DIAMOND RESORTS INTERNATIONAL, INC.

EU – U.S. PRIVACY SHIELD
AND
SWISS-U.S. PRIVACY SHIELD

1. Purpose/Compliance

Diamond Resorts International® ("Diamond") acknowledges the European Union's ("EU") and Switzerland's standards for personal data protection. Through its relationship with a global customer base, Diamond has access to Personally Identifiable Information ("PII") of customers and employees in the EU and Switzerland. This EU – U.S. Privacy Shield and Swiss-U.S. Privacy Shield ("Privacy Shield Policy" or "Policy") addresses the privacy concerns of European and Swiss customers and employees due to data transfer between Diamond's European/Swiss and U.S. business units. Diamond has adopted this Privacy Shield Policy to establish and maintain an adequate level of PII privacy protection for the European and Swiss customers and employees.

Specifically, Diamond complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of PII transferred from EU member countries and Switzerland to the United States, respectively. Diamond has certified that it adheres to the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability. If there is any conflict between this Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view Diamond's certification page, please visit https://www.privacyshield.gov/.

The Federal Trade Commission ("FTC") has jurisdiction over Diamond's compliance with the Privacy Shield.

A corporate officer of Diamond will annually self-certify to the U.S. Department of Commerce that it will abide by the Privacy Shield Principles. Diamond will also state annually in its published privacy policy statement that it adheres to these Principles.

All Diamond employees who handle PII from the EU and Switzerland are required to comply with the Principles stated in this Policy.

2. Responsibilities

Diamond has designated the Legal Department to oversee its information security program, including its compliance with the EU – U.S. Privacy Shield program and Swiss-U.S.

Privacy Shield program. The Legal Department shall review and approve any material changes to this program as necessary. Any questions, concerns, or comments regarding this Policy also may be directed in writing to Gabriel Kotch, Corporate Counsel, Diamond Resorts International, 8415 S. Park Circle, Suite 200, Orlando, Florida 32819 or by telephoning 407.226.1000.

3. Collection and Use of Personal Data

Diamond provides various services to its European and Swiss customers who purchase its products and to its employees outside of the employment relationship. Diamond collects PII from European and Swiss customers when they purchase its products, become members in its Club, request information or otherwise communicate with it. Diamond collects PII from its employees when they become employees.

The PII that Diamond collects may vary based on a customer's or employee's interaction or role with Diamond and his or her request for its services. As a general matter, Diamond may collect the following types of PII from its European and Swiss customers and its employees: name, e-mail address, mailing address and telephone numbers, as well as payment or payroll information, including credit card/debit card data. Individual customers and employees have the option to contact Diamond online, via telephone or in person; Diamond will collect the foregoing categories of PII to the extent customers and employees choose to provide to it through these mediums.

The information that Diamond collects from its EU and Swiss customers and its employees is used for selling the products and services the European and Swiss customers may buy from it, managing transactions, reporting, invoicing, renewals, other operations related to providing customer services and products to the individual customer and for providing services to the employees outside of the context of the employment relationship.

Diamond does not sell PII to third parties and has no present intention of doing so in the future. However, Diamond may share PII with (i) its subsidiaries and affiliates; (ii) third party employment-service providers; (iii) third party data processors; (iv) third parties to act on its behalf for projects such as market-research surveys and contest-entry processing; and (v) external suppliers such as airline/car rental companies, for the following purposes:

1. maintaining and supporting its products, delivering and providing the requested products/services, and complying with its contractual obligations related thereto (including managing transactions, reporting, invoices, renewals, and other operations related to providing services to EU and Swiss customers);

2. satisfying governmental reporting, tax, payroll and other requirements;

3. storing and processing data, including PII, in computer databases and servers located in the United States;

4. verifying identity (e.g., for employment verification and customer access to accounts);

5. in response to a lawful request by public authorities, including to meet national security or law enforcement requirements;

6. for other business-related purposes permitted or required under applicable local law and regulation; and

7. as otherwise required by law.

3.1 Notice

Diamond will inform customers and employees in the EU and Switzerland about the purposes for which PII will be collected and used. Information will be provided regarding how customers and employees can contact Diamond with inquiries or complaints regarding PII. Diamond will give notice to employees and customers regarding third parties to which it discloses the information, and restrictions that limit the information's use and disclosure. In certain situations, data is "anonymized" so that the names of the customers and employees are not known by data processors within Diamond. In these cases, customers and employees do not need to be notified regarding the purpose for which PII will be collected and used.

3.2 Choice

Prior to disclosing PII to a third party, Diamond will give a customer or employee the opportunity to choose whether their PII is disclosed to that third party or used for a purpose incompatible with the basis for which it was originally collected or subsequently authorized by that individual. If Diamond collects Sensitive Information, an affirmative choice will be given to the employee or customer if the Sensitive Information is to be disclosed to a third party or used for a purpose other than its original purpose or the purposes authorized subsequently by the individual. To communicate with Diamond about disclosure of PII, customers and employees may contact Diamond as follows:

In Europe, by writing to our Customer Services Department at Citrus House, Caton Road, Lancaster, LA1 3UA, by telephoning our Customer Services Department at 0345 3590010, or by e-mailing our Customer Services Department at euhsirm@diamondresorts.com

In the United States or Canada, by writing to our Customer Service Department at 10600 W. Charleston Blvd, Las Vegas, Nevada 89135, by telephoning 877.374.2582, or by e-mailing our Customer Services Department at theclub@diamondresorts.com.

3.3 Onward Transfer (Transfer to Third Parties)

Diamond may transfer PII to third parties under limited circumstances. Prior to disclosing PII to a third party, Diamond will apply the Notice and Choice principles enumerated above.

Diamond will commit to taking reasonable and appropriate steps to ensure that the third party keeper of PII processes the data for the limited purpose for which it was provided and subscribes to the EU Privacy Shield Policy and Swiss Privacy Shield Policy Principles or any other EU and Swiss adequacy findings. Unless otherwise exempted under the U.S.-EU Privacy Shield Framework or Swiss-U.S. Privacy Shield Framework, Diamond will also enter into a written agreement with such third party requiring that the third party provide at least the same level of personal data protection as is maintained by Diamond. Diamond may be liable for appropriate onward transfers of personal data to third parties.

Please note that Diamond may be required to release an individual's personal information in response to lawful requests by public authorities including to meet national security and law enforcement requirements.

3.4 Access

Diamond acknowledges the right of individuals to have access to their personal data. Customers and employees covered under this Policy will have access to PII about them that Diamond holds, and will be able to correct, amend or delete information if it is inaccurate (the exception is when the burden or expense of providing access would be disproportionate to the risks of the individual privacy in the case in question or the rights of persons other than the individual would be violated.) For more information on how to contact Diamond regarding PII, see Section 3.2 above.

3.5 Security

While no system is absolutely secure, Diamond has put in place reasonable and appropriate data security measures to protect PII from loss, misuse and unauthorized access, disclosure, alteration and destruction. Access to PII of European and Swiss employees and customers will be provided to a limited number of authorized users on a need-to-know basis.

3.6 Data Integrity and Purpose Limitation

PII maintained by Diamond will be relevant for purposes of customer relations, compliance and legal considerations, security and fraud prevention, preserving or defending Diamond's legal rights, and other purposes consistent with the expectations of a reasonable person given the context of the collection. Diamond will take reasonable steps to ensure that the data is reliable and that it is applied to its intended use. Diamond will also take reasonable and appropriate steps to ensure that the information is accurate, complete and correct. Absent consent from the individual customer or employee, Diamond will not process PII in a way that is incompatible with the purpose for which it was originally collected or subsequently authorized by that customer or employee.

3.7 Recourse, Enforcement and Liability

In compliance with the EU-U.S. and Swiss-U.S. Privacy Shield Principles, Diamond commits to resolve complaints about EU and Swiss customers' or employees' privacy and its collection or use of their PII. EU and Swiss customers and employees with inquiries or complaints regarding this Policy should first contact Diamond at:

Diamond Information Security Council, Diamond Resorts International, 10600 W. Charleston Blvd., Las Vegas, Nevada 89135 or by e-mail to isc@diamondresorts.com

Diamond has further committed to refer unresolved privacy complaints under the EU-U.S. and Swiss-U.S. Privacy Shield Principles to BBB EU PRIVACY SHIELD, a non-profit alternative dispute resolution provider located in the United States and operated by the Council of Better Business Bureaus. If you, as an EU or Swiss customer or employee, do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit www.bbb.org/EU-privacy-shield/for-eu-consumers/ for more information and to file a complaint.

Please note that if your complaint is not resolved through these channels, under limited circumstances, a binding arbitration option may be available before a Privacy Shield Panel.

4. Limitation on Application of Principles

Adherence by Diamond to these principles may be limited (a) to the extent required to respond to a legal or ethical obligation; (b) to the extent necessary to meet national security, public interest or law enforcement obligations; and (c) to the extent expressly permitted by applicable law, rule or regulation.

5. Internet Privacy

Diamond sees the internet, and the use of other technology, as valuable tools to communicate and interact with customers, employees, business partners, and others. Diamond recognizes the importance of maintaining the privacy of information collected online and has created a specific Internet Privacy Policy (the "IPP") governing the treatment of PII collected through web sites that it operates. With respect to PII that is transferred from the EU or Switzerland to the U.S., the IPP is subordinate to this Policy. However, the IPP also reflects additional legal requirements and evolving standards with respect to internet privacy. Diamond's Internet Privacy Policy can be found at https://www.diamondresorts.com/Privacy-Policy.

6. Contact Information

Questions or comments regarding this Policy should be submitted to the Diamond Information Security Council by mail to:

Diamond ISC Diamond Resorts International
10600 W. Charleston Blvd.

Las Vegas, Nevada 89135

Or by e-mail to: isc@diamondresorts.com

7. Posting of Policy/Changes

This Policy is posted on www.diamondresorts.com and on its corporate intranet.

This Policy may be amended from time to time, consistent with the requirements of the Privacy Shield Principles. When we amend this Policy, the revised, updated date will be displayed at the bottom of this page.

8. Definitions

Diamond / Diamond Resorts International® - Means Diamond Resorts Corporation, its predecessors, successors, parents, subsidiaries, divisions, and groups in the United States.

European Union – The European Union ("EU") consists of 27 independent sovereign states: Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.

Personally Identifiable Information (PII or Personal Data, for the purposes of this policy) – Any personal information relating to an identified or identifiable natural person who is a Diamond employee or customer and who can be identified, directly or indirectly, in particular by a reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

Personal Data relating to Diamond employees will be limited to data outside the context of the employment relationship.

Sensitive Information – Sensitive Information is data that pertains to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, income records, health, sexual orientation or alleged commission of any offense. This data may not be transferred to a third party unless an individual gives explicit consent.

9. Exceptions

Exceptions to this Policy are based on the risk involved in not complying with the Policy and what mitigating actions can be taken to lessen the risk. In the event risk cannot be mitigated, exceptions may not be granted.

9.1 Procedure

The Policy Exception Form is completed by the Business Relationship Owner (for outsourced systems) or the appropriate Technology Director and submitted to the Information Security Council. Risks, including regulatory risks, are identified and measured against available mitigating actions. The Information Security Council then informs either the Technology Director or the Business Relationship Owner whether the exception has been granted.

9.2 Basis

Exceptions are granted when a system is essential to the continued business operation of the Diamond, the system is not technically capable of meeting the requirements of the Policy, and the service or system cannot be moved to a more compliant system. Mitigating actions, settings, or procedures may be presented to reduce the identified risks. If the Information Security Council agrees that the suggested mitigating actions are sufficient to reduce the risk to acceptable levels, the exception may be granted.

9.3 Mitigation

Mitigation of risk may include additional management controls, alternate security settings, physical or virtual isolation, increased monitoring, or the like. Mitigation must be in addition to actions or settings required by the information security policies.

10. Non-Compliance

Non-compliant behavior will be brought first to the attention of the correct department head and efforts will be made to bring the individual or group into compliance. Violators may be subject to disciplinary action, up to and including dismissal.

The consequence of non-compliance with this policy may result in violations of federal and /or state law and may result in disciplinary, civil, and/or criminal actions against the individual.