STOTSENBERG LEISURE PARK
& HOTEL CORPORATION
PRIVACY POLICY

1. PRIVACY STATEMENT

This Privacy Policy (the "Policy") reflects Stotsenberg Leisure Park & Hotel Corporation's ("SLPHC") commitment to ensure that all Personal Information or Data collected and processed by the SLPHC, and its partners are given all the protection under the law. SLPHC reserves the right to amend and/or modify this Policy whenever necessary in order to comply with the changes in existing laws, regulations and best practices.

2. SCOPE AND APPLICATION

This Policy applies to all personal data processing activities of SLPHC, including, but not limited to, the collection, use, storage, sharing, and disposal of all Personal Information or Data of its guests, employees and contractual counter-parties.

3. DEFINITIONS

- **Data Subject-** is defined under Section 3(c) of the Data Privacy Act as any individual whose personal information is processed.

- **Data Sharing Agreement** - refers to a contract, joint issuance, or any similar document which sets out the obligations, responsibilities, and liabilities of the Personal Information Controllers involved in the transfer of the same between or among them, including the implementation of adequate safeguards for data privacy and security, and upholding the rights of the Data Subjects: provided, that only Personal Information Controllers should be made parties to a Data Sharing Agreement.

- **Processing**- is defined as any operation or any set of operations performed upon Personal Information or Data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

- **Personal Information or data** - is defined as any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

- **Personal Information Controller** - is defined as a person or organization who controls the collection, holding, processing or use of Personal Information or Data, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose Personal Information or Data on his or her behalf. The term excludes:

(1) A person or organization who performs such functions as instructed by another person or organization; and

(2) An individual who collects, holds, processes or uses Personal Information or Data in connection with the individual's personal, family or household affairs.

- **Personal Information Processor** - is defined as any natural or juridical person qualified to act as such under this Act to whom a Personal Information Controller may outsource the processing of Personal Information Data pertaining to a Data Subject.

- **Sensitive Personal Information** – is defined as Personal Information:

  a. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

  b. About an individual's health, education, genetic and/or biometric data, sexual life and/or orientation, or any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;

  c. Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

  d. Specifically established by an executive order or an act of Congress to be kept classified.

4. COLLECTION AND USE OF PERSONAL INFORMNATION

4.1. Guest's Personal Information or Data

As a hotel and casino operator licensed under the Philippine Amusement and Gaming Corporation ("PAGCOR"), we necessarily collect personal information or data from our guests for the following purposes:

a) For compliance with applicable laws, rules and regulations;

b) To perform functions that are vital and necessary to our services, including internal security, quality assurance, customer feedback and real time monitoring of client/customer activities, winnings and losses for purposes of client/customer care and efficient and timely service delivery;

c) For business development, including the conduct of marketing/information campaigns relating to our services, promotions, loyalty and rewards programs, and discounts, business analysis and research; and

d) The achievement of our corporate objectives and other related business endeavors.

We collect such information directly from data subjects upon visiting our websites, and through our Membership Application Forms, and encode the same in our Hotel and Casino Data Management System.

4.2. Applicant and Employee Personal Data

As an organization that employs a significant number of individuals to meet our corporate objectives and business goals, we collect and process Personal Information or Data from our applicants and employees for administrative and human resource development purposes including, but not limited to:

1. Identity verification;
2. Pre-qualification and post-qualification assessment;
3. Performance evaluation and career development;
4. Processing of employment compensation and benefits, including health insurance coverage, retirement benefits and housing assistance;
5. Internal Security
6. Compliance with regulatory requirements
7. For the protection of lawful rights and interests of the organization in internal administrative and court proceedings, or the establishment, exercise or defense of legal claims against potentially malfeasant employees.

4.3. THE RIGHTS OF DATA SUBJECTS

In accordance with the Data Privacy Act of 2012, SLPHC fully recognizes that our guests and employees, being Data Subjects, are accorded with the following rights in connection with the Processing of their Personal Data:

A. Right to be Informed. The Data Subject has the right to be informed whether Personal Data pertaining to him or her shall be, are being, or have been processed. The Data Subject shall be notified and furnished with information indicated hereunder before the entry of his or her Personal Data into the records of the Company, or at the next practical opportunity:

1. description of the Personal Data to be entered into the system;
2. purposes for which they are being or will be processed, including Processing for direct marketing, profiling or historical, statistical or scientific purpose;
3. basis of Processing, when Processing is not based on the consent of the Data Subject;
4. scope and method of the Personal Data Processing;
5. the recipients or classes of recipients to whom the Personal Data are or may be disclosed or shared;
6. methods utilized for automated access, if the same is allowed by the Data Subject, and the extent to which such access is authorized, including

meaningful information about the logic involved, as well Personal as the significance and the envisaged consequences of such Processing for the Data Subject;

7. the identity and contact details of the DPO;
8. the period for which the Personal Data will be stored; and
9. the existence of their rights as Data Subjects, including the right to access, correction, and to object to the Processing, as well as the right to lodge a complaint before the National Privacy Commission.

B. Right to Object. The Data Subject shall have the right to object to the Processing of his or her Personal Data, including Processing for direct marketing, automated Processing or profiling. The Data Subject shall also be notified and given an opportunity to withhold consent to the Processing in case of changes or any amendment to the information supplied or declared to the Data Subject in the preceding paragraph. When a Data Subject objects or withholds consent, the Company shall no longer process the Personal Data, unless:

1. the Personal Data is needed pursuant to a subpoena;
2. the Processing is for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the Data Subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the Company and the Data Subject; or
3. the Personal Data is being collected and processed to comply with a legal obligation.

C. Right to Access. The Data Subject has the right to reasonable access to, upon demand, the following:

1. Contents of his or her Personal Data that were processed;
2. Sources from which Personal Data were obtained;
3. Names and addresses of recipients of the Personal Data;
4. Manner by which his or her Personal Data were processed;
5. Reasons for the disclosure of the Personal Data to recipients, if any;
6. Information on automated processes where the Personal Data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the Data Subject;
7. Date when Personal Data concerning the Data Subject were last accessed and modified; and
8. The designation, name or identity, and address of the DPO.

D. Right to Rectification. The Data Subject has the right to dispute the inaccuracy or rectify the error in his or her Personal Data, and the Company shall correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the Personal Data has been corrected, the Company shall ensure the accessibility of both the new and the retracted Personal Data and the simultaneous receipt of the new and the retracted Personal Data by the intended recipients thereof:

Provided, that recipients or third parties who have previously received such processed Personal Data shall be informed of its inaccuracy and its rectification, upon reasonable request of the Data Subject.

E. Right to Erasure or Blocking. The Data Subject shall have the right to suspend, withdraw, or order the blocking, removal, or destruction of his or her Personal Data from the Company's filing system.

1. This right may be exercised upon discovery and substantial proof of any of the following:

   (a) The Personal Data is incomplete, outdated, false, or unlawfully obtained;
   (b) The Personal Data is being used for purpose not authorized by the Data Subject;
   (c) The Personal Data is no longer necessary for the purposes for which they were collected;
   (d) The Data Subject withdraws consent or objects to the Processing,and there is no other legal ground or overriding legitimate interest for the Processing by the Company;
   (e) The Personal Data concerns private information that is prejudicial to Data Subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
   (f) The Processing is unlawful; or
   (g) The Data Subject's rights have been violated.

2. The DPO may notify third parties who have previously received such processed Personal Data that the Data Subject has withdrawn his or her consent to the Processing thereof upon reasonable request by the Data Subject.

F. Transmissibility of Rights of Data Subjects. The lawful heirs and assigns of the Data Subject may invoke the rights of the Data Subject to which he or she is an heir or an assignee, at any time after the death of the Data Subject, or when the Data Subject is incapacitated or incapable of exercising his/her rights.

G. Data Portability. Where his or her Personal Data is processed by the Company through electronic means and in a structured and commonly used format, the Data Subject shall have the right to obtain a copy of such data in an electronic or structured format that is commonly used and allows for further use by the Data Subject. The exercise of this right shall primarily take into account the right of Data Subject to have control over his or her Personal Data being processed based on consent or contract, for commercial purpose, or through automated means. The DPO shall regularly monitor and implement the National Privacy Commission's issuances specifying the electronic format referred to above, as well as the technical standards, modalities, procedures and other rules for their transfer.

4.4. POLICY ON THE COLLECTION AND USE OF PERSONAL INFORMATION

It is the policy of SLPHC to:

a. Adequately inform our guests and employees of their rights as data subjects;

b. Ensure that our guests and employees, are fully and adequately informed of all processing activities performed by the organization with respect to their Personal Information or Data including the scope, purpose and means used by SLPHC for such processing, its sources, recipients, methods, disclosures to third parties and their identities, automated processes, manner of storage, period of retention, manner of disposal and any changes thereto before the same is implemented;

c. Obtain the express, informed and properly documented consent of our guests and employees, whenever necessary, for our Data Processing activities. Where, by its nature, the processing does not require consent, we endeavor, nonetheless, to fully inform our guests and employees of the purpose of such processing;

d. Ensure that our guests and employees have the facility to reasonably exercise their rights as Data Subjects, and that we can effectively respond to such requests within reasonable time, including the provision of personal data in a machine-readable, or data portable format if requested;

e. Ensure that our guests and employees have the facility to dispute any inaccuracy or error in their Personal Information or Data, to object to any changes in the manner and purpose by which their Personal Information or Data is being processed, to withdraw consent where applicable, and to suspend, withdraw, block, destroy, or remove any unnecessary, falsely collected or unlawfully processed Personal Information or Data;

f. Ensure that the Personal Information or Date obtained from our guests and employees are proportional, necessary and limited to the declared, specified and legitimate purpose of the processing;

g. Ensure that the Personal Information or Data of our guests and employees are retained for only a limited period, or until the lawful purpose of the processing has been achieved;

h. Ensure that the Personal Information or Data of our guests and employees are destroyed or disposed of in a secured manner and in accordance with law and best practice;

i. Ensure that our guests and employees have the facility to lodge complaints to SLPHC relating to any violations to the rights of our customers and employees as Data Subjects and that such complaints are adequately and timely addressed.

5. DATA PRIVACY GOVERNANCE

5.1. DATA PROTECTION OFFICER

SLPHC takes data protection seriously and has appointed a Data Protection Officers ("DPO") tasked

to monitor compliance with any and all applicable data privacy laws, rules, and regulations, including best practices

5.2. CONTACT INFORMATION

Our Data Privacy Office is fully committed to protecting our guests' and employees ' privacy rights. Should you have any concerns regarding SLPHC's privacy practices and policies, including requests for exercise of data subjects' rights, you may reach the DPO through the following contact information:

Data Privacy Officer	
E-mail	dpo@hotelstotsenberg.com
Office Address	Gil Puyat Ave. corner Andres Soriano St., Clark Freeport Zone, Pampanga

6. PERSONAL DATA SECURITY POLICY

6.1. STORAGE OF AND ACCESS TO PERSONAL INFORMATION

In order to protect the Personal Information or Data we collect, we only store the same in a secured database with the necessary data security protection to prevent possible breach. Transfers of Personal Information or Data within and outside the organization are only made in accordance and under strict security protocols.

6.2. RETENTION AND DISPOSAL OF PERSONAL DATA

We only retain Personal information for a limited period or until the lawful and legitimate purpose of the processing is achieved or whenever retention is necessary for statistical analysis. To that effect, we have established procedures for securely disposing files that contain Personal Information or Data whether the same is stored on paper, film, optical or magnetic media, personal data stored offsite, and computer equipment, such as disk servers, desktop computers and mobile phones at end-of-life.

6.3. MANAGEMENT OF THIRD-PARTY RISKS

Any processing of Personal Information or Data by an external agent or entity (third-party service provider) on our behalf of are covered by a valid written agreement which expressly sets out the this Policy as a subject matter and duration of the processing, the nature and purpose of thereof, the type of information and categories of Data Subjects, our rights and obligations, and the geographic location of the processing.

The fact that we entered into such agreement or arrangement does not give the said external agent or entity the authority to subcontract to another entity the whole or part of the subject matter of said contract or arrangement, unless expressly stipulated in writing in the same agreement or

evidenced by our separate written consent/agreement. The Subcontracting Agreement must also comply with the standards/criteria prescribed by the immediately preceding paragraph.

In addition, the contract and the Subcontracting Agreement shall include express stipulations requiring the external agent or entity (including the subcontractor) to:

a. process the Personal Information or Data only upon our documented instructions, including transfers of the same to another country or an international organization, unless such transfer is required by law;

b. ensure that an obligation of confidentiality is imposed on persons and employees authorized by the external agent/entity and subcontractor to process such information;

c. implement appropriate security measures;

d. comply with the Data Privacy Act and other issuances of the National Privacy Commission, and other applicable laws, in addition to the obligations provided in the contract, or other legal act with the external party;

e. not engage another processor without our prior written instruction; provided, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing;

f. assist SLPHC, by appropriate technical and organizational measures, and to the extent possible, fulfill the obligation to respond to requests by Data Subjects relative to the exercise of their rights;

g. assist SLPHC in ensuring compliance with the Data Privacy Act and other issuances of the National Privacy Commission, taking into account this Policy, the nature of processing, and the information available to the external party who acts as a Personal Information Processor as defined under the Data Privacy Act;

h. at our option, delete or return all personal information to us after the end of the provision of services relating to the processing: provided, that this includes deleting existing copies unless storage is authorized by the Data Privacy Act or other applicable laws or regulations;

i. make available to SLPHC all information necessary to demonstrate compliance with the obligations laid down in the Data Privacy Act, and allow for and contribute to audits, including inspections, conducted by SLPHC or another auditor mandated by said agency; and

J. immediately inform SLPHC if, in its opinion, an instruction violates the Data Privacy Act or any other issuance of the National Privacy Commission.

7. BREACH AND NOTIFICATION

Personal Data Breach refers to a breach of security leading to the accidental or unlawful destruction,

loss, alteration, unauthorized disclosure of, or access to, Personal Information or Data transmitted, stored, or otherwise processed. Personal Information or Data breaches shall be subject to notification and remediation requirements.

a. **Data Breach Notification**. All our employees and agents involved in the Processing of Personal Data are tasked with regularly monitoring for signs of a possible data breach or security incident. In the event that such signs are discovered, the employee or agent shall immediately report the facts and circumstances to the DPO within twenty-four (24) hours from his or her discovery for verification as to whether or not a breach requiring notification under the Data Privacy Act has occurred as well as for the determination of the relevant circumstances surrounding the reported breach and/or security incident. The DPO shall notify the National Privacy Commission and the affected Data Subjects pursuant to requirements and procedures prescribed by the DPA. The notification to the National Privacy Commission and the affected Data Subjects shall at least describe the nature of the breach, the Personal Information or Data possibly involved, and the measures taken by the Company to address the breach. The notification shall also include measures taken to reduce the damage or negative consequences of the breach and the name and contact details of the DPO. The form and procedure for notification shall conform to the regulations and circulars issued by the National Privacy Commission, and related issuances.

b. Breach Reports. All Personal Information or Data breaches shall be documented through written reports, including those not covered by the notification requirements. In the case of such breach, a report shall include the facts surrounding an incident, the effects of such incident, and the remedial actions taken by SLPHC. In other security incidents not involving Personal Information or Data, a report containing aggregated data shall constitute sufficient documentation. These reports shall be made available when requested by the National Privacy Commission. A general summary of the reports shall be submitted by the DPO to the National Privacy Commission annually.

8. HUMAN RESOURCE POLICY

SLPHC requires its employees to undergo periodic and mandatory training privacy and data protection in general and in areas reflecting job-specific content. Likewise, it will ensure that all employees, representatives, and agents exposed to personal data pursuant to their function are adequately bound by strict confidentiality.