Trip.com Group User Privacy Protection Policy

Protecting user privacy is not only a legal requirement but also a core principle that Trip.com Group (hereinafter referred to as "we" or the "Group") has consistently upheld. The Group recognizes the importance of personal information security and privacy protection to users, so we will safeguard users' personal information in compliance with global laws and regulations. Unless otherwise provided by the law, the Group will explicitly inform users and obtain their consent before we process their personal information.

The Trip.com Group User Privacy Protection Policy (hereinafter referred to as this "Policy") will help users understand how we collect, store, use, process, transmit, provide, disclose, and delete their personal information.

I. Organizational Management Structure for User Privacy Protection

The Group attaches great importance to user privacy protection. We have established a comprehensive mechanism for assessing and supervising personal information protection to effectively implement user privacy protection requirements, better safeguard users' personal information security, ensure the security of personal information transmission, storage, and processing, prevent and respond to security incidents, and reduce risks of data breaches and non-compliant personal information processing activities.

II. How We Collect and Use Users' Personal Information

We collect and use users' personal information according to the specific products or services they choose on the principles of "legality, legitimacy, and necessity" since we provide a variety of products and services. We primarily collect users' personal information for the following purposes:

1. Information necessary for fundamental business functions of our products and services: This information is necessary for the proper functioning of our fundamental products and services. Users need to authorize us to collect and use this information when using our products by agreeing to the user agreement and personal information protection policy. If users do not agree to the relevant agreement and policy, we will not be able to provide fundamental business services.

2. Information that may be needed for additional business functions of our products and services: This information is needed for non-fundamental business functions. Users can choose whether or

not to authorize us to collect it. If users refuse to provide this information, additional business functions may be unavailable or may not achieve the intended additional effect, but it will not affect the users' normal use of the Group's fundamental business functions.

Should we use user information for other purposes not provided above, we will inform the user again and try to receive their consent, unless otherwise provided by applicable law.

III. How We Share, Transfer, and Publicly Disclose Users' Personal Information

1. Sharing

The Group may share users' order information, account information, contact information, and other information with third parties, such as our partners, in accordance with applicable laws to ensure the smooth completion of the products or services provided to users. However, the Group will only share users' personal information for legal, legitimate, necessary, specific, and clear purposes, and will only share personal information that is necessary for the provision of products or services.

2. Transfer

We will not transfer users' personal information to any other companies, organizations, or individuals, except that:

(1) We have obtained the prior express authorization of the user;

(2) Such transfer is required by applicable laws and regulations, requirements of legal proceedings, or mandatory administrative or judicial orders;

(3) In cases including merger, division, acquisition, asset assignment, or similar transactions that involve the transfer of personal information, we will inform the user of the name and contact information of the receiving company or organization before the information transfer officially starts, and require the new company or organization holding the user's personal information to continue to perform the obligations for the processing of the personal information that was originally assumed by us.

3. Public disclosure

We will only publicly disclose personal information under the following circumstances:

(1) We have obtained the prior express authorization of the user;

(2) Such disclosure is required by applicable laws and regulations, requirements of legal proceedings, or mandatory administrative or judicial orders;

IV. How We Store and Delete User Information

The Group stores users' personal information in accordance with the requirements of applicable laws and provides adequate protection of users' personal information. In addition, we retain users' personal information only for as long as is necessary for the Group's products or services, or within the time limit required or permitted by laws and regulations. Upon expiration of the storage period, or if the user exercises the right to delete personal information or close the account, the Group will delete or anonymize the user's personal information in accordance with the requirements of applicable laws and regulations.

V. How We Protect Users' Personal Information

1. We attach great importance to information security and have set up a dedicated team to supervise the processing of personal information and the measures taken to protect it. We endeavor to protect users' information by taking appropriate management, technical, and physical security actions. We have established an information security protection system that fits our business development based on domestic and international information security standards and best practices. We have obtained the ISO27001 information security management system requirements certification, the ISO27701 privacy information management system certification, and the Payment Card Industry Data Security Standard (PCI-DSS) certification.

2. We have taken data security protection actions covering collection, storage, display, processing, use, and destruction to ensure lifecycle management of data. We take different control actions according to the level of information sensitivity, including but not limited to access control, SSL encrypted transmission, encrypted storage using AES 256-bit or other more advanced encryption algorithms, and de-identification of sensitive information before it is displayed.

3. In the event of a personal information security incident, the Group will, pursuant to the applicable laws and regulations, (1) inform users of the incident's basic details and potential

impact, the measures we have taken or will take, recommendations for users to prevent and reduce risks, and any remedial measures; (2) notify users of the incident via social media, app push notifications, and other methods; and/or (3) report the handling of personal information security incidents to the competent supervision agencies as required.

VI. Protection of Minors

The Group values the protection of minors' information. If any of our products or services involve the processing of minors' personal information, we will protect it pursuant to applicable laws and regulations. If a user provides information of minors for purposes such as booking, we will require the user to obtain the prior consent of the minor's guardian. We will collect, store, use, transfer, disclose, and process the personal information of minors pursuant to applicable laws and regulations following the principles of legitimacy and necessity, informed consent, clear purpose, security, and lawful use.

VII. Supplier Privacy Requirements

1. The Group implements strict data security management measures for third-party collaborators (including suppliers and other partners), such as security capability assessments and the signing of personal information processing agreements and confidentiality agreements. Additionally, we continuously review partners involved in data transmission to ensure they have obtained relevant information security management qualifications.
2. The Group encourages suppliers to implement user privacy protection measures according to our standards, adhering to the principles of minimization and necessity to safeguard user privacy.

VIII. Contact Us

If users have any questions, opinions, or suggestions regarding this policy, or if they discover that their personal information may have been leaked, they can contact us through our official customer complaint channels:

Privacy email: privacy@ctrip.com; sg_dataprotection@trip.com

Customer service hotline: 86-95010

App service chat