Carnival Corporation and plc
Security and Privacy Specifications for the Data Privacy and Security Addendum (DPSA)

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 27001:2013. • Obligation to align with the ISO 27002:2013 security standard or above • 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 and VPN-based access controls to protect the private service networks and back-end servers • Denial of Service protection • Data loss prevention • Advanced Persistent Threat detection/prevention • Mobile device management • Web application security • Continuously monitoring infrastructure security • Regularly examining security risks by internal employees and third-party auditors • Role-based access control implemented in a manner consistent with principle of least privilege • Remote access secured by using various two-factor authentication tokens, or multi-factor authentication
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 Controller 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, Processor 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 Controller. Processor must be able to demonstrate the established commonly accepted data protection and privacy control objectives.

5.	**Physical Site Security** **and** **Device hardening**	Security Measures in place as applicable to at the location where Confidential Information will be processed or stored: Established security areas • Electronically locked doors • Electronic access card reading system • Management of keys/documentation of key holders • 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 • Remove unused software and services from devices used to Process Personal Data. • 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 Controller'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 while 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 during 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 (particularly including Sensitive Personal Data) are encrypted in flight using the latest secured transmission protocols Transport Layer Security (TLS) 1.2 with a 2048-bit RSA key exchange 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. • Utilization of user identification credentials • 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 • Privacy and information security 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 & 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 generator • 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 are on equipment owned by Processor
14.	**Communications**	Promptly communicate Investigation results from incident response to Controller. • Systems and processes are in place to communicate incident and response investigation results • *Contact privacy@carnival.com to inform Controller.*

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 Controller 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 for access to the correct notices.	Processor uses a fwdlink to the current, published Controller 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 Controller Personal Data to ensure that the only data collected is that required to perform the Services required under the Agreement.	Processor can provide documentation that shows the Controller 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 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, or data relating to criminal convictions and offenses.) 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, unless continued retention of the Personal Data is required by Law.	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 organizational measures, insofar as possible, to fulfil its obligations to respond to requests for Data Subjects seeking to exercise their Data Subject Rights.	Documented evidence that processes 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 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.
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 Controller Personal Data, about that Data Subject. • Make a reasonable effort to locate the Personal Data and Controller 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.	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.
	• 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 and cooperate with Controller as necessary to resolve the issue	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 Controller Personal Data, Processor must: • Obtain Controller's express written consent prior to subcontracting services or making any changes concerning the addition or replacement of Subprocessors; • Document the nature and extent of Personal Data, sub-Processed by Sub-processors, ensuring that the information collected is required to perform Services 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 Subprocessor 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.	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 Subprocessors. Demonstrate how a Data Subject preference is utilized by Sub-processors. 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.