Associate Privacy Statement

Last Updated: June 19, 2025

1. **Introduction**

   The **Marriott Group**, which includes Marriott International, Inc. and its affiliates ("Marriott," "we," "our" or "Company"), is committed to protecting the Personal Data (as defined below) of our associates ("you" or "your"). Marriott operates in many different countries or regions, which has laws related to the collection, use, transfer, and sharing of individuals Personal Data, including associate related Personal Data.

   This Associate Privacy Statement (this "Statement") describes Marriott's practices in connection with the Personal Data we collect, use, transfer, and share from or about you. The Personal Data that Marriott collects from associates helps the Company in business planning and internal talent searches, in addition to supporting human resources and operational processes. However, this Statement does not apply to the Personal Data of contractors, consultants, franchised hotel employees, and business partners. Please see the **Marriott Group Non-Employee Privacy Statement** for more information.

2. **The Personal Data Marriott Collects, Uses, Transfers, and Shares**

   During your employment, Marriott may have collected or will collect data about you and your working relationship with the Company, or about your spouse, domestic/civil partner, or dependents ("Dependents"). Marriott refers to such data as "**Personal Data**." For more specific information regarding the 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 to you may include additional details or information. Marriott will not use the Personal Data of associates 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).

   Except certain Personal 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. However, if you do not provide certain required Personal Data, Marriott may not be able to accomplish some of the purposes outlined in this Statement.

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

3. **Access to Personal Data and Sharing with Third Parties**
   Access to associate Personal Data within Marriott is limited to: (i) personnel with a legitimate business need to know and may include your managers and their designees, personnel in Human Resources, Information Technology, Compliance, Legal, Finance & Accounting and Internal Audit, (ii) in accordance with Company policies, and (iii) for purposes described at the end of this Statement. However, 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.

   In some countries, owners may be employers of record. Owners therefore need access to limited Personal Data for compliance with their own legal obligations and for accounting and recordkeeping purposes. Owners are independently responsible for the processing of the Personal Data.

   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 your Personal Data 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; and
   - as advisable in light of Marriott's legal position (such as in regard of applicable statutes of limitations, litigation, or regulatory investigations).

6. **Individual Rights Requests**
   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 your Personal Data current and inform us of any significant changes. 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 during your relationship with Marriott. You will not access or use 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 necessary to fulfill the employment contract or otherwise necessary to establish and maintain your employment relationship with us; (iii) because such data is of particular importance to us, and we have a specific legitimate interest to process it; 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, to (1) ensure that our networks and data are secure; (2) administer and generally conduct business within Marriott; and (3) 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]**
   Due to the global nature of Marriott operations, we may share Personal Data with personnel and departments throughout the Company 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 or region where you are based.

   We may transfer Personal Data to countries or regions located outside of the European Economic Area ("EEA"). Some of these countries or regions are recognized by the European Commission as providing an adequate level of protection according to EEA standards (the full list of these countries or regions is available **here**↗). For the United Kingdom ("UK"), the full list of countries or regions recognized by the UK government as adequate is available **here**. For transfers from the EEA to other countries or regions, we have put in place adequate measures, Data Transfer Agreements, and/or Standard Contractual Clauses to protect your data.

10. **EU-U.S. Data Privacy Framework Certification**
    Marriott and certain of its U.S. affiliates have certified to the U.S. Department of

Commerce that it adheres to the EU-U.S. Data Privacy Framework ("EU-U.S. DPF") regarding the processing of Personal Data received from the EEA, the United Kingdom (which includes Gibraltar, hereinafter referred to as the "UK"), and Switzerland under the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (collectively the "DPF").

Our certifications can be found at **here**. For more information about the DPF, please visit: Data Privacy Framework. Our HR Data Privacy Framework Statement can be found at the bottom of this Statement.

11. **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 the processing of your Personal Data.

    If you are not satisfied, you may contact the data protection officer responsible for your country or region via Marriott DPO. In your email, please indicate the country or region 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 EC Europa Newsroom↗.

    You may also send your complaint to us via postal mail at:
    Marriott International, Inc.
    Data Protection Officer (DPO)
    7750 Wisconsin Avenue
    Bethesda, MD 20814
    United States of America

    If you work in the European Economic Area, the United Kingdom, or Switzerland, the data controller is Luxury Reservations Limited, with an address of:
    Luxury Reservations Limited
    10 Earlsford Terrance
    Dublin D02 T380
    Ireland

    If you work in the United Kingdom, the data controller is:

Marriott Hotels Limited
3 More London Riverside, 4th Floor
London SE1 2AQ
England

12. **Changes to this 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 this 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.
- **Information Required under Immigration Laws:** Citizenship, passport data, details of residency or work permit, and if applying for an employer-sponsored immigration benefit, any information required by the government agency adjudicating the work permit application.
- **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, Application, and Digital Communications Access Data:** Data required or used to access Marriott systems and applications such as unique identification numbers or codes (e.g., System ID, current and former associate EID, LAN ID, or IP address), email account, instant messaging account, system passwords, associate status, and previous department details. Marriott may also collect information included in files, emails or digital communications transmitted or stored on Marriott systems or applications, contents of communications on third-party instant messaging applications used for Marriott business purposes ("Third-Party Apps"), and electronic/digital content produced using Marriott systems or applications, or private devices connected to Marriott systems or applications (e.g., information on usage of IT systems including browser history and downloads, the presence of malware or suspicious user activity, and logs generated by security applications).
- **Sensitive Personal Data:** Marriott may also collect certain types of Sensitive Personal 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 or regions such as Germany where required for statutory tax deductions; and diversity-related Personal Data (such as gender, race, disability status, status as a protected

veteran, or ethnicity) to comply with legal obligations and internal policies relating to diversity and anti-discrimination. Marriott will only use such Sensitive Personal Data for the purposes listed below and in accordance with applicable law or local regulations.

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 coverage and benefits, pensions and savings plans, training, leaves of absence, including for health-related reasons, transfers, secondments, honoring other contractual benefits (such as making available other employee benefits), providing employment references, loans, performing workforce analysis, workforce planning, workforce scheduling activities, supporting business operations, 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, post-termination and alumni actions and communications, and creating and maintaining one or more internal associate directories. Marriott may use workforce analytics for activities such as succession planning, workforce management, data loss prevention and other data security measures. 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, safeguarding and maintaining IT Assets, facilitating communication with you and your nominated contacts in an emergency. For security, business continuity, crisis management and health and safety

purposes, video surveillance cameras may be deployed at Marriott properties.

- **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:**In accordance with applicable laws, Marriott will monitor and inspect IT Assets and Company Information (as defined in Company policies) to identify security threats, suspicious user activity, and ensure compliance with Marriott policies. Please be aware that all electronic communications (including telephone conversations, mail, or transmissions) and internet access or usage by associates using any electronic device or system provided for use in connection with Marriott's business may be monitored at any time, consistent with applicable laws and local regulations. This includes the associate's use of computers, Third-Party Apps, telephones, wires, radios, electromagnetic systems, photoelectronic systems, or photo-optical systems.

Further information regarding Marriott's approach to monitoring and inspection of IT Assets and Company Information:

- **Ownership of IT Assets**: IT Assets and Company Information are the sole and exclusive property of Marriott regardless of where they are used or accessed, including access from outside of a Marriott office, property, or facility. Use of passwords or encryption does not affect Marriott's ownership of Company Information or our right to access or monitor Company Information.
- **Use of IT Assets**: Use of IT Assets is subject to Marriott applicable policies and standards. In relation to your use of IT Assets and Company Information, Marriott may:
    - Log and review use of IT Assets, including but not limited to successful and failed logins; internet browsing; use of applications and services; access, use, modification, deletion, upload or download of Company Information; volume of data consumed or transmitted; calls made and received on company-issued or personally-owned mobile devices used to conduct Marriott business; attempts to download or install software on IT Assets; use of scripting and systems or network management tools; and date and time stamps of any of the foregoing. This includes when you use IT Assets on any Marriott or third-party network, or your personally owned device on Marriott's network.
    - Monitor, intercept, retrieve, search, review, analyze, and delete any messages or other content stored, created, or transmitted using IT Assets, either in real time or from storage. If you use IT Assets for personal purposes, you acknowledge that this applies to personal communications and content. Despite Marriott's efforts to avoid monitoring and inspecting purely personal content, using IT Assets for personal use (in countries or regions where Associates are permitted to use IT Assets for incidental personal use) may result in such monitoring, even if your Digital Communications are encrypted. Copies of Digital Communications may exist even after you delete them. Although Marriott does not seek to capture Sensitive Personal Data through its technology monitoring activities and takes appropriate steps to limit such processing, the monitoring may involve the incidental processing of Sensitive Personal Data in some cases.

- **Digital Communications via IT Assets**: Digital Communications, such as emails or instant messages using Company-provided Digital Communication services, the Company Network, or from Company-owned Devices sent, received, or stored on IT Assets do not grant personal, privileged, or confidential status or rights in such communications to the sender, recipient, or user of such messages. Digital Communications are generally not private communications. Associates should refrain from sending or receiving on IT Assets any Digital Communications that they would prefer to keep private. Associates have no right to privacy or to assert any privileges with respect to such Digital Communications, except as Company policies or applicable laws may provide. Marriott reserves the right to access, monitor, review, copy, and/or delete any such Digital Communications as permitted by law. Marriott also reserves the right to assert privileged or confidential status or rights in such communications as permitted by law.
- **Use of Third-Party Apps**: In accordance with applicable laws, Marriott may access, and review communications conducted over Third-Party Apps on any device an associate uses for business purposes (whether the device is a Company-owned Device or is the associate's personally owned device). By using Third-Party Apps, you agree to cooperate with investigations at Marriott, including by providing to investigators any mobile device and any Third-Party Apps you use for business-related communications. Although Marriott seeks to access and review only business-related communications, Marriott may incidentally access private or personal messages you send using Third-Party Apps. Please see *MIP-99, Associate Use of Third-Party Instant Messaging Applications for Business Communications*, for further information.

Marriott monitors and analyzes activities involving IT Assets and Company Information where we have a legitimate interest to do so, including our interests in: (i) meeting our obligations under the laws of the countries or regions where we operate; (ii) meeting our commitments to business partners, customers, associates and other parties; deterring, detecting, and (iii) mitigating threats to our workforce, facilities or information; protecting the confidentiality, integrity, and availability of IT Assets and Company Information; ensuring the proper use and performance of IT Assets; preventing, investigating, and addressing policy violations and unlawful activity; and for other purposes set out in this Privacy Statement. We also monitor to comply with our legal obligations (including but not

limited to those arising out of our role as an employer), and to establish, exercise or defend a legal claim in the case of litigation or regulatory investigations.

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 administrators and 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).

Related Links

Marriott Group Non-Employee Privacy Statement

California Consumer Privacy Act Addendum to Associate Privacy Statement

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

MARRIOTT HR DATA PRIVACY FRAMEWORK STATEMENT

Marriott International, Inc. and the U.S. affiliates listed at the end of this Statement ("Marriott U.S.", "we", "us", or "our".) have created this Data Privacy Framework Statement ("Privacy Statement") to help you learn about how we handle Human Resources ("HR") Personal Data that we receive from our affiliates, Owners, and Franchisees located in the European Economic Area (the "EEA"), the United Kingdom ("UK"), Gibraltar, and Switzerland under the EU-U.S. Data Privacy Framework ("EU-U.S. DPF"), the UK Extension to the EU-U.S. DPF (which includes Gibraltar, hereinafter referred to as the "UK"), and the Swiss-U.S. Data Privacy Framework (collectively "DPF"). This DPF Privacy Statement supplements the Associate Privacy Statement. Unless specifically defined differently in

this Statement, capitalized terms in this DPF Privacy Statement have the same meaning as in the Associate Privacy Statement.

Marriott U.S. has certified to the U.S. Department of Commerce that it adheres to the DPF with regard to the processing of associate Personal Data received from the EEA, the UK, and Switzerland in reliance on the DPF. More information about the DPF, including the list of certified organizations, can be found at Data Privacy Framework.

Personal Data Received From the EEA, United Kingdom, and Switzerland

Marriott U.S. may receive Personal Data of associates ("you" or "your") from entities in the EEA, UK, and Switzerland as further described in our Associate Privacy Statement.

Use of Personal Data

Any Personal Data collected by Marriott U.S. may be used by Marriott U.S. and its agents for the purposes indicated in the Associate Privacy Statement. If we intend to use your Personal Data for a purpose that is materially different from these purposes, or if we intend to disclose it to a third party (a non-agent) not previously identified, we will notify you and offer you the opportunity to opt-out of such uses and/or disclosures where it involves Personal Data or opt-in where Sensitive Personal Data are involved.

Disclosures to Affiliates and Third Parties

As more fully described in the Associate Privacy Statement, Personal Data may be disclosed to the following:

- **Marriott Group**
- **Owners:** Owners of Marriott Group branded properties that we manage
- **Service Providers:**Companies that provide products and services to Marriott such as payroll, pension scheme, benefits administrators and 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).

Disclosures to Service Providers

Service Providers acting as agents may have access to Personal Data needed to perform their functions but are restricted from using the Personal Data for purposes other than providing services for us or to us. Marriott U.S. requires that its Service Providers that have access to Personal Data received from the EEA, the UK, and Switzerland provide the same level of protection as required by the DPF. We are responsible for ensuring that our Service Providers process the Personal Data in a manner consistent with our obligations under the DPF.

Data Security

We use reasonable physical, electronic, and administrative safeguards to protect your Personal Data from loss, misuse and unauthorized access, disclosure, alteration, and destruction, taking into account the nature of the Personal Data and the risks involved in processing that information.

Data Integrity and Purpose Limitation

We limit the collection and use of Personal Data to the information that is relevant for the purposes of processing and will not process Personal Data in a way that is incompatible with the purposes for which the information has been collected or subsequently authorized by you. We take reasonable steps to ensure Personal Data are reliable for their intended use, accurate, complete and current to the extent necessary for the purposes for which we use the Personal Data.

Access to Personal Data

If you want to access, correct, or delete the Personal Data we maintain about you, please initiate your request through your local Human Resources representative.

Data Privacy Framework Enforcement and Dispute Resolution

If non-Marriott associates have any questions or concerns about their Personal Data, they should contact the appropriate representative. Current associates of Marriott should contact the Human Resources function at their location. Former associates should contact the Data Privacy Office at MarriottDPO@marriott.com.

If we are unable to resolve your complaints or disputes, you may submit a complaint directly to your local data protection authority (i.e., EU/EEA Member State data protection authority; UK Information Commissioner's Office; Gibraltar Regulatory Authority; or the Swiss Federal Data Protection and Information Commissioner and they will investigate and assist you free of charge in resolving your complaint.

As further explained in the DPF Program, a binding arbitration option is also available to you in order to address residual complaints not resolved by any other means. Marriott U.S. is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission.

Disclosures Required by Law

We may need to disclose Personal Data in response to lawful requests by public authorities for law enforcement or national security reasons or when such action is necessary to comply with a judicial proceeding or court order, or when otherwise required by law.

Contact Information

If you have any questions regarding this DPF Privacy Statement, please contact your local Human Resources representative, or contact the data protection officer responsible for your country or region via Marriott DPO. In your email, please indicate the country or region from which you are contacting us. You may also write to the data protection officer at the following address:

Marriott International, Inc.
Global Compliance, Privacy
7750 Wisconsin Avenue
Bethesda, MD 20814
United States of America

Privacy Statement Changes

This Policy may be changed occasionally, consistent with the Data Privacy Framework Program requirements. You can determine when this Policy was last revised by referring to the "LAST UPDATED" legend at the top of this page. Any changes to our Statement will become effective upon our posting of the revised Statement on the Site.

Marriott U.S. Entities Covered by this Statement

Marriott International Administrative Services, Inc.

Marriott Rewards, Inc.

Marriott Payment Services LLC