

Associate Privacy Statement

LAST UPDATED: July 19, 2018

1. Introduction

The Marriott Group, which includes Marriott International, Inc. and its affiliates (“Marriott”), is committed to protecting associate personal data. This data helps Marriott in business planning and internal talent searches, in addition to supporting human resources, and operational processes.

Marriott operates in many different countries or regions. Some of these countries or regions have laws related to the collection, use, transfer and sharing of the personal data of individuals, including Marriott’s associates. Marriott takes these obligations seriously and is committed to protecting the privacy of Marriott’s current and former associates. The purpose of this Associate Privacy Statement (the “Statement”) is to give associates information about what personal data Marriott collects, uses, transfers and shares, and why.

2. What Data About Associates Marriott Collects, Uses, Transfers and Shares, and Why

During your employment, Marriott may have collected or will collect data about you and your working relationship with Marriott, or about your spouse, domestic/civil partner or dependents (“Dependents”). Marriott refers to such data as “Personal Data.” For more specific information regarding what Personal Data about you Marriott may collect, use, transfer and share, and the purposes for which it may be collected, used, transferred and shared, please see the end of this Statement. Local associate handbooks, office manuals and notices provided may provide additional details or information. Marriott will not use Personal Data for any purpose incompatible with the purposes described in this Statement, unless it is required or authorized by law, authorized by you, or is in your own vital interest (*e.g.*, in the case of a medical emergency).

With the exception of certain data that is required by law, necessary or important to the performance of our business, your decision to provide Personal Data to Marriott is voluntary. If you do not provide certain required data, Marriott may not be able to accomplish some of the purposes outlined in this Statement.

We receive Personal Data from you as well as from other sources, such as colleagues, managers, references, clients and background check providers.

3. Transfer and Use of Personal Data

Due to the global nature of Marriott operations, Marriott may share Personal Data with personnel and departments throughout Marriott to fulfill the purposes described at the end of this Statement. This may include transferring Personal Data to other countries or regions (including countries or regions other than where you are based that have a different data protection regime than is found in the country where you are based). A list of the Marriott Group affiliated companies that may process and use Personal Data is available [here](#).

Access to Personal Data within Marriott will be limited to personnel with a business need to know the data, as per our policies, for the purposes described at the end of this Statement, and may include your managers and their designees, personnel in Human Resources, Information Technology, Compliance, Legal, Finance and Accounting and Internal Audit.

All personnel within Marriott will generally have access to your business contact data such as name, position, business telephone numbers, business postal address and business email address.

From time to time, Marriott may need to make Personal Data available to owners of Marriott Group branded properties that we manage or other unaffiliated third parties. For a list of the categories of unaffiliated third parties, please see the end of this Statement. Some of the owners and unaffiliated third parties will be located outside of your home jurisdiction, including in the United States. Third party service providers and owners are expected to protect the confidentiality and security of Personal Data, and only use Personal Data for the provision of services to Marriott, or in accordance with agreements with our owners, and in compliance with applicable law.

4. Security

Marriott will take appropriate measures to protect Personal Data that are consistent with applicable privacy and data security laws and regulations, including requiring service providers to use appropriate measures to protect the confidentiality and security of Personal Data.

5. Data Integrity and Retention

Marriott will take reasonable steps to ensure that the Personal Data processed is reliable for its intended use and is accurate and complete for carrying out the purposes described in this Statement. Marriott will retain Personal Data for the period necessary to fulfill the purposes outlined in this Statement unless a longer retention period is required or permitted by law.

The criteria used to determine our retention periods include:

- as long as Marriott has an ongoing relationship with you
- as required by a legal obligation to which Marriott is subject
- as advisable in light of Marriott's legal position (such as in regard of applicable statutes of limitations, litigation, or regulatory investigations)

6. Access, Correction, and Deletion Requests and Questions

Please contact your local Human Resources representative if you have any questions or concerns about how Marriott processes Personal Data. If you wish to request access, correction, suppression or deletion of Personal Data about you or request that Marriott cease using it or if you would like to request a copy or portability of your Personal Data, please initiate your request with your local Human Resources representative. Marriott will respond consistent with applicable law. Please note, however, that certain Personal Data may be exempt from these requests pursuant to applicable data protection laws or other laws and regulations.

7. Associate Obligations

Please keep Personal Data current and inform us of any significant changes to Personal Data. You agree to inform your Dependents whose Personal Data you provide to Marriott about the content of this Statement, and to obtain their consent (provided they are legally competent to give consent) for the use (including transfer and disclosure) of that Personal Data by Marriott as set out in this Statement. You further agree to follow applicable law and Marriott's policies, standards and procedures that are brought to your attention when handling any Personal Data to which you have access in the course of your relationship with Marriott. In particular, you will not access or use any Personal Data for any purpose other than in connection with and to the extent necessary for your work with Marriott. You understand that these obligations continue to exist after termination of your relationship with Marriott.

8. Reasons and Basis for Collection, Use, Transfer and Disclosure

Marriott collects and processes data about you: (i) because we are required to do so by applicable law; (ii) because such data is of particular importance to us and we have a specific legitimate interest under law to process it; (iii) because such data is necessary to fulfill the employment contract; or (iv) where necessary to protect the vital interests of any person. Marriott's legitimate interest in collecting and processing Personal Data is detailed at the end of this notice and includes, for example: (1) to ensure that our networks and data are secure; (2) to administer and generally conduct business within Marriott; and (3) to prevent fraud. Where none of these reasons apply, your decision to provide Personal Data to Marriott is voluntary, and we will process such data with your consent, which you may withdraw at any time.

9. Transfers and Use of Associate Data in the European Economic Area (EEA)¹

We may transfer Personal Data to countries located outside of the European Economic Area (“EEA”). Some of these countries are recognized by the European Commission as providing an adequate level of protection according to EEA standards (the full list of these countries is available [here](#)). For transfers from the EEA to other countries, we have put in place adequate measures, such as Privacy Shield to protect your data. Information on our Privacy Shield certification is noted in the “Privacy Shield Certified” section below.

10. Data Protection Officer Contact Information and Complaints

If you have any questions or concerns, please initiate your request with your Human Resources representative. We will investigate and attempt to resolve complaints and disputes regarding use and disclosure of Personal Data in accordance with the Privacy Shield Principles.

If you are not satisfied, you may contact the data protection officer responsible for your country or region via MarriottDPO@marriott.com. In your email, please indicate the country in which you are located. Additionally, you may lodge a complaint with a data protection authority for your country or region or where an alleged infringement of applicable data protection laws has occurred at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080.

You may also send your complaint to us via postal mail at:

Marriott International, Inc.
Data Protection Officer (DPO)
10400 Fernwood Road
Bethesda, MD 20817
United States of America

11. Privacy Shield Certified

Marriott has certified to the EU-U.S. and Swiss-U.S. Privacy Shield frameworks. Our certifications can be found at: www.privacyshield.gov/list. For more information about the Privacy Shield principles, please visit: www.privacyshield.gov. Our Privacy Shield Policy for HR Data can be found here: <https://www.marriott.com/about/applicantprivacy.mi>.

¹ The EEA includes EU countries and Iceland, Liechtenstein and Norway.

12. Changes to the Statement

Marriott reserves the right to amend this Statement at any time in order to address future business developments or changes in the industry or legal trends. Marriott will post the revised Statement on Marriott Global Source (MGS) or announce the change on the home page of this website. You can determine when the Statement was revised by referring to the “Last Updated” legend on the top of this Statement.

Types of Personal Data Marriott May Collect, Use, Transfer and Share

- **Personal Details:** Name, associate identification number, work and home or residential contact details (email, phone numbers, postal address) language(s) spoken, gender, date and place of birth, national identification number, social security number, nationality, marital/civil partnership status, domestic partners, dependents, disability status, emergency contact information and photograph.
- **Documentation Required under Immigration Laws:** Citizenship, passport data, details of residency or work permit.
- **Compensation and Payroll:** Base salary, bonus, benefits, compensation type, salary step within assigned grade, details on stock options, stock grants and other awards, type of currency, pay frequency, effective date of current compensation, salary reviews, banking details, working time records (including vacation and other absence records, leave status, hours worked and department standard hours), pay data and termination date.
- **Position:** Description of current position, job title, corporate status, management category, job code, salary plan, pay grade or level, job function(s) and subfunction(s), company name and code (legal employer entity), unit/department, location, employment status and type, full-time/part-time, terms of employment, employment contract, work history, hire/re-hire and termination date(s) and reason, length of service, retirement eligibility, promotions and disciplinary records, date of transfers and reporting manager(s) information.
- **Talent Management Data:** Details contained in letters of application and resume/CV (previous employment background, education history, professional qualifications, language and other relevant skills, certification, certification expiration dates), data necessary to complete a background check, details on performance management ratings, development programs planned and attended, e-learning programs, performance and development reviews, willingness to relocate, driver's license data and data used to populate associate biographies.
- **Management Records:** Details of any shares of common stock or directorships.
- **System and Application Access Data:** Data required to access Marriott systems and applications such as System ID, LAN ID, email account, instant messaging account, mainframe ID, previous associate ID, previous manager associate ID, system passwords, associate status, previous department details and electronic content produced using Marriott systems.
- **Sensitive Personal Data:** Marriott may also collect certain types of sensitive data only when permitted by local law, such as biometric, health/medical data, trade union membership information, religion and race or ethnicity. Marriott collects this data for specific purposes, such as health/medical information to accommodate a disability or illness and to provide benefits; religion or church affiliation in countries such as Germany where required for statutory tax deductions; and diversity-related Personal Data (such as gender, race or ethnicity) to comply with legal obligations and internal policies relating to diversity and anti-discrimination. Marriott will only use such sensitive data for the purposes listed below and as provided by law.

The Purposes for which Marriott May Collect, Use, Transfer and Share Personal Data

- **Managing Workforce:** Managing work activities and personnel generally, including: recruitment, hiring, appraisals, performance management, promotions and succession planning, rehiring, administering salary, and payment administration and reviews, wages and other awards such as stock options, stock grants and bonuses, healthcare, pensions and savings plans, training, leaves of absence, including for health-related reasons, promotions, transfers, secondments, honoring other contractual benefits, providing employment references, loans, performing workforce analysis and planning, performing associate surveys, performing background checks, managing disciplinary matters, grievances and terminations, reviewing employment decisions, making business travel arrangements, managing business expenses and reimbursements, planning and monitoring of training requirements and career development activities and skills, workforce reporting and data analytics/ trend analysis, and creating and maintaining one or more internal associate directories. Marriott may use workforce analytics for activities such as succession planning, workforce management, and data security among other programs. For instance, Marriott uses workforce analytics to assist in planning succession, to design associate retention programs and diversity initiatives, to offer training opportunities and to identify patterns in systems used to protect Marriott's people and property.
- **Communications, Security, Facilities and Emergencies:** Facilitating communication with associates, ensuring business continuity and crisis management, providing references, protecting the health and safety of associates and others, including: the use of cameras for video surveillance at the properties for security purposes, safeguarding and maintaining IT infrastructure by using various security tools, office equipment, facilities and other property, facilitating communication with you and your nominated contacts in an emergency.
- **Business Operations:** Operating and managing the IT, communications systems and facilities, managing product and service development, improving products and services, managing Marriott assets, allocating Marriott assets and human resources, strategic planning, project management, business continuity, compilation of audit trails and other reporting tools, maintaining records relating to business activities, budgeting, financial management and reporting, communications, managing mergers, acquisitions, sales, re-organizations or disposals and integration with purchaser.
- **Compliance:** Complying with legal and other requirements applicable to Marriott's business in all countries or regions in which Marriott operates, such as income tax and national insurance deductions, record-keeping and reporting obligations, conducting audits, compliance with government inspections and other requests from government or other public authorities, responding to legal process such as subpoenas, pursuing legal rights and remedies, defending litigation and managing any internal complaints or claims (including those received through the hotlines), conducting investigations including reported allegations of wrongdoing, policy violations, fraud, financial reporting concerns, and complying with internal policies and procedures.

- **Monitoring:** Monitoring compliance with internal policies and Code of Conduct, including pursuant to Marriott's policies and procedures with regard to monitoring activity in public places by CCTV, monitoring of telephone, email, Internet, instant messaging and other Marriott resources, and other monitoring activities as detailed in internal policies and/or permitted by local law.

The Categories of Unaffiliated Third Parties with whom Marriott May Share Personal Data

- **Service Providers:** Companies that provide products and services to Marriott such as payroll, pension scheme, benefits providers, human resources services, performance management, training, expense management, IT systems suppliers and support, third parties assisting with equity compensation programs, credit card companies, medical or health practitioners, trade bodies and associations, accountants, auditors, lawyers, insurers, bankers, and other outside professional advisors and service providers.
- **Public and Governmental Authorities:** Entities that regulate or have jurisdiction over Marriott such as regulatory authorities, law enforcement, public bodies and judicial bodies.
- **Corporate Transactions:** A third party in connection with any proposed or actual reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of Marriott business, assets or stock (including in connection with any bankruptcy or similar proceedings).