7SEAS ENTERTAINMENT LIMITED
PRIVACY AND DIGITAL PERSONAL DATA PROTECTION POLICY

(Approved/Amended by the Board of Directors on 18 July 2026)

CIN: L72900TG1991PLC013074

Registered Office: 5th Floor, Plot Nos. 92, 93 and 94, Kavuri Hills, Madhapur, Hyderabad, Telangana – 500081

Classification: Public – to be hosted on the Company's website

1. Purpose and application

This Policy governs digital personal data processed through the Company's websites, games, mobile and web applications, social-media login, customer support, investor relations, employment and business interactions. It is designed for the Digital Personal Data Protection Act, 2023 ("DPDP Act"), DPDP Rules, 2025 and the continuing information-technology framework.

2. Roles and accountability

The Company is a Data Fiduciary for purposes determined by it and may engage Data Processors under written contracts. The Board shall oversee privacy risk; the designated Grievance Officer/Data Protection contact shall administer rights and complaints; business owners remain accountable for lawful processing.

3. Categories of personal data

- Name, email, telephone number, address and account identifiers.
- Device, IP address, cookie, SDK, gameplay, diagnostic and usage data.
- Transaction, billing, support, complaint and communication data.
- Employee, applicant, vendor, director, shareholder and regulatory data.
- Children's or parental data only where lawfully and necessarily processed.

4. Specified purposes and lawful processing

Personal data shall be processed for specified lawful purposes such as providing games/services, authentication, support, security, fraud prevention, transactions, legal compliance, investor servicing and consented communications. Processing shall not exceed the notice or continue after purpose exhaustion unless lawfully retained.

5. Notice and consent

Notices shall be clear, standalone and itemise data and purposes, manner of rights exercise and complaint channels. Consent shall be free, specific, informed, unconditional, unambiguous and indicated by affirmative action. Records of notice and consent shall be maintained. Bundled, pre-ticked or deceptive consent is prohibited.

6. Withdrawal and preference management

Withdrawal shall be as easy as giving consent and shall stop future consent-based processing within a reasonable time, subject to lawful retention and consequences

explained to the Data Principal. Consent and communication preferences shall be honoured across relevant systems and processors.

7. Rights of Data Principals

- Access to information concerning processing and sharing.
- Correction, completion and updating.
- Erasure where the purpose is no longer served and retention is not legally necessary.
- Grievance redressal.
- Nomination of another individual to exercise rights in the event of death or incapacity.

8. Children and parental consent

A child means an individual below eighteen years unless a lawful exemption applies. Verifiable parental consent shall be obtained where required. Processing likely to cause detrimental effect, tracking or behavioural monitoring of children and targeted advertising directed at children are prohibited except as lawfully permitted.

9. Security and processor management

Reasonable safeguards shall include access control, encryption or masking where appropriate, secure development, logging, monitoring, backups, vulnerability management, incident response and employee training. Processor contracts shall cover instructions, confidentiality, security, sub-processing, rights assistance, breach reporting, audit and deletion.

10. Personal data breaches

Suspected breaches shall be reported immediately, contained and assessed. Affected Data Principals and the Data Protection Board shall be notified in the form and timelines prescribed. Material cyber incidents shall also be assessed under Regulation 30 and reported to CERT-In and other authorities where applicable.

11. Retention, erasure and cross-border processing

Retention schedules shall link each data category to purpose and legal requirement. Data shall be securely erased or anonymised on expiry, including from processors where feasible. Cross-border processing shall comply with restrictions and orders issued by the Central Government.

12. Grievance and contact

Requests and deletion instructions may be sent to systems@7seasent.com. Privacy grievances may be escalated to the designated officer identified on the website. The Company shall authenticate requests proportionately and respond within the prescribed period before a Data Principal approaches the Data Protection Board.

13. Interpretation and overriding effect

Terms not specifically defined in this Policy shall have the meanings assigned to them under the Companies Act, 2013, the rules made thereunder, the applicable SEBI regulations and other governing law. References to statutes and regulations

include amendments, clarifications, circulars and re-enactments. If any provision of this Policy conflicts with applicable law, the law shall prevail and this Policy shall be read as modified to the minimum extent necessary.

14. Administration and responsibility

The Board shall retain overall responsibility for this Policy. The committee or officer identified in this Policy shall administer it, maintain evidence of compliance and report material deviations. Every director, officer, employee, consultant and service provider within scope shall provide information and cooperation reasonably required for implementation.

15. Records, training and assurance

The Company Secretary/Compliance Officer shall ensure that approvals, registers, declarations, notices, reports, training records and supporting documents are retained for the period prescribed by law and the Company's document-retention schedule. Periodic awareness and role-based training shall be conducted. Internal audit or an independent reviewer may test compliance and recommend corrective action.

16. Review and amendment

This Policy shall be reviewed at least annually and earlier upon a material change in law, business model, organisation, risk profile or regulatory guidance. Material amendments shall be placed before the competent committee and the Board. The Managing Director and Company Secretary/Compliance Officer may jointly make clerical, contact-detail and statutory-reference corrections that do not alter substantive rights or obligations, subject to reporting to the Board.

For 7Seas Entertainment Limited
Company Secretary / Compliance Officer