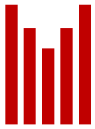

MILLENNIUM

HOTELS AND RESORTS

MILLENNIUM ▪ COPTHORNE

Data Protection Guidance

Objective

This guidance sets out how the Millennium & Copthorne plc group and its direct and indirect subsidiaries ("MHR") should handle data of consumers, customers, suppliers and staff as per our Global Data Protection Policy. We need all our staff to think about data protection in their roles every day to ensure that this guidance is put into practice and to avoid MHR being in breach of Data Protection Laws. Any organisation which processes any personal data must comply with the laws governing the use of personal data.

Table of Contents

Who does this guidance apply to?

This protocol applies to the handling of data by MHR. This protocol (and all other related data protection policies) must be read by all staff members. "Staff member" means all MHR permanent and temporary employees, and all agency and interim staff.

When we refer to "you" in this policy, we mean each individual staff member.

Why is this guidance document important?

A breach of the Data Protection Laws can result in enforcement action by the regulator against MHR and in significant fines being imposed on MHR. Under GDPR fines can be up to €20,000,000 or 4% of worldwide turnover, whichever is higher, depending on the nature and extent of the data breach. Some breaches of the Data Protection Laws even rise to the level of constituting a criminal offence.

More importantly, a breach of Data Protection Laws may cause serious harm or distress to individuals, such as exposure to identity theft through the release of non-public identifiers such as a passport number.

Every type of data is relevant (e.g. names, addresses, e-mail addresses, telephone numbers) and it must all be treated carefully and in accordance with this protocol and the MHR Global Data Protection Policy.

Consequently, any breach of this policy will be taken seriously and may result in disciplinary action.

Which terms do you need to know?

This section gives definitions of the terms used in the Data Protection Laws and which are used in this protocol.

Term	Definition
Controller	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.
Data Protection Laws	The General Data Protection Regulation (EU) 2016/679 ("GDPR"), the UK Data Protection Act 2018 ("UKDPA") and any other national legislation (including the Singapore Personal Data Protection Act 2012 ("PDPA")) that relates to data protection and privacy and applies to MHR.
Data subject	See definition within the definition of personal data below.
European Economic Area or "EEA"	European Union member states plus Norway, Liechtenstein and Iceland.
Information Commissioner's Office or ICO	The regulator in the UK that is responsible for implementing, overseeing and enforcing GDPR and the UKDPA.
Personal Data	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 guidelines relating to the disclosure and protection of personal data apply to the personal data of deceased individuals. In such event, these guidelines 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.
Processing	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.
Processor	A person, public authority, agency or other body which processes personal data on behalf of the controller.
Special categories of data	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.

How do I look after the Data Protection Principles?

There are six principles that we must comply with. The table below gives a high-level summary of these principles. The sections that follow describe how you apply those principles in practice.

DATA PROTECTION PRINCIPLES

1. Personal data must be processed fairly and lawfully and in a transparent manner in relation to individuals;

2. Personal data must be collected for specified, explicit and legitimate purposes and only processed for those purposes except for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes which are allowed;

3. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which the data are processed;

4. Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, are erased or rectified without delay;

5. Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods only for archiving purposes in the pubic interest, scientific or historical research purposes or statistical purposes and only if safeguarding measures are put in place; and

6. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection again unauthorized or unlawful processing and against accidental loss, destruction of or damage to that data, using appropriate technical or organizational measures.

Principles 1 and 2: How do I process personal data fairly and lawfully?

To process personal data fairly, you need to make sure that you only process personal data if the data subject has been told at least:

- who the controller is;
- the purpose for which the data is to be processed by MHR; and
- the identities of anyone to whom the data may be disclosed or transferred.

The information is contained in 'privacy notices' which we give to employees, job applicants, guests, visitors and any other individuals whose personal data we process in different circumstances. You must ensure that you are familiar with our privacy notices and only process personal data as described in those privacy notices. Our privacy notices can be found on our website, guest registration cards and other relevant documentation. Our privacy notice for staff members can be requested from HR.

You can never use data that MHR stores for any different purposes – just because we hold data legitimately does not mean you can re-use for any reason. Also, never access data unless you need to do so for your job.

Personal data may only be processed for the specific purposed notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Data Protection Laws. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before carrying out any new processing (except in certain circumstances where a legal exemption applies).

To process personal data lawfully we must meet certain conditions that are set out in the Data Protection Laws. The conditions that are most relevant to us as an organization are summarized in Tables A and B below.

IMPORTANT

When processing **non-special categories of data**, you must make sure that **at least one of the conditions in Table A** applies.

When processing special categories of data, you must make sure that one of the conditions in Table A applies and at least one of the conditions in Table B also applies.

Table A – Key conditions for processing any personal data

Contracts	Processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract between the data subject and MHR. This is what we use most of the time to provide our services to our customers.
Legal Obligations	Processing is carried out to comply with a legal obligation placed on MHR. This could be so that we can comply with health and safety rules or tax requirements, for instance.

Vital Interests of Data Subject	Processing is carried out to protect the vital interests of a data subject or another person (e.g., where the data subject needs medical care).
Legitimate Interests	Processing is carried out to pursue MHR's legitimate business interests (e.g. collecting personal data from our customers so that MHR can provide its services). This condition only applies if the processing does not adversely affect the interests or fundamental rights and freedoms of the individual concerned. If there is a serious mismatch of competing interests between the business and the individual, the individual's interests will have priority over business interests. This requires careful consideration and a balancing act. Just because we could do something that would be beneficial to MHR does not mean we should, unless we are also protecting and promoting the privacy of our customers and employees.
Consent	Processing is carried out in accordance with any freely given, specific, informed and unambiguous consent of the data subject. Consent must be presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form. Data subjects can withdraw their consent to the processing of their personal data at any time. Consent must be recorded, including what information the data subjects were given about the processing to which they consented.

Table B – Most relevant conditions for processing special categories of data

Explicit Consent	Processing is carried out with the explicit consent of the data subject, unless reliance on consent is prohibited by law.
Employment Obligations	Processing is carried out as part of MHR exercising its obligations under employment, social security or social protection laws, or a collective agreement.
Vital Interests of Data Subject	Processing is carried out to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent (e.g., to give medical care).
Publicly Available Information	Processing is carried out where it relates to the personal data manifestly made public by the data subject.

Consent and explicit consent

One of the possible conditions upon which we can rely to process personal data is the consent of the data subject. Except in the case of sales and marketing campaigns, consent should be utilized as a basis for processing personal data sparingly, and other applicable conditions should be considered. This is for various reasons:

- data subjects can withdraw consent at any time and that would mean that MHR would have to stop processing their data, and this may complicate MHR's processes and may not be possible through existing systems;

- consent is only valid if the data subjects had a genuine choice about whether or not to allow MHR to use their data and it must be freely given, specific and informed; as these standards are hard to meet so there is a risk that any consent may not be valid;

- it will be very difficult to get consent where there is an imbalance in position between MHR and the data subject; and

- best practice guidance stipulates that organizations should not rely on consent where any other condition is available.

The requirement for 'explicit' consent where processing special categories of personal data must meet all the requirements for 'consent' but must be accompanied by a very clear statement which is selected or ticked by the data subject equivalent to:

"I consent to processing of data relating to my medical conditions by MHR in order to [*explain why you need the information, e.g., provide me with a guest room adapted to my needs*]".

Note: The Global Data Protection Policy includes further guidance on the data protection requirements associated with the different types of data processing activities that occur within MHR, such as processing for purposes of employment, marketing (business to consumer and business to business), CCTV and audio recordings, service communications and guest registration.

Principle 3: How do I ensure processing is adequate, relevant and excessive?

Personal data should only be collected because it is required for the specific purpose notified to the data subject. Any personal data which is not necessary for that purpose should not be collected.

Please be cautious when inputting information about individuals into MHR systems (such as a property management system, customer relationship management system, etc.). Do not include information that is not required, e.g., notes/observations about an individual, because this could go beyond the purpose for which the data was originally collected and is not necessary for the processing carried out by MHR.

As well as ensuring that any personal data you process is necessary and relevant for the purpose for which you are processing it, you must at the same time ensure that you have adequate personal data for your purpose. In other words, you should obtain enough information about an individual to enable you to perform your purpose(s) **but no more**.

Principle 4: How do I keep personal data accurate and up to date

Information which is incorrect or inaccurate is misleading and steps therefore should be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date personal data should be destroyed or erased from our systems promptly once you know it is wrong.

Although, ultimately it is MHR's responsibility to make sure personal data is up to date and accurate, we will often be reliant on data subjects themselves to tell us of changes to their personal data. From a practical perspective you should encourage data subjects to contact us if personal data we hold about them becomes out-of-date of if they are aware of any inaccurate data we hold about them (and we encourage data subjects to do this in our privacy notices).

Always enter data into our systems carefully and double check your entries – it could make the difference between having the right or wrong phone number for a customer who you may need to call back to resolve an issue.

Principle 5: How do I ensure personal data is not kept for longer than necessary?
Personal data should be destroyed or erased from our systems when it is no longer required.

For guidance on how long certain data should be kept before being destroyed, see our Data Retention and Disposal Policy, which is available on our compliance policies website (https://www.millenniumhotels.com/en/corporate/grouppolicies/) under Data Protection or can be requested from the Global Director of Risk Management and Compliance.

Note that the Data Retention and Disposal Policy does not give information about how long to retain every type of personal data that may be processed. You therefore must also consider whether there are any data retention policies and procedures that are specific to your department, and with which you will need to comply. It may also be the case that you will need to make decisions about how long to keep certain personal data on a case-by-case basis.

Principle 6: How do I keep data secure
Security measures need to cover technical and physical aspects of security. The security applied must be appropriate to the risk to the data subject of being disclosed, stolen or destroyed. Please refer to MHR's Information Security Policy for further details on MHR's information security requirements.

How do I process data in accordance with the data subjects' rights?
Data subjects are granted various rights by the Data Protection Laws. They can request that MHR take certain actions in respect of their data, in which case we will need to implement such requests promptly.

You need to be aware of the data subject rights listed below so that you can recognize if someone asks for them and follow the correct protocol. Further detail for each of these rights and how to respond to them are set out in the **Global Data Protection Policy** which is available on https://www.millenniumhotels.com/en/corporate/grouppolicies/.

- the right to **rectify** personal data
- the right to erasure **('right to be forgotten')**
- the right to **restriction** of processing
- the right to data **portability**
- the right to **object** to processing
- the right not to be subject to a decision when it is based on **automated processing or profiling**
- the right to access personal data held by MHR **(data subject access request)**

What security measures must I comply with?
Personal data must be kept secure from unauthorized access and from being accidently lost, destroyed or damaged. MHR's Global Information Security Policy sets out our standards and protocols which aim to keep personal data secure and protected.

Security Do's and Don'ts

- Always **keep your password and user name secure** and do not share them.
- Always **lock your computer** while it is unattended.
- **Do not open email attachments** from an unknown source.
- **Do not download** programmes or games or run any of these sent by email.
- **Do not download** business data onto any laptop unless authorized by IT.
- When taking a laptop with you to **another country** for business, or accessing it from another country on a regular basis, ensure that it only contains the customer information you need, and you only access the information you need.

- If your laptop is lost or stolen, contact IT immediately.

If sending an email

- Before sending an email, please think about **what you are trying to achieve** and decide on the best communication method to use. For example, **a telephone call might be more effective.**
- Keep your message brief and relevant and **do not send unnecessary copies** of the message.
- Double **check the recipients** to see you have not mis-entered details.
- Do not attach documents containing **large amounts of data** about people to emails.
- When writing your emails, **always assume that they may have to be disclosed** to a court or regulator, or the people mentioned in the email.
- **Always write your emails as if they are permanent**, because even when they have been deleted from your system, depending on our retention policies they can often still be retrieved and may be disclosable to a court or regulator.
- Your **emails**, even if marked private or confidential, **might also be viewed** by network supervisors or management when lawful to do so.
- **Avoid asking for sensitive personal data** unless necessary for a legal or business purpose **or passing on** sensitive personal data about somebody else.
- Always sending personal data by email **with password protection**.
- **Do not make negative comments** about any individual, including customers, employees or suppliers. If you feel that there is an issue which other people need to be aware of, then sending an email is not the appropriate way of doing this. Speak to your manager first about the next steps.
- Please **tidy your inbox, outbox and folders regularly**. Do not store messages or attachments longer than necessary. (Check out our **Data Retention and Disposal Policy**).

When can I share personal information?

We may disclose personal data we hold to third parties:

- If we have a contract with the third party which includes clauses covering data processing. See 'How do I work with data processors' below.

- If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or comply with any contract with the data subject or other agreements, or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organizations for the purposes of fraud protection and credit risk reduction.

- If the police or law enforcement agencies or regulators require us to provide information to investigate a crime or breach of any law, generally we must comply with their request.

- In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or asset.

If you do send personal data to another organization, you need to think about how do you this and whether you are sending only data that is required by the other organization. You must ensure that any transfer of personal data to a third party is authorised. Please consult the Global Director of Risk Management and Compliance if you have any questions.

How do I work with data processors?

Whenever we work with data processors (who will be our suppliers, such as hosting providers, payroll providers, CRM provider, etc.), we must:

- carry out checks to ensure that they understand their obligations and responsibilities when processing personal data for MHR and that they are capable of meeting the requirements imposed by the Data Protection Laws;

- include a minimum set of clauses in the contract with the data processor, including obligations around security and reporting breaches. Please contact the MHR legal team for assistance with data processor agreements and clauses;

- carry out regular audits or inspections during the life of any agreement, or obtain copies of reports from the data processor which have been carried out by an independent assessor that verify the data processor's compliance with the contract;

- consider whether information will be transferred outside of the EEA (see below); and

- ensure that the processing meets one of the conditions and is covered by the relevant privacy notice and that the other data protection principles will be adhered to, i.e., only relevant and the minimum amount of personal data is disclosed and processed.

Can I transfer personal data out of the EEA?

MHR must not transfer personal data to a country outside of the EEA (European Economic Area) unless one of the following applies;

- it is necessary **to perform a contract** with the data subject (with stress on 'necessary', e.g., to make a hotel booking in another country);

- the data subject has **explicitly consented** to such transfer;

- the country is on the European Commission's approved countries list. You can find a maintained list of approved countries here http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.tm;

- if the personal data is being sent to a US-based organization which is compliant with the 'Privacy Shield'. A list of companies which are signed up to the Privacy Shield can be found here https://www.privacyshield.gov/list; or

- a contract has been put in place with the non-EEA based third party recipient of the personal data and that contract includes European Commission approved standard contract clauses for transfers of personal data outside of the EEA (known as the 'Standard Contractual Clauses').

Note that a transfer of personal data outside of the EEA not only includes sending data to an entity in a non-EEA country (e.g., by email), but also includes allowing access to data from another country, even if the data itself remains within the EEA. For example, where an IT support services company, where employees based in India, remotely accesses MHR systems located in the UK, this constitutes transfer of personal data outside of the EEA.

When do I need to carry out Data Protection Impact Assessments ("DPIA")?

These are key to helping MHR ensure that its processes and systems are privacy-friendly and comply with Data Protection Laws. They are a tool to assess and manage risks to privacy and document the decisions taken by MHR.

Sometimes MHR will be legally required to carry out a DPIA if we are implementing a project which is deploying new technology or new process which involves processing of personal data which are likely to result in a **high risk** to the rights and freedom of individuals. Technologies and processes likely to cause this risk are:

- systematic evaluation based on profiling which leads to decisions that have a legal or significant effect on someone;
- large scale processing of special categories of data or of criminal convictions; or
- systematic monitoring of publicly accessible areas on a large scale.

Examples of projects where a DPIA must be undertaken are implementing a new CCTV system, new HR system/database, new customer loyalty programme or launching a mobile phone app that will capture personal data.

MHR's DPIA template can be found here: https://www.millenniumhotels.com/en/corporate/grouppolicies/. Once completed please issue to your regional compliance team for sign off. A DPIA must be completed and approved prior to the new system or project being launched.

You should speak your regional compliance team if you are doing work that involves any of the following types of processing and discuss with them the likely risks to individuals to determine whether a DPIA is required. Even if it is not mandatory, it is good practice to complete one.

What is likely to cause a high risk to individuals?

It is the new technology or new processing involves two or more of the following types of processing, it is likely to cause a high risk to individuals:

1. Evaluation and monitoring:
   (a) *Evaluation or scoring*: e.g., screening against credit reference agencies, conducting anti-money laundering checks, building behavioural marketing profiles, predicting health risks based on test results.
   (b) *Making automatic decisions that have a legal or similarly significant effect*: e.g., resulting in offering a job to someone or not, offering credit or not.
   (c) *Systematic monitoring*: e.g., observing and monitoring behaviour, especially where people are not aware they are being observed.
   (d) *Refusing people a service:* e.g., if the processing results in a decision not to offer a loan.

2. Sensitive data or data subjects:
   (a) *Sensitive or very personal data*: e.g., any of the special categories of data, criminal data, financial data, location data, electronic journals, personal emails or any data that could be used for identity theft.
   (b) *Vulnerable data subjects*: e.g., data about the elderly, children, mentally ill, asylum seekers, patients, etc.

3. Scale of processing:

(a) *Large scale*: e.g., consider the geographical extents of the data, duration or permanence of processing, volume/range of data, number of data subjects (as a specific number or proportion of the population).
(b) *Combining data sets*: e.g., bringing together data from two different controllers and using it in a way that the data subject would not expect.

4. Innovation or new technologies: e.g., using facial recognition technology. People are less likely to know how their data might be processed by new technologies.

How do I do it?

A DPIA must include:

- a description of the processing operations, showing who inputs data, where it goes, who accesses it, what systems are used, what third parties or international transfers are involved etc.;
- the purposes of the processing and MHR's legal grounds for processing;
- an assessment of the necessity and proportionality of the processing in relation to the purposes;
- an assessment of the risks to the rights of individuals (note: this is not the risk to BPS but the impact on individuals if their data was lost, hacked, corrupted, disclosed, etc.); and
- the measures taken to address these risks.

What to do if a breach occurs?

How do I identify a personal data breach?

The first step is to be able to identify a personal data breach. It can happen in a number of ways. *It isn't only about loss or theft of personal data*. There are many other examples of personal data breaches, including:

- human error, e.g., sending an email to the wrong recipient or sensing a marketing email to recipients in the "to" or "cc" field, thereby enabling each recipient to see the email addresses of the other recipients;
- loss or theft of data or equipment on which data is stored, e.g. leaving a laptop, USB stick or a paper file containing personal data on the train;
- unauthorized access to personal data, e.g., an individual has accessed data that they should not have been to access by using someone else's password;
- our IT systems being hacked and personal data being taken or personal data being obtained by cyber-criminals be deception, e.g., through spoof or blagging emails;
- personal data being encrypted by hackers demanding a ransom to unencrypt it or if the key to encrypted data is lost;
- failure or unavailability of equipment that means that personal data is unavailable, e.g., if we experience a power failure or if hackers prevent us from using our IT systems; and

- loss or unavailability of personal data due to fire or flood.

Reports all concerns quickly!

MHR must report certain data breaches to relevant regulatory bodies within a very short period of time. Since data security concerns may arise at any time and in light of the strict obligations imposed on MHR under the Data Protection Laws, you must report any concerns you have to your regional compliance team as soon as possible, so we can deal with it appropriately. If you have done something that has caused a personal breach, please do not panic! Immediately report the personal data breach as described in the paragraph below so that the correct procedures can be followed. Failure to report a breach may be a disciplinary offence.

How do I report a concern?

You should immediately log an incident with your regional compliance team if you know, or suspect, that a personal data breach has occurred. A cross-functional data breach team will then take appropriate steps to deal with the report using our Data Breach Policy, which is available separately. They may need to talk to you to find out more details so please respond to them quickly if they do.

Please do not do anything else about the breach on our behalf. If we need to notify any affected individuals or the regulator, the data breach team will take responsibility for this.

Data Protection by design and by default

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start, taking into account the state of the art, cost of implementation and the nature, scope, context and purposes of processing as well as the risks to rights and freedoms of data subjects. It includes using tools and techniques such as pseudonymizing data minimization to protect rights and freedoms of data subjects.

Privacy by default requires controllers to adhere to the data protection principles.

MHR aims to achieve these standards by implementing the following tools and principles:

- governance of privacy within MHR through a central steering group and regional compliance teams;

- training staff annually to ensure that privacy is a live issue and one they are required to think about in the course of carrying out their jobs;

- data protection risk assessments will be a key tool, embedded in our project management procedures and change management procedures to ensure that every project assesses whether or not a DPIA is required, and if required, is carried out before implementation of the project to allow privacy risks to be raised, assessed and resolved;

- our security measures to protect personal data from external and internal malicious threats;

- access rights on our systems form part of our security measures and are key to ensuring that the right staff have access to the right information to enable their job and to protect privacy;

- our policy framework informs staff about how to handle personal data and the importance of keeping it secure and protecting the privacy of our staff, customers and suppliers; and

- we demand high standards from our suppliers who process data; we conduct due diligence on them before we enter into a contract and if required monitor their performance through the life of the contract, including specifically addressing privacy issues.

Version Control

This information will be updated annually.

Document:	Department:	Approved By:
Global Data Protection Guidance	Risk & Compliance	General Counsel
Effective Date:	**Last Review Date:**	**Reviewed By:**
12/07/2019	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
13/03/2019	Initial Document Modification from Gowlings, LLP Template	Vanessa van Balkom