



**MILLENNIUM**  
HOTELS AND RESORTS

**PRIVACY NOTICE (EU)**  
**FOR EMPLOYEES, WORKERS AND CONTRACTORS**

## 1. BACKGROUND STATEMENT

1.1 Millennium & Copthorne Hotels plc and its direct and indirect subsidiaries (“MHR”, “we”, “us” or “our”) is committed to protecting the privacy and security of your personal information.

1.2 This Privacy Notice (“**the Notice**”) applies to individuals who work for us, whether employed by us or not, and describes how we collect and use personal information about you during and after your working relationship with us, and also about those who apply to work with us, in accordance with the EU General Data Protection Regulation (“**GDPR**”), any successor legislation to the Data Protection Act 1998 and the GDPR in the United Kingdom, and in particular the Data Protection Bill 2017-2019, once it becomes law; including where applicable, any guidance notes and codes of practice issued by the European Commission and applicable national regulators, including the UK Information Commissioner (the “**Data Protection Laws**”).

1.3 In brief, this Notice explains the following:

1. **BACKGROUND STATEMENT**
2. **STATUS OF THIS NOTICE**
3. **DEFINITION OF DATA PROTECTION TERMS**
4. **DATA PROTECTION PRINCIPLES**
5. **WHAT PERSONAL DATA WE HOLD AND WHY WE PROCESS IT**
6. **HOW WE OBTAIN YOUR DATA**
7. **WHO GETS TO SEE YOUR DATA**
8. **TRANSFERS OF PERSONAL DATA OUTSIDE THE EEA**
9. **HOW WE PROTECT YOUR PERSONAL DATA**
10. **HOW LONG WE KEEP YOUR PERSONAL DATA**
11. **ACCESS TO YOUR PERSONAL DATA AND OTHER RIGHTS**
12. **COMPLAINTS**
13. **DATA BREACHES**
14. **TRAINING ON THIS NOTICE**
15. **REVIEW OF THIS NOTICE**

## 2. STATUS OF THIS NOTICE

2.1 This Notice does not form part of any employee's contract of employment and does not create contractual rights or obligations. It may be amended by MHR at any time. If we do so, we will provide you with an updated copy of this Notice as soon as reasonably practical. Nothing in this notice is intended to create an employment relationship between us and any non-employee providing services to us.

2.2 This Notice sets out our rules on data protection and the minimum requirements with which all group members of MHR (each a “**group member**”), including their corporate employees and the employees of MHR owned and managed hotels, must comply in relation to their processing of Personal Data of employees, workers and contractors. Any breach of the obligations under this Notice will be taken seriously and may result in disciplinary action against the relevant breaching group member(s) and/or employee(s). MHR may, from time to time, conduct audits and inspections, to ascertain and ensure compliance with such requirements.

2.3 The recipients of Personal Data can be any group member of MHR and such group member will be bound by this Notice. A list of all such group members, and where the companies are located, can be found in MHR's latest Annual Report and Accounts.

2.4 If you are starting a new business activity that involves the processing of Personal Data of employees, workers and/or contractors, have any questions or concerns about the operation of this Notice, or if you consider that the requirements under this Notice have not been followed in respect of data about yourself or others, you should refer the matter, in the first instance, to a member the Human Resources team or Legal Department. If you do not feel comfortable raising the matter with any of those individuals or an issue remains unresolved after doing so, please contact the Head of Internal Audit or the Company Secretary.

### 3. DEFINITION OF DATA PROTECTION TERMS

The following definitions apply to this Notice. The terms and definitions may vary in each country depending on each country's relevant Data Protection Laws, but even if this is the case in your country, please ensure that you continue to adhere to the minimum standards set out in this Notice based on the following definitions.

- (a) **"Data"** includes all forms of information, whether held on paper, in electronic form, on magnetic or audio devices, or in photographic, digital or other media that is capable of being accessed and read
- (b) **"Personal Data"** means any information relating to an identified or identifiable natural living person (**"data subject"**); an identifiable natural living person is one who can be identified, directly or indirectly (including any data processed automatically), in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- (c) Reference to **"processed automatically"** in section 3(b) above means any Personal Data that is collected automatically by technical processes including by CCTV and when you use devices such as a laptop or mobile phone or access a building using an electronic key card, etc.
- (d) **"Processing"** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal Data to third parties.
- (e) Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health, sexual orientation, sex life, trade union membership and genetic and biometric data are subject to special protection and considered by EU privacy law to be **"special categories"** of Personal Data or **"sensitive Personal Data"**.

References in the Notice to "employment," "work" and similar expressions include any arrangement we may have under which an individual works for us or provides us with services. By way of example, when we mention an "employment contract," that includes a contract under which you provide us with services; when we refer to ending your employment, this includes terminating a contract for services.

We use the word "you" to refer to anyone within the scope of this Notice.

### 4. DATA PROTECTION PRINCIPLES

We, and those who work for us, will comply with Data Protection Laws. As such, the Personal Data we hold about you must be:

- (a) Used lawfully, fairly and in a transparent way
- (b) Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes
- (c) Relevant to the purposes about which we have informed you and limited only to those purposes
- (d) Accurate and kept up to date
- (e) Kept only as long as necessary for the relevant purposes
- (f) Kept securely

### 5. WHAT PERSONAL DATA WE HOLD AND WHY WE PROCESS IT

We process data for the purposes of our business, including management, administrative, employment and legal purposes. We set out below specific information on these purposes, on the type of data that may be processed and on the grounds on which we process data.

## 5.1 The kind of information we hold about you

We may collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses
- Date of birth
- Gender
- Marital status and dependants
- Next of kin and emergency contact information
- National Insurance number (NIS), Social Security
- Education and training
- Recruitment information (including copies of right to work documentation, references, qualifications and any other information included in a CV or cover letter or as part of the application process)
- Copy of passport/driving license/ID card
- Employment records (including job titles, work history, working hours, holidays, training records and professional memberships)
- Photographs
- Salary, annual leave, pension and benefit schemes information
- Performance management records
- Compensation history including bonus
- Leave information (e.g. parental leave, annual leave, etc.)
- CCTV footage and other information obtained through electronic means, such as swipe card records
- Disciplinary and grievance information
- Bank account details, payroll records and tax status information
- Mobile phone tracking data
- Electronic identification data, such as IP address, login data, cookies, etc.
- Location of employment or workplace
- Start date and, if different, the date of your continuous employment
- Leaving date and your reason for leaving
- Any other information as required from time to time

We also may collect, store and use the following "special categories" of more sensitive personal information:

- Diversity information (including information about your race or ethnicity, religious beliefs, sexual orientation, political opinions)
- Information about your health, including any medical condition and health and sickness records, particularly:
  - ✓ in the event you leave employment and under any share plan operated by an MHR group company the reason for leaving is determined to be ill-health, injury or disability, the records relating to that decision;
  - ✓ details of any absences (other than holidays) from work, including any statutory parental leave and sick leave;
  - ✓ in the event you leave employment and the reason for leaving is related to your health, information about that condition needed for pensions and permanent health insurance purposes; and
  - ✓ Any occupational health reports obtained during the course of your employment
- Information about criminal convictions and offences

## 5.2 Legal grounds for processing your Personal Data

### (a) *Legal grounds for processing Personal Data under Data Protection Laws*

Under Data Protection Laws, there are various grounds pursuant on which we can rely when processing your Personal Data. In some contexts more than one ground will apply. We have summarised these grounds as "Contract," "Legal obligation," "Legitimate interests" and "Consent", and outline what those terms mean in the following table.

Term	Ground for processing	Explanation
Contract	Processing necessary for performance of a contract with you or to take steps at your request to enter a contract	This covers carrying out our contractual duties and exercising our contractual rights
Legal obligation	Processing necessary to comply with our legal obligations	Ensuring we perform our legal and regulatory obligations. For example, providing a safe place of work and avoiding unlawful discrimination
Legitimate interests	Processing necessary for our or a third party's legitimate interests	We or a third party have legitimate interests in carrying on, managing and administering our respective businesses effectively and properly and in connection with those interests processing your data  Your data will not be processed on this basis if our or a third party's interests are overridden by your own interests, rights and freedoms
Consent	You have given specific consent to processing your data	In general processing of your data in connection with employment is not conditional on your consent, but there may be occasions where we do specific things such as provide a reference, deduct union dues or obtain medical reports and may rely on your consent to our doing so

*(b) Our purposes for processing your Personal Data*

We outline below the purposes for which we process your Personal Data. More specific information on these purposes, the types of data and the grounds pursuant to which we process your data are in the table below. Please note that this is not an exhaustive list.

Purpose	Types of Personal Data that may be processed	Grounds for processing
Recruitment	Standard data related to your identity (e.g., your name, address, email address, ID information and documents, telephone numbers, place of birth, nationality, contact details, professional experience and education (including university degrees, academic records, professional licenses, memberships and certifications, awards and achievements, and current and previous employment details), financial information (including current salary information) language skills, and any other Personal Data that you present us with as part of your application related to the fulfilment of the role  Information concerning your application and our assessment of it, your references, any checks we may make to verify information provided or background checks and any information connected with your right to work  If necessary, information concerning your health, any disability and in connection with any adjustments to working arrangements  Information relating to criminal convictions and offenses	Contract Legal obligation Legitimate interests
Your employment contract, including entering it, performing it and changing it	Information on your terms of employment from time to time, including your pay and benefits, such as your participation in pension arrangements, life and medical insurance; and any bonus or share schemes.	Contract Legal obligation Legitimate interests
Contacting you or others on your behalf	Your address and phone number, emergency contact information and information on your next of kin	Contract Legitimate interests

Purpose	Types of Personal Data that may be processed	Grounds for processing
Payroll administration	<p>Information on your bank account, pension contributions and on tax and national insurance</p> <p>Information on attendance, holiday and other leave and sickness absence</p>	<p>Contract Legal obligation Legitimate interests</p>
Supporting and managing your work and performance and any health concerns	<p>Information connected with your work, anything you do at work and your performance, including records of documents and emails created by or relating to you and information on your use of our systems, such as computers, laptops or other devices</p> <p>Management information regarding you including notes of meetings and appraisal records</p> <p>Information relating to your compliance with our policies</p> <p>Information concerning disciplinary allegations, investigations and processes and relating to grievances in which you are or may, directly or indirectly, be involved</p> <p>Information concerning your health, including self-certification forms, fit notes and medical and occupational health reports</p>	<p>Contract Legal obligation Legitimate interests</p>
Changing or ending your working arrangements	<p>Information connected with anything that may affect your continuing employment or the terms under which you work including any proposal to promote you, to change your pay or benefits, to change your working arrangements or to end your employment</p>	<p>Contract Legitimate interests</p>
Physical and system security	<p>CCTV images; records of use of swipe and similar entry cards; records of and log-in information related to your use of our systems, including computers, phones and other devices</p>	<p>Legal obligation Legitimate interests</p>
Providing references in connection with your finding new employment	<p>Information on your working for us and on your performance.</p>	<p>Consent Legitimate interests</p>
Providing information to third parties in connection with transactions that we contemplate or carry out	<p>Information on your contract and other employment data that may be required by a party to a transaction such as a prospective purchaser, seller or outsourcer</p>	<p>Legitimate interests</p>
Monitoring of diversity and equal opportunities	<p>Information on your nationality, racial and ethnic origin, gender, sexual orientation, religion, disability and age</p>	<p>Legitimate interests</p>
Monitoring and investigating compliance with policies and rules – both generally and specifically	<p>We expect our employees to comply with our policies and rules and may monitor our systems to check compliance (e.g., rules on accessing pornography at work)</p> <p>We also may have specific concerns about compliance and check system and other data to look into those concerns (e.g., log-in records, records of usage and emails and documents, CCTV images, etc.)</p>	<p>Legitimate interests</p>
Day to day business operations including marketing and customer/client relations	<p>Information relating to the work you do for us, your role and contact details including relations with current or potential customers or clients; this may include a picture of you for internal or external use</p>	<p>Legitimate interests</p>
Maintaining appropriate business records during and after your employment	<p>Information relating to your work, anything you do at work and your performance relevant to such records</p>	<p>Contract Legal obligation Legitimate interests</p>

Purpose	Types of Personal Data that may be processed	Grounds for processing
Disputes and legal proceedings	Any information relevant or potentially relevant to a dispute or legal proceeding affecting us	Legitimate interests Legal obligation

### 5.3 Processing sensitive Personal Data

If we process sensitive Personal Data about you (for example, but without limitation, storing your health records to assist us in ensuring that we provide you with a healthy and safe work workplace or processing Personal Data relating to diversity monitoring), then as well as ensuring that one of the grounds for processing mentioned above applies, we will make sure that one or more of the grounds for processing sensitive Personal Data applies. In outline, these include:

- Processing being necessary for the purposes of your or our obligations and rights in relation to employment in so far as it is authorised by law or collective agreement;
- Processing relating to data about you that you have made public (e.g. if you tell colleagues that you are ill);
- Processing being necessary for the purpose of establishing, making or defending legal claims;
- Processing being necessary for provision of health care or treatment, medical diagnosis, and assessment of your working capacity; and
- Processing for equality and diversity purposes to the extent permitted by law.

As a general guideline, it is appropriate to exercise greater care and caution when handling sensitive Personal Data, such as identity document numbers. Identity document numbers of individuals, for instance, should not be collected if there are available alternatives (e.g., a telephone number or a unique employee number) that can serve the same purpose, unless required by law (e.g., right to work checks).

## 6. HOW WE OBTAIN YOUR DATA

When you start employment with us, the initial data about you that we process is likely to come from you: for example, contact details, bank details and information on your immigration status and whether you can lawfully work in the relevant jurisdiction. We also may require references and information to carry out background checks. In the course of employment, you may be required to provide us with information for other purposes such as assessing sick pay (or statutory sick pay) and family rights (e.g., maternity and paternity leave and pay). If you do not provide information that you are required by statute or contract to give us, you may lose benefits or we may decide not to employ you or to end your contract. If you have concerns about this in a particular context, you should speak to a representative in the Human Resources department.

In the course of your work, we may receive Personal Data relating to you from others. Internally, Personal Data may be derived from your managers and other colleagues or our IT systems; externally, it may be derived from our customers or those with whom you communicate by email or other systems.

## 7. WHO GETS TO SEE YOUR DATA

### 7.1 Internal use

Your Personal Data may be disclosed to your managers, Human Resources team members and administrators for employment, administrative and management purposes as mentioned in this Notice.

We also may disclose your Personal Data to other group members as part of our regular administrative, reporting and assessment activities, in the context of a business reorganisation or group restructuring exercise, for system maintenance and support and/or the hosting of data. For instance, we will share Personal Data relating to your participation in any share plan or pension scheme operated by a group member with those companies (and other group members), including Directors of Millennium & Copthorne Hotels plc who are members of the Remuneration Committee and Directors of the pension trustee, for the purposes of administering the share plans and pension schemes. Also, as senior executives of MHR are often employed in other jurisdictions, by different

group members, Personal Data relating to your performance may be shared with them as part of the group's performance management processes, such as bonus assessments.

## 7.2 External use

- (a) We will only disclose your Personal Data outside the group if disclosure is consistent with a ground for processing on which we rely and doing so is lawful and fair to you.

We may disclose your data if it is necessary for our legitimate interests as an organisation or the interests of a third party (but we will not do this if these interests are over-ridden by your interests and rights in particular to privacy). We also may disclose your Personal Data if you consent, where we are required to do so by law and in connection with criminal or regulatory investigations.

- (b) Specific circumstances in which your Personal Data may be disclosed include:
- Disclosure to organisations that process data on our behalf such as our payroll provider, currently ADP, insurers and other benefit providers, administrators of our share schemes, including Equiniti, providers of training and compliance programmes, our banks and organisations that host or service our IT systems and data (including property management systems, finance systems and email systems);
  - Disclosure to external recipients of electronic communications (such as emails) which contain your Personal Data;
  - Disclosure on a confidential basis to a potential buyer of our business or company for the purposes of evaluation, but only if we were to contemplate selling;
  - Disclosure as necessary to respond to law enforcement agency requests or where required by applicable laws, pursuant to court orders, or arbitral or tribunal orders or rules of procedure, or to government departments or agencies or regulatory bodies (including to tax authorities, such as disclosures to HM Revenue & Customs in connection with share scheme filings, immigration authorities, employment tribunals, pension regulators and any other regulatory bodies);
  - Disclosure on a confidential basis to our advisers for example to our lawyers for the purposes of seeking legal advice or to further our interests in legal proceedings and to our accountants for auditing purposes; and
  - Disclosure of aggregated and anonymised diversity data to relevant regulators as part of a formal request.
- (c) All of our third-party service providers and our group members are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your Personal Data for marketing purposes. We only permit them to process your Personal Data for specified purposes and in accordance with our instructions.

## 8. **TRANSFERS OF PERSONAL DATA OUTSIDE THE EEA**

- 8.1 We may transfer your Personal Data outside the EEA, where necessary and as set out in this privacy notice, to members of our group in Asia (particularly Singapore) and North America in connection with our business and for employment, administrative, management and legal purposes.

In relation to intra-group transfers, the members of our group of companies have entered into an intra-group data sharing agreement ensuring appropriate and suitable safeguards with our controllers/processors outside the EEA. These are in standard terms approved by the European Commission. If you wish to know more about details of these safeguards, please consult with a member of the Legal Department.

- 8.2 We may transfer your Personal Data outside the EEA to our global Human Resources systems provider, which currently processes data in the U.S. and in India, in order to perform our contract with you.
- 8.3 We will ensure that the transfers are lawful and that there are appropriate security arrangements in



place. To ensure that your personal information does receive an adequate level of protection we have put in place the EU Standard Contractual Clauses requiring that your personal information is treated by those third parties in a manner that is consistent with, and which respects, the EU laws on data protection.

A list of data recipients who receive material amounts of Personal Data and are located outside of the EEA is set out below.

MHR recipients located outside the EEA	Country
Millennium & Copthorne International Limited	Singapore
M&C Hotel Interests, Inc.	United States

Third party recipients located outside the EEA	Country
ADP	United States and India

## 9. HOW WE PROTECT YOUR PERSONAL DATA

- 9.1 We have put in place measures to protect the security of your information against unlawful or unauthorised access, collection, use, disclosure, copying, modification, disposal, loss and damage, and other similar risks. Please refer to the relevant policies and procedures such as policies governing the use of company devices, equipment and systems which can be obtained from your Human Resources department.
- 9.2 Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.
- 9.3 We limit access to your personal information to only those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to duties of confidentiality.

## 10. HOW LONG WE KEEP YOUR PERSONAL DATA

- 10.1 We will only retain your Personal Data for as long as necessary to fulfil the purposes for which we collected it, including for the purposes of satisfying any legal, accounting, or reporting requirements. Therefore, we do not keep your Personal Data for any specific period, but will not keep it for longer than is necessary for our purposes. In general, we will keep your Personal Data for the duration of your employment and for a period afterwards.
- 10.2 In considering how long to keep your Personal Data, we will take into account its relevance to our business and your employment either as a record or in the event of a legal claim. If your data is only useful for a short period of time (for example, CCTV or a record of a holiday request). Personal Data relating to job applicants (other than those who are subsequently hired) will normally be deleted after 12 months. Please refer to our records retention policy for further details.

## 11. ACCESS TO YOUR PERSONAL DATA AND OTHER RIGHTS

### 11.1 Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

### 11.2 Your rights in connection with Personal Data

Under certain circumstances, by law you have the right to:

- Request access to your Personal Data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- Request correction of the Personal Data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your Personal Data. This enables you to ask us to delete or remove

personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below). However, note that in such instances we may retain your information for a period of time for legal or regulatory reasons.

- Object to processing of your Personal Data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation that makes you want to object to processing on this ground. Should we receive such an objection, we will assess the legitimate interest against your reasons for objecting and make a determination on any future processing, acting fairly. You also have the right to object where we are processing your Personal Data for direct marketing purposes.
- Request the restriction of the processing of your personal information. This enables you to ask us to suspend processing, for example if you want us to establish the accuracy of your Personal Data or the reason for processing it.
- Request the transfer of your Personal Data to another party, subject to the rights of others and any legal or other privilege that may attach to such data.
- Right to withdraw consent. In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your Personal Data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Human Resources department or send an email to [dataprivacy@millenniumhotels.com](mailto:dataprivacy@millenniumhotels.com). Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes to which you originally agreed unless we have another legitimate basis for doing so.

If you want to review, verify, correct or request erasure of your Personal Data, object to the processing of it, or request that we transfer a copy of your personal information to another party, please contact the Human Resources department in writing or send an email to [dataprivacy@millenniumhotels.com](mailto:dataprivacy@millenniumhotels.com).

You will not have to pay a fee to access your Personal Data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access your Personal Data (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

## 12. COMPLAINTS

If you have complaints relating to our processing of your Personal Data, you should raise these with the Human Resources department in the first instance or you may send an email to [dataprivacy@millenniumhotels.com](mailto:dataprivacy@millenniumhotels.com) or contact the Company Secretary should you not feel comfortable raising your concerns with another party.

You also may raise complaints with the supervisory authorities or regulators in your respective country. In the UK, that the appropriate authority is the Information Commissioner's Office (<https://ico.org.uk/>). For contact details of the relevant authorities in other jurisdictions, please consult with a representative from the Human Resources team or Legal Department.

## 13. DATA BREACHES

- 10.1 We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.
- 10.2 We maintain an incident response plan, which identifies roles and responsibilities, contacts and procedures to respond to suspected attacks and breaches, in accordance with our Data Breach Policy (located at <https://www.millenniumhotels.com/en/corporate/groupolicies/>).
- 10.3 Each member of the Human Resources team and Legal Department is aware of MHR's crises response procedures should a data breach occur. If you believe Personal Data may have been lost

or stolen, you should notify one of these team members immediately.

**14. TRAINING ON THIS NOTICE**

All staff shall be required to complete online Personal Data protection training. More specialised training on the operation of this Notice will be provided to specific employees as necessary.

**15. REVIEW OF THIS NOTICE**

We will continue to review the effectiveness of this Notice on an annual basis to ensure it is achieving its stated objectives.

Please sign and return to the Human Resources department, retaining an original for your own records.

I have read and understood the contents of this Notice:

Signed: \_\_\_\_\_ Print name: \_\_\_\_\_ Date: \_\_\_\_\_