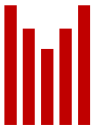

MILLENNIUM

HOTELS AND RESORTS

MILLENNIUM ▪ COPTHORNE

Global Data Protection Policy

1. Policy Statement

1.1 The Millennium & Copthorne Hotels plc group ("**MHR**", "**we**", "**us**" or "**our**"), including its direct and indirect subsidiaries (each a "**group member**"), are committed to protecting the privacy and security of the personal data of those who are employed by or otherwise work for MHR group members and former and prospective employees, as well as personal data we collect and process pertaining to other individuals, including our customers and guests, suppliers, service providers, and shareholders (collectively "**Covered Parties**" or each a "**Covered Party**").

1.2 This Global Data Protection Policy ("**Policy**") describes our rules on data protection and in particular how we collect and process personal data about Covered Parties in accordance with the EU General Data Protection Regulation ("**GDPR"**), UK Data Protection Act 2018 and the Singapore Personal Data Protection Act 2012 ("**PDPA**")—as those laws generally are considered to be the strictest data protection laws applicable to MHR and its operations—including where applicable, any guidance notes and codes of practice issued by the European Commission and applicable national regulators; and any other regulations, laws, statutes, rules and guidelines in any other jurisdictions in which we operate (collectively, the "**Data Protection Laws**")

1.3 Each MHR operating region has, or shall establish, a dedicated data privacy working group comprised of members from the legal, information technology and operations teams and, in most cases, other functional departments (each a "**Regional Compliance Team**"). The remit of these Regional Compliance Teams is to monitor regional compliance with this Policy and to develop, implement, monitor and update the data privacy policies and procedures for the local jurisdictions in which MHR operates within each region. In addition, MHR has appointed a data privacy compliance officer for certain jurisdictions. Information about the Regional Compliance Teams, including a list of their members for each region, and the current data privacy compliance officers can be found at https://www.millenniumhotels.com/en/corporate/grouppolicies/.

Table of Contents

2. STATUS OF THE POLICY

2.1 This policy sets out our corporate rules on data protection and the minimum requirements with which all MHR group members, including their employees and the employees of MHR owned and managed hotels (referred to in this Policy as "**you**"), must comply in relation to our collection, storage and processing of personal data of Covered Parties. This Policy shall be applicable to and enforced by, every MHR group member. A list of all MHR group members, and where the companies are located, can be found in MHR's latest Annual Report and Accounts (located at https://investors.millenniumhotels.com/financial/annual-reports). This Policy does not form part of any employee's contract of employment, and does not create any contractual rights or obligations between MHR group members, as employers, on the one hand and employees, on the other hand. Nothing in this Policy is intended to create an employment relationship between us and any non-employee providing services to us.

2.2 Any breach of this Policy will be taken seriously and may result in disciplinary action against the relevant MHR group member(s) and/or employee(s). MHR may, from time to time, conduct audits and inspections to ascertain and ensure compliance with this Policy.

2.3 We may update or amend this Policy at any time and if we do so, we will endeavor to notify you as soon as possible. The most recent version of this Policy can be downloaded from https://www.millenniumhotels.com/en/corporate/grouppolicies/.

3. DEFINITION OF DATA PROTECTION TERMS

The following definitions apply to this Policy. 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 Policy based on the following definitions.

(a) "**Controller**" is a person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

(b) "**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.

(c) "**EU/EEA**" means those countries within the European Union and the European Economic Area, as such areas may be defined from time to time.

(d) "**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 through 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.

Personal data includes data, whether true or not, about an individual who can be identified (i) from that data, or (ii) from that data and other information to which we have or are likely to have access. Personal data can be factual or it can be an opinion (such as a performance appraisal).

The Data Protection Laws in some jurisdictions, including Singapore, require that the obligations and guidelines in this Policy relating to the disclosure and protection of personal data apply to the personal data of *deceased individuals*. In such event, this Policy shall apply only to personal data of those deceased individuals who have been deceased for ten (10) years or less, unless a longer period is required under local requirements. Care should be

taken to ensure you adhere to such requirements to the extent they apply to the jurisdictions in which you collect and process data.

(e) Reference in this Section to personal data being "**processed automatically**" or to "**automatic processing**" means the automatic collection of personal data by technical processes, including by CCTV and devices such as a laptop or mobile phone or an electronic key card used to access a building or room, etc.

(f) "**Processing**" is any activity that involves use of the data. It refers to obtaining, recording or holding the data, or carrying out any operation or set of operations on the data, whether through automatic processing or otherwise, including collecting, organising, amending, retrieving, using, disclosing, combining, storing, erasing or destroying it. Processing also includes transferring personal data to third parties.

(g) "**Processor**" is a person, public authority, agency or other body which processes personal data on behalf of the controller.

(h) 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 may be considered under certain Data Protection Laws, such as GDPR, to constitute "**special categories**" of personal data or "**sensitive personal data**".

4. APPLICATION OF LOCAL LAWS

This Policy is designed to assist you and the MHR group members in your efforts to comply with the GDPR and the PDPA in particular. However, we recognise that the laws of certain other countries or jurisdictions might impose more specific or stricter standards, in which case the more specific or stricter standards shall apply in addition to the requirements under this Policy. All relevant MHR group members must handle personal data in accordance with the local laws applicable to the locations where personal data are collected and processed.

For the avoidance of doubt, any processing of personal data relating to Covered Parties may be subject to the GDPR in the event that (i) a MHR group member acting as a controller is located in the EU/EEA (regardless of whether the processing takes place in the EU/EEA); or (ii) a MHR group member, which is not established in the EU/EEA, but which is acting as a controller or processor, processes personal data related to Covered Parties who are located in the EU/EEA

5. DATA PROTECTION PRINCIPLES

We must comply with Data Protection Laws. As such, the personal data we collect and hold about Covered Parties is required to be:

(a) Used lawfully, fairly and in a transparent way;

(b) Collected only for valid purposes that we have clearly explained to the Covered Parties and not used in any way that is incompatible with those purposes;

(c) Relevant to the purposes about which we have informed the Covered Parties and limited only to those purposes;

(d) Accurate and kept up to date;

(e) Kept only as long as necessary for the purposes about which we have told the Covered Parties; and

(f) Kept securely.

6. OUR OBLIGATIONS REGARDING THE COLLECTION AND PROCESSING OF YOUR PERSONAL DATA

As employers, MHR group members collect and process your personal data for the purposes of our business, including for management, administrative, employment and legal purposes. For employees, workers and contractors of group members located in the EU/EEA, please refer to the Privacy Notice (EU) for Employees, Workers and Contractors for a description of the personal data we collect about you, how we process such data and the purposes for which we process it, our legal grounds for processing it, and your rights in respect of such data. For employees, workers and contractors of group members located in other jurisdictions, please contact a member of your human resources department for such information.

7. YOUR OBLIGATIONS REGARDING THE COLLECTION AND PROCESSING OF PERSONAL DATA OF COVERED PARTIES

Not only do MHR group members, as employers, have obligations to you with regard to your personal data, but to the extent you collect or process personal data of Covered Parties—including other employees, customers and guests, suppliers, service providers and shareholders—as part of your role, then you have certain responsibilities in respect of those activities. This Section 7 summarises how we expect you to apply the principles prescribed by the Data Protection Laws and the general requirements underpinning those principles. The specific requirements applicable to some of the most common data collection and processing activities performed by MHR group members are contained in Section 8 below.

7.1 New business activities and Data Protection Impact Assessments

(a) If you are considering a new business activity or initiative that involves the collection or processing of personal data of Covered Parties, such as the development of a new loyalty programme or new booking channel, we may be required, as an initial step, to perform a formal Data Protection Impact Assessment ("DPIA") if the new activity or initiative is likely to result in a high risk to the rights and freedoms of the data subjects involved.

(b) A DPIA will need to consider the reasons for the proposed activity or initiative, the nature of the personal data to be collected and how it will be processed, the legal bases for such processing, how the processing will impact the data subject and whether the impact is proportionate to any concerns identified through the DPIA.

Please refer to our 'Guidance for DPIA' and 'DPIA template', both can be found on www.millenniumhotels.com/en/corporate/grouppolicies.

7.2 Collection of personal data

(a) When collecting personal data from or about an individual:

(i) Collect only the minimum personal data reasonably necessary for the purposes for which the data is being collected. Where individuals need not be identifiable for the purposes in question, data should be collected and kept in an anonymised form.

(ii) The individual providing the data must be informed about the purposes for which the data is to be processed by us and the identities of anyone to whom the data may be disclosed or transferred.

(iii) In certain instances, it may be necessary not only to inform the individual of the purposes for which his or her data is to be processed, but also to obtain the individual's express consent to the processing of such data for such purposes. This may be the case where an individual's personal data is to be used for direct marketing purposes. A record should be kept of any consent obtained from a data subject, how and where it was obtained and for what purposes.

(b) If you wish to purchase or license personal data, such as a mailing list, from a third party, you must ensure that:

(i) You inform your Regional Compliance Team about the proposal;

(ii) There is a written contract in place with the third-party controller of the data, which contract must be reviewed and approved by your regional legal department prior to execution; and

The third party has complied with applicable Data Protection Laws in connection with its collection and processing of the purchased or licensed data, including its transfer to us. For instance, where MHR intends to market to individuals whose personal data is being purchased or licenced, you must ensure that the third party providing the data to MHR has received from the individual data subjects appropriate and explicit consent to allow MHR to market to them directly. It would not be sufficient for such consent to refer to MHR in general terms, such as a "hotel partner," rather the consent must expressly identify MHR and the purposes for which MHR may process the personal data of the data subjects.

7.3 Processing personal data

(a) Personal data may only be processed for the specific purposes which are notified to the individual providing the data when the data was first collected. Personal data must not be collected for certain purposes and then used for other reasons. If it becomes necessary to change the purposes for which data is to be processed, the individual who provided the data must be informed of the new purposes, and a new consent may need to be obtained from that individual before any processing occurs.

(b) There must be a legal basis for processing personal data. The legal basis may include our legitimate interests in processing the personal data, the performance of our obligations under a contract, our compliance with a legal obligation or a consent provided by the data subject. Please contact your Regional Compliance Team to assist you in assessing the appropriate legal basis for any proposed collection or processing activities.

(c) You should take measures to keep any personal data we collect accurate, complete and up-to-date. This may require, for example, reminding data subjects of the information we hold about them and asking them to update their personal data from time to time.

7.4 Transfers of personal data to third parties

MHR may use third party providers to perform services on our behalf. As MHR may be legally responsible for the processing performed by these third-party providers, it is very important that they comply with Data Protection Laws; otherwise, MHR may be in breach of the Data Protection Laws. If personal data is to be transferred to a third-party providing goods or services to us or on our behalf, then:

(a) A DPIA may be required, as set out in this Policy and in the Guidance for DPIA.

(b) You should ensure that a contract is entered into with the third party and that such contract includes legally compliant data protection clauses that require that third party to provide adequate protection to the personal data and that limit our liability for such third party's failure to provide adequate protection. You should also ensure that such contract has been reviewed and approved by your regional legal department.

(c) With regard to data transfers from within the EU/EEA or Singapore to outside of the EU/EEA or Singapore, respectively, specific data transfer clauses must be incorporated into the contract (including the relevant model contractual clauses promulgated by the European Commission from time to time, as applicable).

(d) If any existing contracts with third party providers do not have adequate data protection and data transfer clauses, it will be necessary to enter into an addendum (or letter agreement) to vary these existing contracts. This must be done as soon as possible. If a third-party provider refuses to enter into the addendum (or letter agreement), it may be necessary to terminate the contract taking into consideration the nature and purposes of the contract.

7.5 Intra-group transfers of personal data

(a) As a global company, personal data we hold may be transferred to our group members around the world in connection with our business and for employment, administrative, management and legal purposes. Any such transfers must be lawful and in accordance with this Policy, and appropriate security arrangements should be in place before conducting any transfer.

(b) Similar to transfers of personal data to third parties, before transferring any personal data to another MHR group member, you must ensure that appropriate contractual provisions are in place between the relevant companies. Your regional legal department can assist you with regard to any such intra-group transfer.

7.6 Data subject access requests and other rights of data subjects

With regard to any personal data held by an MHR group member, individual data subjects have certain rights. The most common rights that will be exercised by individuals include the rights to:

(a) Request access to their personal data – Such requests, commonly known as "data subject access requests", enable individuals to receive a copy of the personal data we hold about them and confirm how we are processing it. If you should receive any such data subject access request, please refer to the Data Subjects' Rights Policy (located at https://www.millenniumhotels.com/en/corporate/grouppolicies/) for more information. It is important for each request to be reviewed and processed promptly as some Data Protection Laws impose strict time limits by which organisations must respond.

In certain circumstances, a third party may request access to the personal data of one or more Covered Parties, in which case:

(i) If law enforcement or a government agency requests the release of personal data about an individual, you should contact a member of your regional legal department immediately, before releasing any such data. Requirements in countries vary, but in many jurisdictions, a court order or other appropriate legal authorisation will be required.

(ii) In the event that any other third party, including friends or family members, requests the release of personal data about an individual data subject, you must obtain the data subject's consent prior to releasing that information unless another legal basis for releasing the requested information applies. Such other legal basis must be assessed by your regional legal department prior to disclosure of the requested information.

(b) Withdraw consent – In the limited circumstances where an individual has provided his or her consent to the collection and processing of his or her personal data for specific purposes, the individual has the right to withdraw that consent for the specified processing at any time. There are several ways an individual may withdraw consent, including by (i) sending an email to dataprivacy@millenniumhotels.com, (ii) informing a member of staff and/or (iii) for members of the My Millennium loyalty programme, visiting the communications preferences page accessible from the individual's account.

Once we have received notification that a person has withdrawn consent, that withdrawal should be reflected in the individual's consent records and where possible, the individual should be informed of the likely consequences of withdrawing consent. That person's data should no longer be processed by us and any intermediaries, contractors or agents working on our behalf should be instructed to cease processing that individual's personal data, in each case unless the processing of the data without consent is required or authorised by the Data Protection Laws. As a general rule of thumb, we should give effect to a withdrawal notice as soon as reasonably practicable, but in any event within ten (10) business days. If more time is needed, it is good practice to inform the individual of the time frame by which the withdrawal of consent will take effect.

(c) Request correction of their personal data – Individuals may request that their personal data be corrected or updated. They may do so by (i) sending an email to dataprivacy@millenniumhotels.com, (ii) informing a member of staff, and/or (iii) for members of the My Millennium loyalty programme, visiting the communications preferences page accessible from the individual's account. In such event, we may need to relay the corrected personal data to other organisations to which we disclosed the personal data, unless those other organisations do not need the corrected personal data for any legal or business purposes.

Other rights of data subjects include the rights to:

(d) Request erasure of their personal data – This enables individuals to ask us to delete or remove personal data about them where there is no lawful reason for us continuing to store or process it. However, note that in such instances we generally retain personal data for a period of time following an erasure request for legal or regulatory reasons.

(e) Object to processing of their personal data – Individuals have an absolute right to object to the processing of their personal data for direct marketing purposes. They also have a right to object, in certain circumstances, where we are relying on legitimate interests (or those of a third party) to process their personal data. Should we receive such an

objection, we will need to assess our legitimate interests against the reasons for the objection and, acting fairly, make a determination on any future processing and whether our legitimate interests may be overridden by the individual's interest, rights or freedoms. Such assessment involves a three-part test, including a "purpose test," a "necessity test" and a "balancing test." Your regional legal department can assist you with any such assessment.

(f) Request the restriction of the processing of their personal data – Individuals may ask us to suspend processing where one of the following reasons applies: (i) they want us to establish the accuracy of their personal data or the reason for processing it; (ii) the processing is unlawful and the data subjects oppose the erasure of the personal data and request that the use of the data be restricted; or (iii) we no longer need the personal data for the purposes for which it was collected, but the data is required by the data subjects for the establishment, exercise or defence of legal claims.

(g) Request the transfer of their personal data to other parties – Any such request by an individual to receive a copy of his or her personal data (which is stored in a commonly used and machine-readable format) and to transfer such data directly to another party will be subject to the rights of others and any legal or other privilege that may attach to such data.

If an individual would like to request the erasure, object to the processing, or request the restriction of the individual's data, or request that we transfer to a third party a copy of the individual's data, the individual should be asked to put his or her request in writing and it should be referred to a member of your Regional Compliance Team or sent to dataprivacy@millenniumhotels.com. Since Data Protection Laws often require actions to be taken within prescribed time periods, we must process and respond to any such request promptly, and in general, within thirty (30) days or sooner if required by applicable Data Protection Laws.

In the event that you receive a request above that relates to personal data scheduled for disposal or destruction, you must ensure that the personal data is preserved while the request is being processed. If the request is eventually rejected by us, we must keep the personal data for a reasonable period (at least thirty (30) calendar days or such longer period as is required under local Data Protection Laws) after rejecting the request so that the individual has an opportunity to seek a review of our decision to reject the request. If such a review is sought, we must preserve the personal data until the review is concluded and any right of the individual to further appeal is exhausted.

Please refer to our Data Subjects' Rights Policy which can be found at www.millenniumhotels.com/en/corporate/grouppolicies.

7.7 Retention and destruction of personal data

(a) We must retain personal data for only as long as is necessary to fulfil the purposes for which we collected it, including for the purposes of satisfying any legal, accounting or reporting requirements. If the purposes for which personal data is retained has ceased, such data must not be kept on a "just-in-case" basis for other purposes.

(b) Personal data must be destroyed or erased from our systems when it is no longer required, after any retention period required for legal or compliance purposes. Promptly after the applicable retention period has ended, the personal data may be: (i) securely deleted or destroyed, (ii) anonymised, or (iii) in some cases, transferred to a secure archive.

For guidance on how long certain data may be kept before being destroyed or erased, please refer to our record retention and disposal policy (located at https://www.millenniumhotels.com/en/corporate/grouppolicies/) for further details or contact a member of your Regional Compliance Team.

(c) When destroying or erasing personal data, you should ensure that it is destroyed or erased in a manner reasonably intended to prevent the misappropriation or other unauthorised access to or use of the information, for instance by shredding paper records, using secure document disposal services and permanently deleting information from computers or other electronic devices.

7.8 Protecting personal data

(a) MHR is committed to taking appropriate security, technical, physical and organisational measures to protect personal data against unauthorised access, unlawful processing, accidental loss or damage and unauthorised destruction, and other similar risks.

(b) In general, access to personal data of Covered Parties should be limited to only those employees, agents and contractors of MHR group members, and other third parties engaged by or on behalf of group members, who (i) have a business need to know the information in connection with our processing of the data for the purposes for which we collected it, (ii) are subject to appropriate controls—including confidentiality obligations—and, and (iii) with regard to third parties, have in place adequate security measures to prevent unauthorised access to the information.

(c) Within MHR group members, appropriate security measures should be implemented for the storage and/or transfer of personal data. Data held in paper form should be stored in locked offices or cabinets that are accessible only by authorised personnel; it should not be left out in the open, on a desk or printer, for instance. Additional security measures required for electronic data are outlined in MHR's Global Information Security Policy, copy of which can be obtained from your regional information technology team or via https://www.millenniumhotels.com/en/corporate/grouppolicies/. MHR will take appropriate action in accordance with this Policy and applicable Data Protection Laws if personal data is accessed, processed, or otherwise used in any way that is inconsistent with the requirements of the relevant policies

8. COMMON DATA COLLECTION AND PROCESSING ACTIVITIES

8.1 Closed circuit television ("CCTV"), telephone and audio recordings

Images of individuals collected through the use of CCTV or other recording equipment, such as telephone and audio recordings, may be considered personal data under Data Protection Laws. We currently use CCTV cameras to view and record individuals on and around the premises of our hotels and corporate offices. To that end, we have put in place guidelines for you explaining why we use CCTV, how we will use CCTV and how we must process data recorded by CCTV cameras and other recording devices to ensure we are compliant with Data Protection laws and best practice. These guidelines also explain how to respond to a data subject access request in respect of such personal data. You should be aware of and follow these guidelines, which are set out in the Closed Circuit Television, Telephone and Audio Recording Policy attached as Schedule 1. However, when using CCTV and other recording devices, care should be taken to ensure you comply with local requirements as well and you should refer any questions to your Regional Compliance Team.

8.2 Employment activities

If you are collecting or processing personal data of employees, interns and/or job applicants in the course of your duties, you are required to comply with all applicable Data Protection Laws, this Policy, and other relevant global and regional MHR policies. A non-exhaustive list of areas in which such personal data may be collected and processed is set out below.

(a) Recruitment and selection

(i) Personal data of individuals may be collected and processed for recruitment purposes. This may occur where an individual fills out a job application form, or otherwise voluntarily provides his/her personal data by submitting his/her resume or CV. For further information, please refer to our recruitment policies, copies of which can be obtained from your regional human resources department.

(ii) Job application forms should only ask for information relevant to the recruitment decision and which is reasonably appropriate to the business needs of MHR. For example, it may be necessary to obtain details of driving experience (including driving offences) of a person who is applying for the position of a car valet or driver, but not of a person who is applying for the position of a chef.

(iii) Do not collect information from applicants to the extent you only need such information should the applicant become an employee of an MHR group member. For example, banking details should only be requested after the applicant has accepted employment.

(b) Employment

(i) As part of the hiring process and on an ongoing basis, employees should be informed about the ways in which the relevant MHR group members that serve as their employers will process their personal data. Employees in the EU/EEA should be provided with the Privacy Notice (EU) for Employees, Workers and Contractors as it describes the data we collect, how we process it, our legal bases for doing so and the rights of employees in respect of that data. In other jurisdictions, certain types of processing of employee data may require employee consent. A copy of the Privacy Notice (EU) for Employees, Workers and Contractors can be found at https://www.millenniumhotels.com/en/corporate/grouppolicies/.

(ii) Relevant data privacy or data protection clauses should be included in employment contracts, as necessary.

(iii) The collection or processing of an employee's personal data for any other purposes that are not relevant to the management or termination of an employment relationship, or evaluation of the employee, may require the prior written consent of the employee. Please check with your human resources department before collecting or processing personal data of employees for any other purposes.

(iv) Personal data of employees must be accurate, complete and kept up-to-date. Employees should be required to update their personal data whenever there is a change in personal circumstances that is likely to impact data used by their MHR employers, or which is likely to be disclosed by the MHR group member to another organisation.

(v) Personnel files of employees should be stored in a secure manner so that only those who have a business need and who are authorised to access the files may do so. For example, keep paper records under lock and key and use password protection for computerised records.

(vi) Employment records should not be kept longer than necessary for the purposes for which such data was collected, or for any other legitimate legal or business purpose. For guidelines on the appropriate retention periods, please refer to MHR's record retention and disposal policies (located at https://www.millenniumhotels.com/en/corporate/grouppolicies/.

(c) Monitoring at work

(i) If employees are being monitored such that information about them is being collected or processed, the applicable Data Protection Laws and this Policy may apply. This can happen, for example, when you video workers to detect crime, enable location tracking on electronic equipment used by employees, check telephone logs to detect excessive private use, and monitor e-mails or check internet use.

(ii) Employees should be made aware that they are being monitored and the reasons why such monitoring is necessary. This could be done by putting up notices or signs in areas of monitoring (e.g., where there is CCTV surveillance), or by way of the staff handbook or a relevant policy or privacy notice.

(iii) Only process personal data obtained through monitoring for the purposes for which you carried out the monitoring, unless a relevant exception applies under applicable Data Protection Laws.

For further information, please refer to the Monitoring Policy set out in Schedule 2.

8.3 Marketing

(a) *Opt-in consent*

(i) Generally MHR may only send an individual direct marketing communications by electronic means after having obtaining the individual's consent to receive such communications. In particular, marketing by electronic means includes emails, text messages, picture messages, video messages, voicemails, direct messages via social media or any similar messages that are stored electronically.

(ii) In order to be valid, an individual's consent needs to comply with strict rules. It must:

· be freely given, specific, informed and unambiguous;

· be unbundled and separate from other terms and conditions;

· involve a statement or a clear affirmative action (an opt-in), excluding therefore any pre-ticked boxes or implied consent;

· be granular in nature and specify any separate processing and purposes for which it will be used;

· clearly name all parties, including any third-party controllers, that will be relying on it;

· be documented, as records must be kept to prove why such consent was obtained;

· be as easy to withdraw as it was to provide;

- be maintained; and
- not be obtained by providing false or misleading information, or using deceptive or misleading practices.

You must not, as a condition of providing a product or service, require an individual to consent to the collection and processing of personal data about the individual beyond what is reasonable to provide the product or service to that individual. Because it is generally considered that marketing purposes are not reasonably necessary to provide specific products or services to an individual, we cannot require individuals to consent to marketing purposes as part of our provision of products or services to them.

(iii) Any consent obtained from an individual, whether electronically or on paper, must be stored as part of the data subject's consent records so that it can be retrieved at a later date, in accordance with MHR's record retention and disposal policies (located at https://www.millenniumhotels.com/en/corporate/grouppolicies/). An individual's election to receive marketing communications, and any subsequent changes to that election, must be reflected in MHR's customer relationship management system (the "CRM System") and MHR's other marketing or campaign management systems. This will help to ensure that an individual who has not consented to receive marketing communications will not receive any such communication inadvertently.

(b) *Ability to opt-out and reminders*

(i) Each marketing communication must contain a clear and easy way for the individual receiving the communication to unsubscribe or opt-out from further marketing communications without charge, preferably through the use of an unsubscribe link.

(ii) At least twice per year—once every six months—reminder emails should be sent to individuals who have opted to receive marketing communications informing them that they have elected to receive such communications and providing them with an opportunity to opt-out or unsubscribe.

(iii) If an individual elects to opt-out or unsubscribe from marketing communications at any time, then that individual's election must be recorded, as part of the individual's consent records, in all relevant MHR marketing systems and in particular the CRM System, as soon as possible so that he or she will cease to receive future marketing communications. It is strictly prohibited to send marketing messages to any person who objects or opts-out of receiving them.

(iv) If an individual objects to receiving marketing communications, you must refrain from sending marketing communications to the individual.

(c) *Marketing campaigns*

The MHR entity that operates its commercial website and the CRM System, M & C Reservations Services Limited ("MCRSL"), is MHR's data controller for purposes of all marketing communications globally. This means that marketing campaigns must be run through MHR's central marketing team, even if the content and initiatives are developed at the regional or hotel level. MHR's regional teams and individual hotels should not maintain separate marketing databases or conduct their own individual marketing campaigns (whether to those residing inside or outside of the EU/EEA) unless the approval has been obtained from MHR's legal and marketing departments to operate as an exception. This process helps to ensure that we comply with Data Protection Laws and speak with one voice to our customers, using consistent messaging and brand collateral.

(d) *Service communications*

MHR's regional and hotel management teams may send "service emails" to guests, such as a booking confirmation, pre-stay and post-stay emails that do not include marketing or promotions. These emails rely on our legitimate interests in providing our services and therefore can be sent without express consent in order to fulfil a booking contract. However, offers of paid room upgrades or packaged services or amenities, such as spa vouchers or theatre tickets, are considered marketing and therefore must not be included in service emails, unless the express prior consent of the individual has been obtained.

In limited circumstances, some jurisdictions (including the UK), operate an exception to the requirement to obtain consent for email marketing, known as a "soft opt-in," which can apply to existing customers where the marketing permission was obtained during the course of a sale or negotiation and relates to similar products or services, and where the person was given a simple opportunity to refuse or opt-out of the marketing, both when first collecting the person's details and in every subsequent message to the person. To the extent you wish to rely on this exception, you must consult with a member of your Regional Compliance Team.

(e) *Email banner advertisements*

Email banner advertisements may be considered marketing and subject to the requirements of this Policy. Such email banner advertisements should not include any offers or promotions of MHR products or services, even if the emails to which they are attached are not sent for marketing purposes, such as communications with suppliers. The email banner may, on the other hand, inform email recipients about MHR corporate events or information, such as the opening or rebranding of new hotels; however, such email banner should not have a link to an offer or promotion.

(f) *Business-to-business marketing*

Marketing to businesses may involve the processing of personal data of employees of those businesses and as such may be subject to certain requirements under Data Protection Laws. Business contact information given for personal rather than business purposes may be deemed, and should be treated, as personal data given for personal purposes (e.g., those given at check-in or for promotional purposes).

(g) *"Do Not Call" registries*

Some jurisdictions provide for central registries that allow individuals to opt-out of receiving certain forms of marketing communications, including via the telephone and post. The Telephone Preference Service in the UK (at www.tpsonline.org.uk) and the Singapore Do Not Call Registry (at www.pdpc.gov.sg/Individuals/Do-Not-Call-Registry-and-You) are examples of these. The effect of these "opt-outs" by individuals may extend outside of the jurisdiction in which a central registry is located, e.g., MHR hotels located outside of Singapore should not direct marketing communications to Singapore telephone numbers, whether by call or text, if the telephone numbers are registered with Singapore's Do Not Call Registry unless clear and unambiguous consent to do so has been obtained from the relevant individuals in written or other accessible form. All persons responsible for direct marketing campaigns must ensure that they are familiar with any such registries in the countries over which they have responsibility or which are within their marketing scope, and that they have in place a process to confirm an individual's status within any such registries prior to sending marketing communications to the individual. Failure to do so may result in significant fines or penalties. Further guidance may be sought from your Regional Compliance Team.

(h) *Contests, lucky draws and other promotions*

Before collecting any personal data through any contest, lucky draw and/or other promotion, please ensure appropriate terms and conditions have been developed for the promotion and you must provide a clear reference to the MHR privacy policy (see Section 8.4 of this Policy below). All individuals entering into the contest, lucky draw and/or other promotion must confirm that they (i) have read and agree to be bound by the relevant terms and conditions (which should include the privacy policy terms) and (ii) have read and understand the MHR privacy policy. Participants should not be asked separately to confirm that they "accept" or "agree to" the MHR privacy policy as they will not be able to take part in such contest, lucky draw or promotion if they do not accept it. However, if any participant should later seek to withdraw his or her consent to the processing of his or her personal data in connection with the contest, lucky draw or promotion, then that participant must be informed that he or she is no longer eligible to participate in the contest, lucky draw or promotion.

(i) *Third-party marketing*

No personal data of an individual may be provided to, or otherwise used by, a third party for direct marketing purposes without the prior express consent of the individual.

(j) *Direct marketing to children*

Personal data of individuals who are under 13 years old may not be used for direct marketing purposes.

Detailed guidelines regarding the requirements under Data Protection Laws when marketing to individuals and business are available from your Regional Compliance Team or by contacting dataprivacy@millenniumhotels.com.

8.4 Customer privacy policy

All MHR websites and marketing communications must contain a link to MHR's approved privacy policy or statement. In most instances, that will be the privacy policy contained on MHR's primary commercial website (via https://www.millenniumhotels.com/en/utilities/privacy-and-cookie-policy/privacy-and-cookie-policy/) and you should familiarise yourself with this policy. When establishing a new MHR website, you should consult a member of your Regional Compliance Team to determine the appropriate form of privacy policy or statement to be included on the site.

8.5 Guest registration

(a) In order to ensure consistency across the various booking channels for MHR's hotels in terms of communicating MHR's privacy policy and obtaining marketing consents from guests, the best single point of contact we have with each guest is at the time of check-in and registration. As such, MHR has created an approved form of guest registration card, with approved data privacy and marketing consent language. A copy of the approved form of registration card can be obtained from your Regional Compliance Team.

(b) Each hotel that is operated by an MHR group member (whether owned by us or not) should utilise the approved form of registration card. Please contact your Regional Compliance Team if you intend to use a guest registration card which differs in substance to the approved form guest registration card. In any event, all guest registration cards must include a reference to MHR's privacy policy (see Section 8.4 of this Policy) and

should state that a printed copy of the policy can be obtained on request, at the reception desk. All guest registration cards also must include agreed form marketing permission language (see Section 8.3 of this Policy).

(c) Since guest registration cards are a primary source of personal data of our guests, hotel front-office personnel should ensure that:

(i) Once a guest registration card has been completed, the information provided by the guest should be entered into your hotel's property management system as soon as possible. You should check the data entered against the data on the registration card and correct any mistakes.

(ii) Copies of guest registration cards should be scanned and stored on an MHR approved electronic storage system as soon as possible. Where MHR obtains a marketing permission (consent) from an individual via a guest registration card, it is essential that we retain a copy of the guest registration card as part of the individual's consent record, and that it is retrievable, in order to demonstrate, should we need to produce evidence in the future that MHR had obtained the appropriate marketing permission from the guest. The length of time such guest registration cards should be retained shall be determined in accordance with MHR's record retention and disposal policies (located at https://www.millenniumhotels.com/en/corporate/grouppolicies/)

(iii) If a guest informs you of an error on the registration card, you should make the correction in the property management system as soon as possible.

(iv) All registration cards should be stored in a safe place (whether digitally or physically) where they cannot be seen or accessed by other guests or members of staff not entitled to view them.

(v) Registration cards completed in error must be destroyed in accordance with MHR's record retention and disposal policies (located at https://www.millenniumhotels.com/en/corporate/grouppolicies/)

(vi) You must not give out details of guests to other guests or members of the public without guest's express consent.

8.6 Third Party Owned Hotels

The following guidance pertains to hotels which are owned by third parties, but which are operated by MHR, under an MHR brand, pursuant to a hotel management agreement with the owner of the hotel (individually, a "Managed Hotel" and collectively, "Managed Hotels").

(a) Generally MHR controls and is responsible for the guest data collected in connection with the operation of Managed Hotels. For this reason, the same data protection policies and procedures that apply to MHR owned hotels also apply to Managed Hotels.

(b) While the general manager and certain other members of the executive team of a Managed Hotel are employed by an MHR group member, typically the remaining hotel employees working within a Managed Hotel are employed by the owner of the hotel, although these employees operate under our direction in accordance with the terms of the management agreement. As such, hotel employees may receive personal data of guests and a limited number of MHR employees in order to allow us to manage the hotel and fulfil our commitments to the owner, guests and other stakeholders. Subject to the terms of the relevant hotel management agreement, hotel employees should not store or

process that information for any other purposes or disclose it to any third parties, including the owner of the hotel, and they should be subject to obligations of confidentiality in respect of that data.

(c) In the event an MHR group member ceases to operate a Managed Hotel, personal data of guests will need to be shared with the owner of the hotel or its designated management company in order to ensure that future bookings are honoured. In this case, data relating to future bookings only may be transferred to the owner or a subsequent management company provided an appropriate data transfer agreement has been put in place, and guests should be properly notified of the data transfer. Please contact a member of your regional legal department or Regional Compliance Team, prior to any change in the management of a Managed Hotel, to assist you with this process.

(d) If an owner of a Managed Hotel requests that MHR collect marketing consents from guests on the owner's behalf, then such request must be considered appropriately under the relevant Data Protection Laws and you should contact a member of your Regional Compliance Team. At a minimum, the guest registration card for the hotel will need to be amended to incorporate a specific opt-in consent identifying the owner and the purposes for which the data is to be used by the owner. Also, we must ensure that the owner is obligated to comply with relevant Data Protection Laws with regard to its use of such data and to indemnify MHR for any claims arising from the owner's misuse of the data, so a data transfer agreement should be entered into prior to sharing any personal data with the owner.

9. DATA BREACHES

We have put in place procedures to deal with any suspected personal data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so. We also 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/grouppolicies/). You must review and familiarise yourself with this policy.

Each member of your Regional Compliance 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, stolen or compromised, you should notify one of these team members immediately.

10. COMPLAINTS AND QUESTIONS

If you have complaints relating to our processing of your personal data or the personal data of a Covered Party or any questions regarding this Policy or the application of Data Protection Laws, you should raise these with your Regional Compliance Team the first instance or you may send an email to dataprivacy@millenniumhotels.com. Also, you may contact the Internal Audit (at Business.Integrity@millenniumhotels.com) should you not feel comfortable raising your concerns with another party.

Please be advised that you also may raise complaints with the supervisory authorities or regulators in your respective country. In the UK, 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 or legal departments.

11. TRAINING ON THIS POLICY

All staff shall be required to complete online or other personal data protection training from time to time. More specialised training on the operation of this Policy will be provided to specific employees as necessary.

12. REVIEW OF THE POLICY

We will continue to review the effectiveness of this Policy on a regular basis to ensure it is achieving its stated objectives.

SCHEDULE 1

CLOSED CIRCUIT TELEVISION, TELEPHONE AND AUDIO RECORDING POLICY

1. CLOSED CIRCUIT TELEVISION ("CCTV")

We believe that CCTV and other surveillance systems have a legitimate role to play in helping to maintain a safe and secure environment for all our staff and visitors. However, we recognise that the use of these systems may raise concerns about their effect on individuals and their privacy. Images recorded by surveillance systems are personal data, which must be processed in accordance with Data Protection Laws. This Schedule is intended to address such concerns and assist staff in complying with their legal obligations when working with personal data obtained through CCTV. In certain circumstances, misuse of information generated by CCTV or other surveillance systems could constitute a criminal offence.

1.1 Reasons for the use of CCTV

MHR utilises CCTV systems in our hotels and corporate offices for the following reasons:

(a) to assist in the prevention and detection of crime;

(b) to help safeguard MHR property, including physical and intellectual property and personal data, customers and staff;

(c) to assist with the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings against staff; and

(d) to monitor the security of buildings and other areas operated by MHR group members. This list is not exhaustive and other purposes may be or become relevant.

1.2 Operation of CCTV

(a) The cameras should be sited in such a way that they only monitor MHR property. If that is not feasible, you should, out of courtesy, inform the owners of other properties that are within the range of the cameras and be aware of this fact when reviewing tapes.

(b) Members of the public should be made aware that CCTV is in operation. In particular, the following guidelines should be followed:

(i) Notices of the operation of a CCTV system should be placed prominently at all points of entry to areas in which a CCTV system is being used and reinforced with further signs within such areas (for example, at the hotel front desk). Signs should:

- be clearly visible and understandable;
- state the purpose(s) for using the CCTV cameras and to the extent required by local regulations, identify the party operating the CCTV system and who may be contacted, by telephone or email, about the use of the CCTV system, e.g., "NOTICE: These premises are under video surveillance for security purposes. This scheme is controlled by Millennium Hotels and Resorts. For more information, call [number] or email [email address]";
- indicate, where applicable, that both video and audio recordings are taking place; and

- be an appropriate size depending on the context, for example, whether they are viewed by car drivers or walk-in hotel guests or pedestrians.

(ii) It is not necessary to disclose the exact location of the CCTV cameras; it is sufficient for the notices to indicate that CCTV cameras are being used in the general locale.

(iii) CCTV cameras must never be used in areas where a reasonable person would have an expectation of privacy, such as inside restrooms or hotel rooms.

(iv) If CCTV cameras have sound recording capabilities, they should not be used to record general conversations of members of the public unless recording is specifically required for the detection and prevention of crime.

(v) Tapes or other magnetic media should be kept in a secure environment. Access to any CCTV footage should be restricted to authorised staff, and strictly for the purposes set out in the notice(s) given.

(vi) Any viewing monitors of CCTV footage should not be visible to others. Authorised staff shall be appropriately trained and supervised in the use and handling of the CCTV surveillance system and CCTV footage.

1.3 Subject access requests

(a) Individuals may make a request for disclosure of their personal data, which may include CCTV images.

(b) Should such a data subject access request be made, in order for us to locate relevant footage, any requests for copies of recorded CCTV images should include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual.

(c) Generally images of third parties should be obscured when disclosing CCTV data as part of a subject access request.

1.4 Sharing CCTV footage and other requests for disclosure

(a) CCTV footage should not be disclosed to any third parties, subject to some limited exceptions.

(i) Data may be shared with other MHR group members, such as hotel footage being shared with corporate office personnel, and/or service providers, such as outsourced security personnel or security firms, where it is reasonably necessary for any of the legitimate purposes set out in this Schedule. Please consult with a member of your regional legal department or Regional Compliance Team to confirm any such data sharing arrangements.

(ii) In some circumstances, law enforcement personnel may have the authority to view or remove CCTV footage where this is required in the detection or prosecution of crime. While generally we should endeavour to co-operate with authorities and not obstruct an investigation, we must balance the interests and rights of law enforcement against the interests and rights of individuals under the Data Protection Laws. Should you be approached by law enforcement in connection with a request for CCTV footage, please contact a member of your regional legal department or Regional Compliance Team immediately, before providing any information to the authorities. At a minimum, you must ensure that that the warrant or authorising paperwork from the enforcement authority allows

for the collection of the information being requested and if possible, you should request a copy of such documentation.

(b) You must maintain a record of all disclosures of CCTV footage.

(c) Appropriate policies should be established regarding requests for images. In the event of any such request, the privacy rights of other recorded persons must be respected. Generally, any standard request to access CCTV footage should be permitted if:

(i) access is only given to an affected individual (i.e., an individual who is requesting CCTV footage about himself or herself); and

(ii) images of other individuals present in the CCTV footage are masked (unless consent of the individuals for such disclosure is obtained, where such consent is required).

In the event access to CCTV footage is requested, you should inform and seek the assistance of your Regional Compliance Team before complying with any such request.

(d) Access to CCTV footage does not have to be provided, and should not be provided, if:

(i) the provision of access could reasonably be expected to:

- threaten the safety or physical or mental health of another individual;
- cause immediate or grave harm to the safety or physical or mental health of the individual who requested access;
- be contrary to national interest; or

(ii) such request:

- would unreasonably interfere with our operations because of the repetitious or systematic nature of the requests;
- would give rise to a burden or expense that would be unreasonable or disproportionate to the individual's interests;
- is for information that does not exist or cannot be found;
- is for information that is trivial;
- is frivolous or vexatious;
- would reveal confidential commercial information that could, reasonably harm our competitive position; or

(iii) any other exception under applicable Data Protection Laws applies.

(e) If access is denied on any of the above grounds, a record of the particulars of the request and reasons for denying access (along with any supporting evidence) must be kept.If it is not possible or prohibitively costly to provide an individual with a copy of requested CCTV footage, the individual should be given a reasonable opportunity to examine the requested data in person (with appropriate masking of the images of other individuals where required).

(f) Where any CCTV footage recording is passed to a third party, such as a law enforcement agency, a note should be kept of:

(i) The name and address of the person to whom the recording was passed;

(ii) The date and time the recording was provided to the third party;

(iii) The date and time of events on the recording;

(iv) The reason the recording was required;

(v) Other relevant information, e.g., a case number;

(vi) Signature of the person taking the recording;

(vii) Date and time of return; and

(viii) Any action taken as the result of viewing the recording.

1.5 Use of personal data gathered through CCTV

(a) In order to ensure that the rights of individuals recorded by CCTV systems are protected, you must ensure that data gathered from CCTV cameras is stored in a way that maintains the integrity and security of the data. This may include encrypting the data, where it is possible to do so.

(b) Given the large amount of data generated by surveillance systems, video footage may be stored using a cloud computing system. In such case, all reasonable steps should be taken to ensure that any cloud service provider maintains the security of our information, in accordance with industry standards. A member of your Regional Compliance Team should be consulted before any cloud storage is to be utilised.

(c) Where you engage data processors to process data on our behalf, you must ensure reasonable contractual safeguards are in place to protect the security and integrity of the data. Please ask a member of your regional legal department to review any such data processing contract.

1.6 Retention and erasure of CCTV data

(a) Personal data from CCTV cameras should not be retained indefinitely, but should be permanently deleted once there is no reason to retain the recorded information. The period of time footage should be retained will vary according to the purpose for which the footage has been recorded. For example, where images are being recorded for crime prevention purposes, data will be kept long enough only for incidents to come to light. In all other cases, recorded images should be kept for no longer than 90 days unless you have been advised otherwise by your Regional Compliance Team. A comprehensive log of when such data is deleted should be maintained.

(b) At the end of their useful life, all images stored in whatever format will be erased permanently and securely. Any physical storage devices, such as tapes or discs, must be disposed of as confidential waste. Likewise, any still photographs or hard copy prints should be disposed of as confidential waste.

1.7 Use of additional surveillance systems

(a) Prior to introducing any new surveillance system, including placing a new CCTV camera in any workplace location, you must consider carefully if the system is appropriate by liaising with your Regional Compliance Team and carrying out a Data Protection Impact Assessment. A DPIA is intended to assist us in deciding whether new surveillance cameras

are necessary and proportionate in the circumstances and whether they should be used at all or whether any limitations should be placed on their use.

(b) No surveillance cameras should be placed in areas where there is an expectation of privacy (for example, in changing rooms) unless, in very exceptional circumstances, it is judged by us to be necessary to deal with very serious concerns.

2. TELEPHONE ENQUIRIES

2.1 Since personal data we hold about individuals should not be disclosed to any unauthorised third parties, any member of staff dealing with telephone enquiries should be careful about disclosing any personal data to a caller, whether the caller purports to be the data subject or another party, such as the individual's employer, family member or a law enforcement agency.

2.2 In the event you receive a request via the telephone to disclose personal data of a Covered Party, you should:

(a) Check and confirm the caller's identity, to make sure that information is only given to a person who is entitled to it.

(b) If you are not able to verify the identity of a caller or confirm that the caller is entitled to the requested information under Data Protection Laws, you must not disclose personal data to the caller. In such event, suggest that the caller put his or her request in writing or refer to a member of your Regional Compliance Team for assistance in difficult situations. Depending on the nature of the request, it may be that the individual ought to make a formal data subject access request for the information.

2.3 Please contact your regional legal department before providing any personal data to any caller identifying himself or herself as a member of a law enforcement agency or other authority.

3. AUDIO RECORDINGS

3.1 Audio recordings can be a useful tool for training and compliance purposes. Voice recordings are not conclusively personal data. Whether they constitute personal data, and are thus subject to Data Protection Laws, depends on the content of the recording. If an individual can be identified from that recording, or from that recording and other information that we have or are likely to have, then such audio or voice recording constitutes personal data and special care must be taken in the collection, storing and using of that recording.

3.2 Prior to using any audio recording device and recording personal data of an individual, notice should be given to the individual and, in most instances (save for, e.g., audio recording collected in connection with the operation of CCTV), consent must be obtained from the individual for the recording and use of the audio information. Such notice should be clear and understandable and state the purpose(s) for the recording and any consent obtained should be recorded.

For example:

(a) Where an audio recording device is to be used at a hotel's reception desk, the following notice could be placed at the desk: "NOTICE: Audio recording devices are in operation. Recordings may be used for training, dispute resolution and security purposes."

(b) Where the audio recording device is being used as part of a telephone customer support service, on the other hand, notice of the recording should be given verbally at the start of the conversation. An example of such a notice includes: "This call may be recorded for quality training purposes or for follow-up queries." The customer service representative

also must be trained to obtain the consent of the individual before proceeding to collect the data.

3.3 Audio recordings must be kept in a secure environment, with access restricted to authorised MHR personnel only, and recording should be deleted in accordance with MHR's record retention and disposal policies (located at https://www.millenniumhotels.com/en/corporate/grouppolicies/).

SCHEDULE 2

MONITORING POLICY

MHR may monitor, access, examine, capture or otherwise intercept ("**Monitor**") (by human or automated means) communications or data transmitted through its IT Systems. As Monitoring will involve the processing of personal data, this Schedule sets out MHR's Monitoring activities and details how we treat the personal data that we may collect through Monitoring. MHR will take steps to ensure that all of its Monitoring activities are conducted both fairly and lawfully.

As used in this Schedule, MHR's "**IT Systems**" include all computers, equipment, devices and storage media connected in any way to MHR's computer network. It includes the local and wide-area network infrastructure, telecommunications systems and components (including telephones, facsimile machines, photocopiers, printers, personal organizers, laptops, iPads, smartphones, computers and servers), telematics and GPS devices installed in company cars, as well as the software and applications running on and services provided by these systems including email and voicemail, internet and intranet, instant messaging and the file storage facilities of MHR. For the purposes of this schedule, MHR's CCTV cameras, networks and systems are also included within the definition of IT Systems.

1. REASONS FOR MONITORING

We Monitor employee usage of MHR's IT systems for a number of reasons, including:

- To maintain the security of the systems;
- To identify and deter security threats;
- To determine whether an employee is complying with our relevant policies and procedures;
- To locate deleted messages or messages lost due to a system failure;
- To monitor messages sent to an absent employee;
- To assist in the investigation of alleged wrongdoing;
- To ensure that MHR's confidential information is protected and has not been compromised;
- To comply with applicable legal obligations;
- To improve and enhance the safety of staff and visitors;
- To protect MHR premises and property (and the property of staff and visitors) from criminal activities;
- To facilitate the identification, apprehension and prosecution of offenders; and
- For the purposes of establishing, exercising or defending legal claims.

2. OPERATION OF MONITORING ACTIVITIES

2.1 Types of Monitoring

Monitoring activities should, at all times, be conducted in a way that is both fair and lawful. The types of Monitoring activities that MHR may undertake include:

- Logging and storing internet usage including details about usernames, times spent on websites and the names of visited websites;

- Blocking access to different categories of prohibited websites, such as gambling, pornographic, criminal activity, social networking or similar types of websites;
- Logging all emails sent and received using MHR's IT Systems, including information about the sender, receiver, subject, time and size of the message and name of attached files. MHR may use this log to the extent necessary for its legitimate interests as set out in this Schedule; and
- Inspecting the content of emails to identify a threat to information security (e.g., virus attacks), or if it is necessary in order to investigate a suspicion of crime, breach of contract or protection of confidential information. The content of emails may also be investigated when employees are absent from work.

When using MHR's IT Systems, emails or text messages that are private or marked "private" or "personal" (e.g., in the subject line or because they are stored in a folder marked "private" or "personal") may be Monitored. The fact that a document, voicemail, data or communication has been "deleted" does not mean that the item cannot be retrieved and reviewed.

2.2 CCTV Monitoring

Closed Circuit Television has a legitimate role to play in helping to maintain a safe and secure environment for all our staff and visitors. Separate CCTV policies and procedures apply to any Monitoring conducted via CCTV.

2.3 Covert or targeted Monitoring

You should not engage in covert Monitoring (that is, where individuals are unaware that the Monitoring is taking place or the Monitoring is specifically targeted towards an individual or segregated group of individuals) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or extremely serious misconduct is taking place and, after suitable consideration, your reasonably believe there is no less intrusive way to address the issue. In such a case, the number of people involved in any such covert or targeted Monitoring should be limited to those who have a business need to know or be involved in the monitoring.

2.4 Data Privacy Impact Assessments

Prior to the commencement of any large scale Monitoring activities, a formal Data Privacy Impact Assessment should be conducted to assess our legitimate interests in conducting the Monitoring activities balanced against the impact the Monitoring will have on the privacy of the affected individuals. A further DPIA should be conducted whenever a new Monitoring activity is being considered that is likely to result in high risk to individuals' interests.

2.5 Retention and erasure of Monitoring data

Personal data collected through Monitoring activities must not be retained for longer than is necessary to achieve the purposes for which it was collected. In the event of an investigation, litigation or court proceedings (or if these are anticipated), personal data may be retained at least for the duration of such investigation, litigation or court proceedings.

Endorsed by the Board of Directors of Millennium & Copthorne Hotels plc on 2 August 2018

I have read and understood the contents of this Policy:

Signed:_____ Name (printed):_____ Date:

Please sign and return to your human resources department, retaining an original for your own records.

Version Control

This information will be updated annually.

Document:	Department:	Approved By:
Global Data Protection Policy	Risk & Compliance	General Counsel
Effective Date:	**Last Review Date:**	**Reviewed By:**
02/08/2019	07/07/2019	Global Risk & Compliance

Summary of Changes

Any approved changes will be made to the document and then added to this table.

Date	Summary of Changes Made	Made By
17/07/2018	V1 Initial Document Modification from Lewis Silkin Template	Legal Team
14/03/2019	V1.1 Added 2 new definitions, new template format	Vanessa van Balkom