MILLENNIUM
HOTELS AND RESORTS
MILLENNIUM ▪ COPTHORNE

Data Protection Impact Assessment (DPIA)

CONFIDENTIAL

MILLENNIUM
HOTELS AND RESORTS
MILLENNIUM • COPTHORNE

Data Protection Impact Assessment

You have to complete this Data Protection Impact Assessment ("DPIA") for certain types of projects where there is likely to be a high risk to the rights and freedoms of individuals. This is required by the General Data Protection Regulation 2016 ("GDPR").

This DPIA template must be used in conjunction with the DPIA Guidance document which can also be found on www.millenniumhotels.com/en/corporate/grouppolicies/.

This DPIA consists of 7 steps. Do them in order:

1. Step One: Context and Background
2. Step Two: Data Map and Data Flows
3. Step Three: Who's who
4. Step Four: Assessment against GDPR requirements
5. Step Five: Risk Analysis and Mitigations
6. Step Six: Consultation (if required)
7. Step Seven: Sign Off

There are notes in the Guidance which explain some of the legal terms used and give more detail to help you answer the questions.

Once the DPIA is signed off, keep the finished document as a record of the analysis, risks identified, mitigations and decisions taken.

If the project /system/ procedure changes significantly, this DPIA should be amended and updated.

If you have any questions about how to complete this DPIA, please contact your Regional Compliance Team or the Director of Risk Management & Compliance at RiskandCompliance@millenniumhotels.com.

STEP ONE: CONTEXT AND BACKGROUND

1 What is the project/system about? (We'll call this "Project" throughout this DPIA.)

2 What will the benefits of the Project be to Company? What are the benefits to individuals?

STEP TWO: DATA MAPS AND DATA FLOWS

1 Insert or attach a data map which shows the following information (this can be a separate document that you attach to this DPIA. It can be a spreadsheet, architecture diagram or table as long as it captures all of the information below. It should be as detailed as you can make it, relevant to the amount of data involved and risks to individuals):

1.1 what personal data will be collected through the Project (e.g. name, address, phone number, NI number, bank details);

1.2 what types of systems will be used (e.g. CRM, HR, finance);

1.3 who 'inputs' data (e.g. consumer users, supplier personnel);

1.4 who views data (e.g. senior management, supplier's support personnel);

1.5 who can amend and/or delete data (e.g. members of HR team, supplier's personnel);

1.6 any third parties who store / see / store/ amend data (e.g. name the third party suppliers) or third parties with whom data is shared for them to use for their own purposes (e.g. a pension trustee sharing with an employer for the employer's purpose);

1.7 any international transfers of data outside of the European Economic Area which is European Union countries plus Norway, Liechtenstein, Iceland and Croatia ("**EEA**").

STEP THREE: WHO'S WHO and WHAT'S WHAT

TABLE 1: Identify the different parties:

Legal name	**Meaning**	**Who is this?**
Controller	Party who decides what data to collect and what it is used for	*[Note: there could be more than one. List them all.* *Include other group companies if they are controllers.* *Controllers could be based outside of the EU if they offer goods or services to EU citizens, or if they monitor EU citizens.* *Some service providers could also be controllers.]*
Processor	Party which processes on behalf of the controller	*[Note: there could be more than one. List them all.* *Include other group companies if they are controllers.]*
Joint controller	Where 2 controllers process for the same purpose	*[Note: this is will be quite rare. Lists the companies if any, or mark N/A]*
Data subject	The individuals whose data is being processed	*[Note: list categories e.g. consumers, employees]*

TABLE 2: Identify the condition for processing each piece of data (not special categories of data):

Piece of personal data	**Purpose of processing**	**Legal condition for processing**	**If relying on legitimate interests…**
[Describe the personal data field e.g. full name]	*[Describe what it is used for e.g. to identify individual's purchase. Where it is used for different things, set all out.* *If one piece of data is used for different purposes, you will need to identify a legal condition for processing for each purpose.]*	*[Select ONE option. See NOTE 1 of the Guidance for an explanation of each]* ☐ Legitimate business interests ☐ To perform a contract with the data subject ☐ To comply with a legal obligation ☐ Vital interests of the data subject ☐ Consent *[Note: this should be a last resort]* ☐ Public interest or exercise of official authority for public authority	What is the legitimate interest? *[insert response]* How does it affect the rights and freedoms of individuals? Why does it override those rights and freedoms? *[insert response]*
		[Note: repeat the options above for each row of personal data]	

TABLE 3: Identify the condition for processing each piece of special categories of data:

Piece of personal data	**Context of processing**	**Legal condition for processing**
[Special categories of data are: • *racial/ethnic origin;* • *political opinions;* • *religious/philosophical beliefs* • *trade union membership* • *genetic data* • *biometric data* • *health data* • *sex life* • *sexual orientation]* *[Describe the personal data field e.g. ethic origin]*	*[Describe what it is used for e.g. to identify individual's purchase. Where it is used for different things, set all out]*	*[Select ONE option. See NOTE 2 of the Guidance for an explanation of each and full list]* ☐ Explicit consent ☐ Employment Obligations ☐ Vital interests of the data subject ☐ Publically available information ☐ Legal claims

TABLE 4: Identify the processors (or service providers which are controllers) and set out:

Name of service provider (whether processor or controller)	**Do you have a written contract containing the minimum clauses?**	**Due diligence – what evidence was collected from the service provider to show that they are GDPR compliant?**	**Is information transferred to the processor (or their subprocessors) outside of the EEA?**	**If so, what approved transfer mechanism is used?** [See Note 3 of the Guidance for more detail on each and for less common mechanisms]
[insert name]	[Yes][No]	*[Note: check with your procurement/legal departments to see what evidence was obtained.]*	[Yes to *[insert countries]*] [No]	☐ Finding of adequacy by European Commission ☐ Binding Corporate Rules (intra group transfers only) ☐Standard Model Clauses ☐ Privacy Shield ☐ [Approved code of conduct - NOT YET available] ☐ necessary for performance of a contract between controller and data subject *[Note: the transfer must be necessary to fulfil the contract e.g. booking a hotel in another country. Merely using a*

				supplier who is based in another country will not be sufficient.]
				[Note: repeat the tick boxes for each row]

STEP FOUR: **ASSESSMENT AGAINST LEGAL REQUIREMENTS**

Risk assessment to be completed by the Department Head and agreed with the Regional Compliance Team.

Number	Question	Answer	R/A/G status
Consent based processing - only complete if consent will be relied on as a condition for processing personal data as noted in Step 3, Table 2.			
1	Consent must be specific, informed and unambiguous. Describe how data subjects will be given clear information about how and why their data is being used for all the processing for which consent is required?		
2	What affirmative action will the data subject take to indicate explicit consent is given (eg. such as a signature, tick box or other action) and does this stand-alone from other consents/actions?		
3	How will evidence be retained to demonstrate that consent was given and that the data subject was provided with clear and unambiguous information about what they were consenting to?		
4	If personal data of children under the age of 16 will be collected in connection with a website, how will the consent of a person with parental responsibility be obtained and evidenced?		
5	How could a data subject tell the Company that they want to withdraw consent? How will this withdrawal be actioned and evidenced?		

Number	Question	Answer	R/A/G status
Privacy notices [See Note 4 of the Guidance]			
6	Will data be obtained directly from the data subject, or from a third party (and if so, which third parties/in what circumstances)?		
7	Certain information must be provided in the privacy notice. [See Note 4 of the Guidance] Has the Legal Department approved the privacy notice?		
8	How and when will privacy notices be provided? (include detail about considerations for layout of privacy notices in small formats / on handheld devices).		
9	How will changes to privacy notices be brought to the attention of individuals?		
Joint data controllers – only complete if joint data controllers were identified in Step 2, Table 1			
10	Which of the joint data controllers will be responsible for providing privacy notices, point of contact for data subject, responding to subject access requests and assisting with requests from data subjects exercising other data subject rights?		
11	How will information about the arrangement between the controllers be made available to the data subject?		

Number	Question	Answer	R/A/G status
Data minimisation [See Note 5 of Guidance]			
12	Is the information you are using of good enough quality for the purposes it is used for (i.e. it is the right information and sufficiently detailed for the purpose)?		
13	Is there any personal data could you not use, without compromising the needs of the Project (i.e. are you collecting/processing too much information to achieve the purpose)?		
14	Are there controls to prevent unnecessary information being collected and processed? (e.g. staff do not record additional information in free text boxes)		
Accuracy [See Note 6 of Guidance]			
15	How are you ensuring that personal data is accurate when it is collected? (e.g. obtained directly from data subject, data subjects correct / amend data themselves, checked against third party source like DVLA or public records).		
16	How is data erased or amended promptly once you are aware data is incorrect?		
17	Are there instances where we will not be able to rectify inaccurate data, for example where it might be held in back-up files that cannot be altered?		

Number	Question	Answer	R/A/G status
	If so, provide relevant detail and what will be done to mitigate risks of relying on inaccurate or incomplete data.		
Storage Limitation [See Note 7 of the Guidance]			
18	How long will data need to be retained for the purpose for which is its processed? There may be different periods for different categories of data. Please set them all out.		
19	How will the Project/systems you have in place allow you to delete information in line with relevant retention periods?		

Number	Question	Answer	R/A/G status
Integrity and confidentiality (security) [See Note 8 of the Guidance]			
20	What measures are in place to protect against security breaches? Consider physical and technical security, across the whole Project i.e. on the Company's systems/processes and any service providers. *[Note: you can cross refer to MHR's Information Security policy or a provider's security policy. It should be attached to the DPIA.]*		
21	How is access to data controlled and recorded? *[Note: this may be covered by the answer to question 20 above.]*		
22	What training and instructions are necessary to ensure that staff (of the Company and any relevant service providers) know how to use/hold personal data securely?		
Record keeping [See Note 9 of the Guidance]			
23	Will necessary records be created and how?		
24	Who will be responsible for creating, holding, maintaining and updating these records?		

Number	Question	Answer	R/A/G status
Rights of data subjects to access their personal data ("Data Subject Access Right") [See Note 10 of the Guidance]			
25	How will the Company respond to requests from individuals to access their personal data? i.e. can you respond within the timeframe, search for personal data across all systems, provide copies of the data (redacted as required) and provide information about automated decisions and profiling (including consequences of decisions/profiling). *[Note: Please refer to MHR's Data Protection Policy and Data Subject Rights Policy.*]		
26	Have you considered whether individuals would be given automated access to all/some of their data?		
Automated decision making and profiling [See Note 11 of the Guidance]			
27	Will any automated decision making/profiling of data subjects take place?		
28	If so, will this have a legal or significant effect on them and if so what effect?		
29	If there will be a legal or significant effect, is this (a) authorised by law or (b) necessary to perform a contract with the data subject? If neither (a) nor (b) apply, how will you obtain consent to the profiling/automated decision?		

Number	Question	Answer	R/A/G status
30	How will individuals be able to contest decisions, express their points of view about a decision and request a human intervention? (e.g. contact data protection officer)		
Criminal convictions and offences [See Note 12 of the Guidance]			
31	Does the Project involve processing of criminal convictions and offences information?		
32	If so, is this permitted by law in the relevant countries and how will safeguards imposed in each country be complied with?		
Rectification and completion requests [See Note 13 of the Guidance]			
33	How will requests for rectification of inaccurate personal data or completion of incomplete data be handled? (e.g. by the customer contact centre team, or by referral to the legal team)		
34	Are there instances where we will not be able to rectify inaccurate data, for example where it might be held in back-up files that cannot be altered? If so, provide relevant detail and what will be done to mitigate risks of relying on inaccurate or incomplete data.		

Number	Question	Answer	R/A/G status
Erasure (right to be forgotten) requests [See Note 14 of the Guidance]			
35	How will requests for erasure of personal data be handled (including checking whether we are required to comply with the request)? (e.g. by the customer contact centre team, or by referral to the legal team)		
36	Are there instances where we will not be able to erase data, for example where it might be held in back-up files that cannot be altered?		
37	How will the data be erased?		
Right to restrict personal data processing [See Note 15 of the Guidance]			
38	How will the Project/the systems you are putting in place allow you to respond to requests from individuals to restrict their personal data? What will be the process for handling these requests?		
Passing on requests for correction, erasure or restriction to third parties [See Note 16 of the Guidance]			
39	If you identified in Step 3, table 4 that you passed personal data to other controllers or processors, how will you tell those companies if a data subject wants to correct, erase or restrict processing of their personal data?		
Requests to receive personal data or transfer personal data to another party (right of portability) [See Note 17 of the Guidance] Only complete if you identified in Step 3, table 2, that data is processed on the basis of consent or for a contract?			

Number	Question	Answer	R/A/G status
40	Are the system(s) able to distinguish between data processed under different conditions or will the Company allow data subjects to port all of their data?		
41	How will data subject rights to receive or transfer personal data to another data controller be handled?		
42	Will it be technically feasible to comply and if not, why not?		
43	What format will data be supplied in?		
Right to object [See Note 18 of the Guidance]			
44	Do privacy notices and company policies ensure that individuals are told about their right to object, clearly and separately, at the point of first communication?		
45	Are marketing suppression lists and processes (including those operated by third parties) capable of recording objection requests?		
Security breach notification [See Note 19 of the Guidance]			
46	Does the Company have a breach notification policy or checklist?		

Number	Question	Answer	R/A/G status
47	If the answer to 46 is no, how are breaches reported internally within the Company? What is the process for notifying the regulator and notifying data subjects if necessary?		
48	Are data processors required to notify of breaches to you and to assist with investigation and mitigation?		
If your organisation is subject to the Human Rights Act or similar, you also need to consider the questions below [See Note 20 of Guidance]			
49	Will your actions interfere with the right to privacy under Article 8 of the European Convention on Human Rights?		
50	Have you identified the social need and aims of the Project?		
51	Are your actions a proportionate response to the social need?		

STEP FIVE: Risk Analysis and Mitigations

(a) What are the risks to individuals? Consider things like unauthorised access, changes that are not permitted or are malicious, loss or disappearance of data. How would these impact individuals (e.g. identity theft, access to bank accounts, claiming benefits). Include the likelihood and severity of such risks. What security/other measures (e.g. training) will be implemented to mitigate the risk?

Risk	**Source**	**Risk to Individuals (e.g. security of their personal data)**	**Severity of risk**	**Likelihood of risk**	**Solution to combat risk**	**Is any remaining risk acceptable because it is proportionate to the nature and scope of the Project?**

(b) List below any amber or red flagged rows from Step 3 above.

Privacy Issue Row Number (link to Red/Amber items in Step 3)	Risk to Individuals (e.g. security of their personal data)	Action point to mitigate risk	Rationale for action point	Is any remaining risk acceptable because it is proportionate to the nature and scope of the Project?

STEP SIX: CONSULTATION

(a) If the Company has a Data Protection Officer or Regional Compliance Team, have they been consulted on the Project and on the responses to this DPIA? Are they satisfied that the DPIA has been carried out in accordance with the requirements of the GDPR?

(b) Have data subjects been consulted (if this is appropriate)?

(c) If there are any risks identified which indicate a high risk to data subjects and the controller cannot mitigate those risk, has the supervisory authority been consulted?

STEP SEVEN: Sign Off

Risks, solutions and outcomes accepted and approved by the Regional Compliance Team and Department Head:

Position:

Date: