO THE DATA PRIVACY AND SECURITY ADDENDUM

Approved Subcontractors

Hosting Facilities (where data is stored):

_____

Sub-contractors used for interpretation and translation services:

_____

Affiliates:

_____

APPENDIX 4 TO THE DATA PRIVACY AND SECURITY ADDENDUM

Standard Contractual Clauses (Processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organization: _____

Address: _____

Tel. _____;

Fax _____;

e-mail: _____

Other information needed to identify the organization:

_____

(the data **exporter**)

And

Name of the data importing organization: _____

Address: _____

Tel. _____;

fax _____;

e-mail: _____

Other information needed to identify the organization:

_____

(the data **importer**)

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a)'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1);

(b) 'the data exporter' means the controller who transfers the personal data;

(c)'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d)'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e)'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f)'technical and organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1.The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2.The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4.The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a)that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b)that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c)that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;

(d)that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security

appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer (2)

The data importer agrees and warrants:

(a)to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b)that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c)that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;

(d)that it will promptly notify the data exporter about:

(i)any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorized access; and

(iii)any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

(e)to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f)at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g)to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing,

unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely _____.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses (3). Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely …
4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

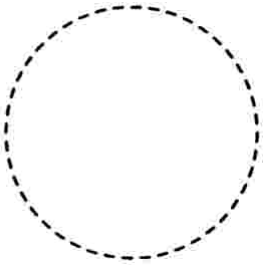
On behalf of the data exporter:

Name (written out in full): _____

Position: _____

Address: _____

Other information necessary in order for the contract to be binding (if any):

	Signature:

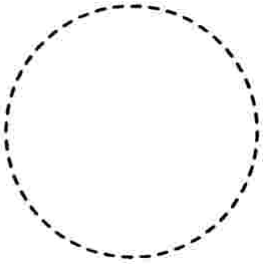
On behalf of the data importer:

Name (written out in full): _____

Position: _____

Address: _____

Other information necessary in order for the contract to be binding (if any):

	Signature:

(1) Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

(2) Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(3) This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

_____

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

_____

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

_____

Categories of data

The personal data transferred concern the following categories of data (please specify):

_____

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

_____

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

_____

DATA EXPORTER

Name: _____

Authorized Signature: _____

DATA IMPORTER

Name: _____

Authorized Signature: _____

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

_____

_____

ILLUSTRATIVE INDEMNIFICATION CLAUSE (OPTIONAL)

Liability

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

(a) the data exporter promptly notifying the data importer of a claim; and

(b) the data importer being given the possibility to cooperate with the data exporter in the defense and settlement of the claim (1).

(1) Paragraph on liabilities is optional.