FOSUN Holiday 复星旅文

Fosun Tourism Group
Personal Information Protection Policy

LC_T_LC•00_005_V2.0

Fosun Tourism Group First published on 22 August 2022
Updated and published on 14 January 2024

FOSUN Holiday 复星旅文

Version	Modified date	Summary of modification	Modified by	Approval date
V1.0	2022.8.23	First published	-	2022.8.23
V2.0	2024.1.4	Updated and published	-	2024.1.4

FOSUN Holiday 复星旅文

Catalogs

1. Objective 1
2. Application Scope 1
3. Definitions 1
4. Personal Information Protection Principles 1
5. Organization Management 3
6. Management of the whole process of handling personal information 4
7. Privacy Policy Management 17
8. Employee Rights Management 20
9. Personal information security impact assessment 21
10. Disposal of personal information security incidents 23
11. Personal information security audits 24
12. Training on personal information security responsibilities 24
13. Complaint Reporting 26
14. Rewards and Penalties 26
15. Others 26

1. Objective

This Policy is formulated in order to implement the obligations of personal Information processors, standardize the personal information processing activities of Fosun Tourism Group and all of its subsidiaries (the "Company"), and prevent personal information from being tampered with, leaked, stolen and other incidents.

2. Application Scope

Applies to all businesses within the Company. In the event that data is shared among the subsidiaries within the Company, the responsibility of the processors of the personal information in question is shared.

3. Definitions

3.1 Personal information: Personal information consists in all kinds of information relating to an identified or identifiable natural person recorded electronically or by other means, excluding anonymized information.

3.2 Sensitive personal information: Sensitive personal information is personal information that, once leaked or illegally used, can easily lead to the infringement of a natural person's human dignity or jeopardize the safety of his or her body or property, including information on biometrics, religious beliefs, specific identities, medical care and health care, financial accounts, whereabouts and trajectories, as well as the personal information of minors who have not reached the age of 14.

4. Personal Information Protection Principles

Personal information shall be protected in accordance with the following principles:

1. **Lawful collection**: Personal information shall not be collected by fraud, enticement, or force and the purpose of such collection shall not be concealed or personal information shall not be obtained through unlawful channels or collected if it is expressly prohibited from being collected by laws and regulations.

2. **Clear Purpose**: Personal information shall be handled with a clear and reasonable purpose, and shall be directly related to the purpose of the handling and in a manner that minimizes the impact on the rights and interests of individuals.

3. **Minimum Necessity**: The collection of personal information shall be limited to the minimum extent necessary to achieve the purpose of processing, and personal information shall not be collected excessively.

4. **Informed consent**: the handling of personal information shall follow the principles of openness and transparency, disclose the rules for handling personal information, express the purpose, manner and scope of handling, and obtain the authorized consent of the subject of the personal information; in the event of a change in the purpose of personal information handling or in the manner of handling and the type of personal information to be handled, a new consent shall be obtained from the individual; and the handling of sensitive personal information shall be subject to a specific consent of the personal information subject.

5. **Quality assurance**: The handling of personal information shall ensure the quality of the personal information to avoid adverse effects on the rights and interests of individuals due to inaccurate or incomplete personal information.

6. **Safety and security**: The Company shall maintain adequate security measures in light of the security risks it faces, and shall take sufficient management actions and technical measures to protect the confidentiality, integrity, and availability of personal information.

7. **Participation of Subjects**: Provide personal information subjects with ways and means to be able to inquire, copy, correct, transfer, delete, restrict processing, cancel accounts, withdraw authorization and file complaints.

5. Organization Management

5.1 The company's legal representative has overall leadership responsibility for personal information security, including the provision of human, financial and material resources for personal information security systems.

5.2 Personal Information Protection Officer: The Corporate Information Security Officer is the person in charge of personal information protection in the company. The responsibilities of the person in charge of personal information protection of the company include:

5.2.1 Comprehensively coordinating and implementing personal information security within the company, and taking direct responsibility for personal information security.

5.2.2 Formulate overall policy and strategy for data compliance management, coordinate the establishment of technical safeguards for data compliance, and take the lead in data risk identification, risk assessment and risk mitigation.

5.2.3 Audit and assess the management and business behavior of the Company to ensure that business activities with suppliers, agents, distributors, affiliates and branches, as well as activities such as handling personal information, comply with the requirements of data regulations, and formulate data risk response measures.

5.2.4 Formulate, issue, implement and regularly update privacy policies and related protocols.

5.2.5 Establish, maintain and update an inventory of personal information held by the Company (including the type, amount, source and recipient of personal information) and an authorized access policy.

5.2.6 Conduct personal information security impact assessments.

5.2.7 Organize and conduct personal information security training.

5.2.8 Test products or services before they are released online to avoid involuntary personal information collection, use, sharing, and other types of processing.

5.2.9 Conduct personal information security audits.

5.2.10 Establish a personal information protection team.

5.2.11 Maintain communication with supervisory and management departments to inform or report on personal information protection and incident handling.

5.3 All employees are under a duty of confidentiality to other employees, customers or others for their personal information.

6. Management of the whole process of handling personal information

The Company shall abide by the following principles in handling users' personal information: the principle of consistency of authority and responsibility, the principle of clarity of purpose, the principle of obtaining consent, the principle of minimum sufficiency, the principle of openness and transparency, the principle of ensuring security and the principle of participation of users, so as to effectively fulfill the obligations of network security, safeguard the rights of users and ensure the security of personal information.

6.1 Collection of Personal Information

6.1.1 Legality Requirements

(1) Subjects of personal information shall not be defrauded, enticed or forced to provide their personal information.

(2) The function of collecting personal information that the product or service has shall not be concealed.

(3) Personal information shall not be obtained from illegal channels.

(4) Personal information that is prohibited from collection by laws and regulations shall not be collected.

6.1.2 Minimization requirements

(1) The type of collection shall be directly related to the objective of the functionalities relating to products and/or services.

(2) The frequency of automated collection shall be the minimum necessary to use the functionalities relating to products and/or services.

(3) The amount of information collected shall be the minimum necessary to achieve the functionalities relating to products and/or services.

6.1.3 Authorized Consent

(1) Direct acquisition: Clearly inform the user of the types of personal information collected for different functionalities relating to products and/or services, as well as the rules for collecting and using personal information, and obtain the user's consent. Consent to handle personal information shall be requested from individuals depending on the specific type of products and/or services, and generalized terms shall not be used to obtain consent.

(2) Indirect acquisition: Require the provider to disclose the source of the personal information and confirm the legitimacy of the source; review the scope of authorized consent and whether the user has authorized consent for sharing or transfer, etc.

6.1.4 Individual express consent for the collection of sensitive personal information

(1) Sensitive personal information such as personal biometrics, religious beliefs, specific identities, medical and health care, financial accounts, whereabouts and trajectories shall be handled with a person's individual consent;

(2) Consent shall be obtained from the guardian of a minor under the age of fourteen for the handling of the minor's personal information;

Methods to obtain express consent include consent by signing, consent by taking action,

actively checking, actively clicking on “agree”, “register”, “send”, etc.

In the event of a change in the purpose of handling personal information, the method of handling personal information, or the type of personal information to be handled, a new consent shall be obtained from the individual, and the rules for handling personal information shall be updated simultaneously.

6.1.5 Safety Technical Measures for the Collection of Personal Information

(1) Anonymization: Personal information shall be anonymized immediately after it is collected, and information needed to restore the identification of individuals shall be stored separately from the anonymized information, and the management of access and use rights shall be reinforced.

(2) Data marking: Personal information collected shall be classified and marked accordingly in accordance with the Company's internal classification and grading management system, so as to realize classification and grading management at the level of the collected data fields.

6.1.6 Supervision of Personal Information Collection Behavior

(1) Verify the authenticity and accuracy of the data, and regularly analyze and monitor the data quality, and correct the abnormal data in a timely manner with alerts;

(2) Tracking and recording the data collection process to ensure the traceability of data collection activities.

6.2 Use of Personal Information

6.2.1 Employees and enterprises carrying out data processing activities shall comply with laws and administrative regulations, respect social morality and ethics, and shall not engage in the following activities:

(1) Endangering national security, honor and interests, divulging state secrets and work secrets;

2) Infringing on others' personality rights, intellectual property rights and other

legitimate rights and interests, etc;

3) Obtaining data by theft or other illegal ways;

4) Illegally reselling or illegally providing data to others;

(5) Producing, publishing, copying and disseminating illegal information;

6) Other behaviors prohibited by laws and administrative regulations.

6.2.2 Personal information shall be used, except where necessary for the purpose and in a manner that eliminates clear identity pointing and avoids pinpointing to a specific individual by using anonymization, masking of sensitive information, etc.

6.2.3 Shall not exceed the scope that is directly or reasonably related to the purpose disclosed at the time of collection, otherwise consent shall be obtained again.

6.2.4 Information resulting from the processing of collected personal information that can be recognized as personal information shall be handled in accordance with the scope of the authorized consent obtained at the time of collection.

6.2.5 Supervision and Approval of the Use of Personal Information

The use of personal information shall be analyzed through log analysis to analyze abnormal behavior for effective identification, monitoring and warning.

Important operation behavior of personal information shall be approved through internal approval process to ensure safe and controllable data usage behavior.

6.2.6 Access control measures for the use of personal information

A unified identity and access management platform is established, and technical measures such as multi-factor authentication and password management are adopted to provide and implement tight access control mechanisms for data, limiting the scope of data accessible to users, and preventing unauthorized leakage, tampering and damage to data.

6.2.7 Handling of sensitive personal information

The handling of sensitive personal information shall be closely related to the specific purpose of the handling and shall comply with the principle of not handling it unless it is necessary.

Before handling sensitive personal information, a personal information protection impact assessment shall be conducted. The handling process shall be recorded at the time of handling to ensure that the process of handling sensitive personal information is legal and compliant.

6.2.8 Handling of non-anonymized personal information

When handling non-anonymized personal information:

(1) Information not related to the purpose initially disclosed shall not be sent to e-mails, cellular phone numbers, etc;

2) Personal information shall not be used to engage in cyber violence;

3) Shall not handle personal information that an individual explicitly refuses to handle.

6.3 Personal Information Storage

6.3.1 Minimization of retention period

Personal information shall be stored for the minimum time necessary to achieve the purpose, and shall be deleted or anonymized after the expiration of the retention period.

6.3.2 Requirements for encrypted storage of personal information:

(1) Encryption and other security measures shall be used when storing personal sensitive information;

(2) Personal biometric information shall be stored separately from personal identification information;

(3) In principle, original personal biometric information (such as samples, images, etc.) should not be stored, and if storage is required, the following measures should be taken:

a) Only the summary information of personal biometric information should be stored;

b) To use directly the personal biometric information through collection terminal to realize identification, authentication and other functionalities;

c) Delete the original image from which personal biometric information can be extracted after using facial recognition, fingerprints, palm prints, iris scan, etc. to realize identification, authentication and other functionalities.

6.3.3 Electronic personal information shall be stored in a secure public cloud drive. The length of the password for the cloud disk shall be not less than 6 digits, the password shall be composed of numbers and letters, the password shall be valid for 90 days, and the new password shall not be the same as the previous 2 passwords.

Personal information on paper documents shall be kept by a person in a safe place that can be locked, and shall be kept in a safe physical environment (e.g., fire prevention, electricity, air conditioning, humidity, static electricity and other environmental protection measures). Individual employees shall not privately store or use the personal information collected and managed and stored by the Company. A strict management system shall be established for the operation and maintenance personnel of data centers where personal information is located, and security background checks shall be conducted for all operation and maintenance personnel.

6.4 Sharing and transfer of personal information

6.4.1 The Company shall not share or transfer personal information except with the authorized consent of the user. If it is necessary to share or transfer personal information to meet the requirements of business development, the following conditions shall be observed:

(1) Depending on the type and scale of personal information to be shared or transferred, the person in charge of personal information security shall decide whether or not to carry out a personal information impact assessment in advance and take effective measures to protect users based on the results of the assessment.

(2) Inform the individual of the purpose, type, manner, scope, storage period and storage location of the personal information provided, as well as the name or name of the recipient, contact information, purpose of processing, and method of processing, and obtain the individual's separate consent, except for cases that do not require the individual's consent in compliance with laws and administrative regulations or have been anonymized;

(3) Sharing and transferring sensitive personal information, in addition to the information given under (2), the user shall be notified of the data security capabilities of the data recipient, and the user's express consent shall be obtained before any transfer. Where laws and administrative regulations stipulate that written consent should be obtained, prior written consent shall be obtained from the user.

(4) Accurately record and preserve the sharing and transfer of personal information, including the date, scale, and purpose of the sharing and transfer, as well as the basic information of the data recipient.

(5) To help users understand the data recipient's preservation and use of personal information, etc., as well as the rights of users.

(6) Agree with the data receiver on the purpose, scope, and processing method of data processing, data security protection measures, etc., clarify the data security responsibilities and obligations of both parties through contracts and other forms, and supervise the data processing activities of the data receiver; when changing the purpose, scope, and method of processing, the user's individual consent shall be obtained again.

(7) Retain for at least five years records of individual consents and log records of personal information, and records of approvals and log records of sharing, trading, and processing of important data.

6.4.2 The following technical measures shall be taken during data transmission:

(1) During transmission, data transmission encryption SSL/TSL protocol shall be used, and application layer symmetric data encryption is to be carried out at the application layer for sensitive data to guarantee the integrity and security of data transmission;

(2) HTTP/HTTPS requests containing sensitive user information must use the POST method and not the GET method;

(3) Prohibit the import and export of sensitive information, only through the API data interface for data flow;

(4) The transmission of files containing sensitive information must be processed using a dedicated file exchange system.

(5) For financial card information (bank card number, CVV, expiration date), field-level encryption means should be taken to prevent information leakage.

6.4.3 In order to guarantee the security of the transmission interface, the following measures should be taken:

(1) Establish a device access mechanism, and perform device access by means of MAC address, IP address or port number binding.

(2) Establish a data transmission process control mechanism, record key operation logs, and formulate interface compacts, including interface name, interface parameters, and interface security requirements.

(3) Establish an interface security monitoring mechanism, sort out sensitive interfaces and form a list, monitor the use of all data transmission interfaces, monitor sensitive interfaces and low-activity interfaces, identify abnormal accesses, and promptly take down obsolete interfaces to improve interface security.

6.5 Public disclosure of personal information

6.5.1 As a matter of principle, personal information shall not be publicly disclosed. In the event that public disclosure is authorized by law or there are reasonable grounds for such disclosure, the following requirements shall be complied with:

(1) Conduct a security impact assessment of personal information in advance and take effective measures to protect the subject of personal information in accordance with the results of the assessment;

(2) Inform the subject of personal information of the purpose and type of public disclosure of personal information, and obtain the express consent of the subject of personal information in advance;

(3) Prior to the public disclosure of sensitive personal information, inform the subject of personal information of the content of the sensitive personal information involved, in addition to the information under (2);

(4) Accurately record and store the public disclosure of personal information, including the date, scale, purpose, and scope of public disclosure;

(5) Personal biometric information shall not be publicly disclosed; and

(6) The results of analysis of personal sensitive data such as race, ethnicity, political views, religious beliefs, etc. of people shall not be publicly disclosed.

6.5.2 For personal information that does need to be disclosed or displayed, different security technical measures should be taken according to different data types, specifically including:

(1) Commonly used contacts and users' personal information shall be hidden when displayed by default;

(2) In addition to generating orders and waiting for payment status, other order status (e.g., order cancellation, order inquiries) should be the phone number, mailbox, bank card, ID card number information for hidden processing;

(3) Identity card number is hidden between the first 4 digits and the last 3 digits, cell phone number is hidden between the first 3 digits and the last 4 digits, mailbox name is hidden between the first 3 digits and @ (when the mailbox name is less than or equal to 3 digits, the mailbox name is hidden between the 1st digit and @), bank card information is hidden beyond the last 4 digits, and landline phone number is hidden 3 digits backward from the last 2 digits;

(4) For passport/Hong Kong and Macao Travel Permit/Taiwanese Travel Permit/Home Visit Permit/International Seaman's Permit/Continental Resident's Permit for Traveling

to and from Taiwan, etc., the numbers between the first 2 digits and the last 2 digits shall be hidden;

(5) The hiding of numbers and letters must be processed as part of the system back-end, not in the system front-end.

6.5.3 Regular updating and evaluating the disclosed data, and recalling or destroying the data that is not suitable for further disclosure or that has exceeded the period of disclosure.

6.5.4 Undertake the corresponding responsibility for any damage caused to the legitimate rights and interests of the subject of personal information as a result of the public disclosure of personal information.

6.6 Deletion of Personal Information

6.6.1 Cases of deletion of personal information

Personal information shall be deleted or anonymized in the following cases:

(1) When the minimum period necessary to realize the purpose, the data storage period stipulated by laws, regulations and supervision is exceeded;

(2) The purpose of processing personal information has been realized, cannot be realized, or is no longer necessary to achieve the purpose of the data processing;

(3) The subject of personal information exercises its right to erasure;

(4) The subject of personal information cancels its account;

(5) The subject of personal information withdraws consent;

(6) Non-essential personal information collected or personal information collected without consent which cannot be avoided due to the use of automated collection technology, etc.

6.6.2 Requirements for personal information deletion

(1) The Company establishes a personal information deletion evaluation and approval procedure to evaluate the scope of data to be deleted, the reasons for deletion, and the possibility of reuse, etc., and implements data deletion after approval by the person in charge of data security of the Company;

(2) Provide data deletion technical measures and tools to delete important data and its copies after approval, including backup data, derived data and operation log data during data processing, etc., to ensure that the deleted data is not recoverable by commercial means;

(3) Establish a mechanism for evaluating the effectiveness of data deletion and regularly check the effectiveness of the deletion measures;

(4) Keep a log of the data deletion process to record the approval and implementation process of data deletion, as well as the specifics of the deleted data;

(5) When deleting confidential information on storage media, perform secure deletion and formatting, or repeat write operations to prevent recovery of deleted data;

(6) If the storage media is to be provided to a third party for use, the storage media administrator needs to confirm that the confidential information has been securely deleted.

6.7 Transfer of personal information

6.7.1 If the transfer of personal information is involved, the user's individual consent shall be obtained.

6.7.2 Personal information outbound, shall be transferred in accordance with the requirements of laws and regulations, in accordance with the relevant system requirements, subject to a personal information impact assessment, the approval of the Company and the person in charge of information security. The security assessment of outbound data shall focus on the following considerations:

(1) Legality, legitimacy, and necessity of the purpose, scope, and manner of data processing by the outbound data and overseas recipients;

(2) The scale, scope, type and sensitivity of the outbound data, and the risks that the data outbound may bring to national security, public interests, and the legitimate rights and interests of individuals or organizations;

(3) The responsibilities and obligations that the overseas recipient undertakes to assume, and whether the management and technical measures and capabilities to fulfill the responsibilities and obligations can guarantee the safety of the outbound data;

(4) The risk of data being tampered with, destroyed, leaked, lost, transferred or illegally acquired or illegally utilized during or after the data transfer, and whether the channels for safeguarding the rights and interests of personal information are ensured;

(5) Whether the contract or other legally binding documents (hereinafter collectively referred to as legal documents) related to data export drawn up with overseas recipients have sufficiently agreed on the responsibility and obligations for data security protection.

6.7.3 Personal information shall not be taken out of the country if any of the following circumstances exist:

(1) No individual consent has been obtained from the subject of the personal information, and no other legal basis for legitimacy exists;

(2) The transfer of data outside will lead to risks arising from national political, economic, scientific and technological, and national defense security, and may affect national security and harm the public interest of the society;

(3) Other data that have been determined by the competent authorities, such as the national Internet information department and the public security department, cannot be allowed to leave the country.。

6.8 Protection of users' rights

Convenient ways and means shall be established to accept and handle the user's subjective rights to personal information, and when receiving the user's request for the rights to personal information, it shall respond in a timely manner and handle the

request within a reasonable period of time. The personal information subject rights that users shall enjoy shall include at least:

6.8.1 Right of access

(1) Provide the user with the means to realize access to personal information.

(2) The information to be accessed includes the following: the personal information or types of personal information held by the Company about the subject; the source of such personal information, the purpose for which it is used; and the identity or types of third parties that have obtained such personal information.

6.8.2 Right to Copy

Provide the user with the means to reproduce copies of personal information.

6.8.3 Right of correction

Provide a means for users to request corrections or additional information.

6.8.4 Right to transfer

Users have the right to request the transfer of their personal information to other platforms, companies or organizations. When a user requests the transfer of his/her personal information, the Company shall examine his/her request, and after passing the examination, it shall provide the user with a way to transfer his/her corresponding personal information under the condition of complying with the regulations of the State Internet Information Department.

6.8.5 Right to delete

Users have the right to request:

(1) The Company to delete their personal information.

(2) If personal information is shared or transferred to a third party, that the Company immediately stop the act of sharing or transferring and notify the third party to delete it in a timely manner.

(3) In the case of public disclosure of personal information, that the Company immediately stop the act of public disclosure and issue a notice requesting the recipient to delete it in a timely manner.

6.8.6 Right to restrict processing

Provides users with the means to restrict the processing of their personal information by non-human automated decision-making mechanisms, including information systems and algorithms. Users have the right to request the Company to clarify the rules of processing through automated decision-making mechanisms.

6.8.7 Withdrawal of Consent

Provides a way for users to withdraw their consent to the collection and use of personal information, and the Company shall not process the corresponding personal information after the user withdraws his/her consent.

6.8.8 Account Cancellation

Provide a way for users to cancel their accounts, and the Company shall delete or anonymize their personal information after cancellation.

7. Privacy Policy Management

7.1 Basic Requirements for Privacy Policies

7.1.1 Privacy policy is stand alone and easy to read

(1) The privacy policy is custom drafted.

(2) The website homepage / App main function page can be accessed within 4 clicks; and the link position is prominent and unobstructed.

(3) The way the text of the privacy policy is displayed (font size, color, line spacing, etc.) should not be difficult to read.

7.1.2 Provides a clear description of each business functionality and the type of personal information it collects:

(1) Business functionalities for which personal information is collected are clearly disclosed and detailed.

(2) The types of personal information collected by each business functionality are clearly disclosed and detailed.

(3) Types of personal information collected by business functionalities should be relevant to the latter.

(4) Sensitive personal information should be identified.

7.1.3 Clear explanation is given of the rules for handling personal information and protection of users' rights and interests:

(1) Disclosure of basic information on the operator, including legal entity name, registered address, and contact information of the person in charge of personal information protection.

(2) Specifications on the use of personal information, such as application scenarios and possible effects on users.

(3) Transfer status of personal information, itemizing the types of personal information transferred outside the country and identifying them prominently.

(4) Measures and capabilities for personal information security protection, including measures taken (e.g. establishment of a personal information protection system, personal information security training, personal information authorization policy, etc.), capabilities (e.g. identity identification, data encryption, etc.), and qualifications (e.g. passed Level 3 evaluation, App security certification, etc.).

(5) Rules for sharing, transferring, and publicly disclosing personal information to the outside world, including the purpose, the type of personal information involved, and the type or identity of the recipient.

(6) Mechanisms for safeguarding users' rights, clearly stating the specific operating methods for users to inquire, copy, correct, transfer, delete, restrict processing, cancel accounts, and withdraw authorization.

(7) User complaint channels and feedback mechanisms.

7.1.4 The Privacy Policy should not include any unreasonable clauses or clauses that exempts itself from responsibility, aggravates the responsibility of users, or waives the main rights of users.

7.1.5 Release of Privacy Policy

(1) Privacy Policy timeliness, clearly identifying the date of the Privacy Policy release, effective and update.

(2) Updates to the Privacy Policy, including the circumstances and methods of updating (as far as possible to directly notify users).

7.2 Development, Review, Publication, and Implementation of Privacy Policy

7.2.1 Formulation

The Privacy Policy was formulated by Intelligent Science and Technology, and the product, development, operation, design, legal and other personnel provided comments and suggestions on the privacy policy.

7.2.2 Publication

The Privacy Policy is issued by the person in charge of personal information protection and published on the website and app. The publication of the Privacy Policy shall inform users in a timely manner through announcements, emails, letters, phone calls, push notifications, and other means.

7.2.3 Implementation

After the Privacy Policy is released, all departments of the Company shall work together to ensure the implementation of the Privacy Policy.

8. Employee Rights Management

8.1 Internal personal information operator

8.1.1 The Company shall assign to the internal personal information operator privileges in accordance with the principle of minimum authorization based on job requirements. That is, the personal information operator shall access the minimum sufficient personal information required for its duties, and only has the minimum data operation authority required to fulfill its duties.

8.1.2 Each functional department and each subsidiary shall specify the internal personal information operator privileges and designate a personal information protection specialist to be responsible for personal information protection matters in each department or subsidiary and to manage personal information in each department or subsidiary.

8.1.3 The addition, change and deletion of personnel data in internal operation positions shall be approved by the highest leader of the department and reported to the person in charge of personal information protection for the record; the addition or change or deletion of authority over data in internal operation positions shall be approved by the person in charge of personal information protection.

8.2 Internal Approval Process

Important operations on personal information, such as bulk modification, copying, downloading, deletion, etc., shall be approved by the person in charge of the department or business and the person in charge of personal information protection in accordance with the principle of minimum authorization.

Changes to the internal approval process shall be approved by the person in charge of personal information protection.

8.3 Excessive Authority Handling

If it is necessary to authorize a specific person to handle personal information beyond the scope of authority due to work requirements, the person in charge of personal information protection shall approve the authorization and record it in the register.

8.4 Key positions for personal information protection

At the level of each department and each subsidiary, the information protection specialist for each individual and employees with the authority to handle personal information in bulk are the key positions for personal information protection. Employees in key positions shall strictly keep the personal information storage management key and keep personal information strictly confidential. Key position employees shall complete the handover of the key before leaving the Company.

9. Personal information security impact assessment

In order to identify, deal with and monitor continuously the security risks in the process of personal information handling, continuously update the scope of personal information protection according to the business requirements, the threatening environment or laws and regulations, standard requirements, etc., and adjust the security control measures so that the process of personal information handling is under control, the Company shall regularly conduct the security impact assessment of personal information.

9.1 Evaluation Circumstances

(1) When there are new requirements in laws and regulations.

(2) When there is a major change in the business model, information system, or operating environment.

(3) When a major personal information security incident occurs.

(4) In addition to the above, the assessment is conducted on a regular basis (once a year).

9.2 Subjects Responsible for Assessment

The personal information security impact assessment is initiated and is the responsibility of the person in charge of personal information protection. The person in charge of personal information protection shall ensure the execution of the assessment process and the quality of the results, and sign the assessment report.

9.3 Content of assessment

The impact assessment of personal information security shall mainly assess the compliance of the processing activities with the basic principles of personal information security and the impact of personal information processing activities on the legitimate rights and interests of the subject of personal information. The content shall at least include:

(1) Whether personal information collection sessions follow the principles of clear purpose, informed consent, and minimum necessity;

(2) Whether the handling of personal information may adversely affect the legitimate rights and interests of the subject of personal information, including whether it may jeopardize the safety of persons and property, damage the reputation and physical and mental health of individuals, or lead to unequal treatment;

(3) The effectiveness of security measures for personal information;

(4) The risk of personal information subjects being re-identified from anonymized processed datasets or re-identified after aggregation with other datasets;

(5) The possible adverse effects of sharing, transferring, or publicly disclosing personal information on the legitimate rights and interests of the subject of personal information;

(6) The possible adverse impact on the legitimate rights and interests of the subject of personal information in the event of a security incident.

10. Disposal of personal information security incidents

10.1 In the event of leakage, tampering or loss of personal information, immediate remedial measures shall be taken. If a security incident is suspected to be a crime, it should be reported to the public security organs in a timely manner.

10.2 Timely reporting

10.2.1 If any personal information security incident occurs, it should be immediately reported to the person in charge of personal information security and the risk control officer.

10.2.2 The content of reporting includes the following parts:

(1) The overall situation of the type, number, content and nature of the subject of personal information involved.

(2) The possible impact of the incident.

(3) Disposal measures taken or to be taken.

(4) Contact information of the person concerned with the disposal of the incident.

10.3 Timely disclosure

10.3.1 In the event of a personal information security incident, except for cases where the Company takes measures that can effectively avoid the harm caused by the information leakage, tampering or loss, it shall promptly inform the affected users of the incident by email, telephone or push notifications. When it is difficult to inform users one by one, it shall take reasonable and effective ways to release warning information related to the general public.

10.3.2 The content of the notification includes the following parts:

(1) The content and impact of the security incident.

(2) Disposal measures taken or to be taken.

(3) Suggestions for users to prevent and reduce risks on their own.

(4) Remedial measures provided for the users.

(5) Contact information of the person in charge of personal information protection.

11. Personal information security audits

The content of the personal information security audit shall include at least:

(1) Auditing the effectiveness of personal information protection policies, related protocols and security measures;

(2) Establishment of an automated audit system to monitor and record personal information handling activities;

(3) The records prepared by the auditing process should provide support for the disposal of security incidents, emergency response and investigation after the facts;

(4) Prevent unauthorized access, tampering or deletion of audit records;

(5) Timely handling of personal information found in the audit process, such as the illegal use and misuse of personal information;

(6) Audit records and retention periods comply with the requirements of laws and regulations.

12. Training on personal information security responsibilities

12.1 Training system:

(1) Employees must participate in the Company's full personal information protection training;

(2) Employees are encouraged to participate in professional training organized by other

industries and departments, and employees are encouraged to participate in other business exchanges and trainings on learnings;

(3) Employees are encouraged to study on their own in conjunction with their work.

12.2 Training content:

(1) Personal information protection, data security, information security, network security and other related laws and regulations;

(2) Company's rules and regulations on personal information protection;

(3) Specialized training for different positions;

(4) Thematic training for business lines with high frequency of security incidents.

12.3 Training Cycle:

(1) Personal information protection training on a Company-wide level is held at least once a year.

(2) Organize personal information protection induction training for new employees from time to time.

(3) Organize customized personal information protection training from time to time.

12.4 Training methods:

(1) Organize special lectures or training courses.

(2) Hire relevant experts to give lectures.

(3) Assigning personnel to exchange and learn from the industry or outside organizations.

13. Complaint Reporting

Employees can report any violation via: Foliday_compliance@fosun.com. The Group strictly protects whistleblowers from attacks and retaliation.

14. Rewards and Penalties

14.1 Employees who make practical suggestions to improve the protection of personal information, actively deal with any emergency or risky matters, or report any violations of laws and regulations, and make contributions to the Company or avoid any loss to the Company, shall be rewarded with reference to the reward and punishment rules of Fosun Tourism Group.

14.2 Violations of this Policy will be punished according to the seriousness of the situation and the consequences caused, with reference to the Reward and Punishment Rules of the Group. If it constitutes a crime, it will be notified to the administrative or judicial organizations to pursue legal action.

15. Others

15.1 This Policy was approved and adopted on August 23, 2022 and came into effect on August 29, 2022 and revised on December 23, 2023.