Data Privacy and Security Addendum to Agreement
[Controller/Processor-Attachment to Agreement]

This Data Privacy and Security Addendum ("Data Protection Addendum") is incorporated into and made a part of the agreement to which it is attached, including any amendments thereto (collectively, the "Agreement"), for the provision of services, products and/or deliverables (collectively with respect to this Data Protection Addendum, the "Services") as more particularly described in the Agreement. For the purpose of this Data Protection Addendum, the "Controller", as defined below, shall be Carnival Corporation, Carnival plc, or one or more of its operating companies, divisions or Affiliates, as applicable, and the "Processor" shall be the third party(ies) who have entered into the Agreement.

This Data Protection Addendum supplements and 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.

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 Personal Data submitted to Processor by or for Controller or collected and processed by or for Controller in connection with the Services. The following provisions do NOT apply to Personal Data received, obtained or processed by Processor on its own behalf or on behalf of a Controller other than the Controller identified in the first paragraph of this Data Protection Addendum.

1. DEFINITIONS

1.1. "Affiliate" means, either Party's 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. A Controller is also a "business" as such term is defined under the CCPA.

1.3. "Controller Data" means any data and information the Controller (including Controller's authorized users of the Services) 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) (the "CCPA"); (iv) the UK GDPR, and (v) any other applicable international, national, local or regional data protection, data privacy or data security laws each as may be amended, replaced, supplemented or superseded from time to time. 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 as further described in this Data Protection Addendum.

1.7. "Data Subject" means an identified or identifiable natural person (i.e. 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) whose Personal Data is Processed by Processor, 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 and regulations of any government authority (US federal, state, provincial, local or international) having jurisdiction whether designated a rule, statute, decree, decision, order, judgments, codes, enactments, resolutions or requirements.

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 Sensitive Personal Data, submitted to Processor by or for Controller (including Controller’s authorized users of the Services) or collected and Processed by Processor for Controller in connection with the Services, relating to a Data Subject from which, or in combination or linked with other information, the identity of the individual can reasonably be ascertained. 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 or other identification number, driver’s license, passport or visa information, e-mail address, user name, password, IP address, location data, transactional information, health or disability information, image, voice, 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 the Security Specifications.

1.18. “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 1 hereto.

1.19. “Processor” means the natural or legal person, public authority, agency or other body identified in the first paragraph of this Data Protection Addendum that Processes Personal Data. Processor includes Joint Controllers who Process Controller Data.

1.20. “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 here: https://www.carnivalcorp.com/vendors-suppliers/third-party-portal the terms of which are incorporated herein by this reference.

1.21. “Sensitive Personal Data” means any special category of information or data revealing a Data Subject’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, unique genetic

or biometric data, mental or physical health condition, marital status, immigration status, sex life or sexual orientation, or data relating to criminal convictions and offenses.

1.22. "Standard Contractual Clauses" means the Standard Contractual Clauses approved by the European Commission's implementing decision 2021/914 of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April, 2016. A copy of the Standard Contractual Clauses is set forth in Appendix 3 hereto if the Parties have checked the box in Section 2.4 regarding the applicability of the GDPR to the Processing of Personal Data in connection with the Services.

1.23. "Sub-processor" means any processor engaged by Processor for carrying out specific Processing activities.

1.24. "UK GDPR" means The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 as supplemented by the Data Protection Act 2018.

1.25. "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 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 this Data Protection Addendum 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, this Data Protection Addendum, 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, have any proprietary or intellectual property interest in, or control the Personal Data, whether anonymized or not. Further, Processor agrees that it shall, in its capacity as Processor in Processing Personal Data:

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

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. Immediately 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 as part of the Services ("Records");

2.3.7. Promptly refer to Controller any requests, notices or other communication relating to Personal Data 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. If permitted by the applicable Data Protection Requirements, promptly inform the Controller about (i) any legally binding request, which may include an inquiry, action, investigation, or inspection, by any data protection authorities or by judicial authorities relating to Personal Data, or (ii) on becoming aware of any direct access by public authorities to Personal Data, including at regular intervals in either case, as much relevant information as possible as soon as possible;

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 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 relating to Personal Data made to it that is received from any regulatory or data protection authority including, but not limited to, any applicable U.S., EU, UK, Canadian, Bermuda, Bahamas, Mexico, Peoples Republic of China, New Zealand, Japanese, South African, or Swiss regulator or data protection authorities or those of any political subdivision thereof.

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.

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 2.3.7 to 2.3.12, 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 Section 2.3.17.1 shall be without prejudice to Section 2.3.17.2;

2.3.17.2. Notwithstanding Section 2.3.17.1 or anything else to the contrary in this Data Protection Addendum or the Agreement, Process Personal Data 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 nor sell, transfer, or otherwise disclose any Personal Data that has been anonymized to any third party, nor aggregate Controller's Personal Data, or any part of it, into a larger data set with other personal data whether anonymized or not except only as necessary to provide the Services;

2.3.17.4. With the exception of those pre-approved subcontractors listed in Appendix 2 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).

2.4. **Applicability of the GDPR. BY CHECKING THIS BOX ☐, THE PARTIES AGREE THAT PURSUANT TO ARTICLE 3 THEREOF, THE GDPR WILL GOVERN THE PROCESSING OF PERSONAL DATA IN CONNECTION WITH THE SERVICES AS SET FORTH IN THE AGREEMENT**, and, accordingly, the Parties further agree to execute and to be bound by the provisions of the Standard Contractual Clauses attached hereto as Appendix 3 the terms of which are incorporated herein by this reference. **THE PARTIES FURTHER AGREE THAT OPTION (1 ☐ OR2 ☐) OF CLAUSE 19(a) OF THE STANDARD CONTRACTUAL CLAUSES WILL APPLY AND THAT THE OPTION IN CLAUSE 11(a) WILL ☐ OR WILL NOT ☐ APPLY.** The following map will direct to the content of each respective Annex to the Standard Contractual Clauses:

Annex IB - Appendix 1
Annex II – Security Specifications
Annex III – Appendix 2

3. RIGHTS OF DATA SUBJECTS

3.1. **Data Subject Requests.** Processor shall promptly, notify Controller of any request received by Processor from a Data Subject whose Personal Data is being Processed 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, and where possible, the Data Subject (with the assistance of Controller, if necessary) of any request for disclosure of Personal Data by a governmental or regulatory body or law enforcement authority (including any data protection supervisory authority) or direct access to Personal Data by public authorities 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 _____, _____(PHONE), _____(EMAIL).** 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 2 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 2 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, 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 measures substantially similar to the Security Specifications, 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 as between Processor and Sub-Processor, where necessary by inspecting the relevant contract documents.

6.7. **Sub-processor in third country.** If the Parties have checked the box in Section 2.4, the provisions of this Section 6 will apply as well if a Sub-processor in a third country Processes or uses the Personal Data of the Controller outside the European Economic Area, Switzerland, or the United Kingdom. In this case the Sub-processor will enter into the Standard Contractual Clauses or utilize the Docking Clause provisions in Clause 7 of the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries approved by the European Commission with an adequacy decision pursuant to Article 45.

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 being Processed. 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, in addition to Processor's information security and privacy policy, Processor shall implement and maintain each of the applicable technical and organizational measures set forth in the Security Specifications as determined by Controller, based on Processor's responses to Controller's Vendor pre-screening process in Section 7.2, as are necessary to safeguard Controller Data, including Personal Data within the Services. 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 Sub-processor, 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. Processor represents and warrants that in accessing Controller systems, Processor, its employees, or permitted Sub-processor will not run any process, audit, or the like, that collects, retrieves, extracts or otherwise provides access to Controller's data, system information, or the like without Controller's prior written consent except solely to the extent required to provide the Services. Processor further represents and warrants that in accessing Controller systems, no computer instructions, circuitry or other technological means will be introduced into Controller systems the purpose of which or effect is to disrupt, damage, extract information from or interfere with Controller's computers, communications facilities or equipment and their use ("Harmful Code"), and Processor shall prevent the introduction of such Harmful Code in accessing Controller systems or into its Services prior to delivery to Customer. "Harmful Code" includes, without limitation, any code containing viruses, Trojan horses, worms or like destructive code or code that self-replicates, or cryptocurrency mining tools.

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 with respect to Personal Data, Processor shall, without undue delay, and in any event within forty-eight (48) hours, notify Controller in writing directed to privacy@carnival.com 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 and to the extent known by Processor at the time but with regular timely updates (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 and as allowed under applicable law. Until the Personal Data is deleted or returned, Processor shall continue to ensure compliance with the provisions of this Data Protection Addendum. 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 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 Data 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. INDEMNITY AND INJUNCTIVE RELIEF

11.1. In addition to any indemnification obligations set forth in the Agreement, Processor shall indemnify, defend, and hold harmless Controller and its Affiliates and their respective shareholders, officers, directors, contractors, representatives, and employees, from, against and in respect of any losses, liabilities, damages, judgements, claims, causes of action, penalties, assessments, fines, charges, liens, costs and expenses (including, without limitation, reasonable attorneys' fees and paraprofessionals' fees, notification and mitigation costs, and court costs) 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.

12. CONFLICT IN TERMS

12.1 In the event that a conflict exists between any term or provision of this Data Protection Addendum and the Agreement, the terms and provisions of this Data Protection Addendum shall control, solely with respect to the Processing of Controller Data and Personal Data, unless specifically provided otherwise in a written document signed by Controller and Processor.

13. SURVIVAL OF OBLIGATIONS

13.1 Processor's responsibilities under this Data Protection Addendum, including, without limitation Sections 2.3.2 - 2.3.4. 2.3.6 - 2.3.10, 2.3.12, 2.3.13, 2.3.17, and 2.4 (if applicable) 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 indemnity obligations under Section11 hereof shall continue indefinitely.

14. LEGAL EFFECT

14.1 This Data Protection Addendum shall only become legally binding between Controller and Processor when the Agreement and, if applicable, the Standard Contractual Clauses are executed in full.

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

APPENDIX 1 DATA PRIVACY AND SECURITY ADDENDUM

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

Processor
Processor is a _____. *(describe the vendor, please be specific)*

Data subjects
Controller has instructed Processor to collect and host certain information as may be submitted in the course of _____. *(describe the work to be done by the vendor under the terms of the agreement)*

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 1: _____ *(describe the full list of the personal information to be processed by the vendor doing the work under this agreement)*

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 1: *(describe the full list of the sensitive personal information to be processed by the vendor doing the work under this agreement)*

_____

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

APPENDIX 2 TO THE DATA PRIVACY AND SECURITY ADDENDUM

Approved Subcontractors

Hosting Facilities (where data is stored): *Include name (if a vendor,) and city, state, country of the location*

_____

Sub-contractors: *(full list of all companies being used by the processor for the work being done by this agreement, including their physical location)*

_____

Affiliates: *(full list of all affiliated companies being used by the processor for the work being done by this agreement, including their physical location)*

_____

APPENDIX 3 TO THE DATA PRIVACY AND SECURITY ADDENDUM

Standard Contractual Clauses (Applicable only if Section 2.4 is checked)