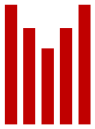

MILLENNIUM

HOTELS AND RESORTS

MILLENNIUM ▪ COPTHORNE

Global Data Protection Impact Assessment (DPIA) Guidance

Table of Contents

NOTE 1: Legal conditions for processing

To lawfully process personal data, a data controller must be able to satisfy what are referred to as 'conditions for processing' for all personal data.

This table lists the conditions for normal personal data (i.e. not special categories).

Business Interests	This is the most commonly used condition to pursue business' legitimate business interests (e.g. collecting personal data from its customers so that the organisation can deliver its projects/services). You must check through that the processing does not adversely affect the individual concerned by overriding their fundamental rights and freedom. If there is a serious mismatch of competing interests between the business and the individual, the individual's interests will come first, especially if that individual is a child.
Contracts	To enter into a contract between the controller and the data subject or to perform such a contract.
Legal Obligations	To comply with legal obligations placed on the organisation. This does not apply to contractual obligations.
Vital Interests of Data Subject	To protect the data subject's vital interests (e.g. where an individual's personal data needs to be disclosed in a medical emergency).
Consent	The data subject has given their consent to the processing (see below). You should avoid relying on this condition unless absolutely necessary due to the high standard that must be achieved for a valid consent and the issue with consent being refused or withdrawn.

CONSENT and EXPLICIT consent – issues to note

- **The organisation must demonstrate (or provide evidence) that consent was given by the data subject to the processing.**

- **Consent must be specific, informed and unambiguous, and involve clear affirmative action. This means the relevant consent must be active and not rely on silence, inactivity or pre-ticked boxes.**

- **The explanation of the processing to which the data subject is giving consent must be in clear, plain, intelligible language and be easily accessible by the data subject. Consents must therefore be granular, i.e. a separate consent for each separate piece of processing.**

- **Consent does not have to be in writing, but if it is given orally, the controller must be able to evidence that consent was given, and what it was given for.**

- **Data subjects must have the right to revoke their consent at any time, and it must be as easy to withdraw consent as it is to give it. In practice, as a minimum this is likely to require organisations to allow consent to be withdrawn through the same media (e.g. website, email, text) as it was obtained.**

- **Consent must be freely given. This means that where the performance of a contract is made conditional on consent to the processing of data that is not necessary for the performance of that contract, such consent will be presumed not to be freely given.**

- **For consent to processing of children's data in relation to the offering of information society services (e.g. social media), it must be given or authorised by a parent or guardian and the organisation must take reasonable efforts to verify the consent is so given or authorised.**

- **Consent must be appropriate to the age and capacity of the individual (i.e. applicable if the personal data is about children and vulnerable adults).**

- **Any consents given should be reviewed periodically to check whether they remain adequate (i.e. the individual's circumstances might change, and this could affect the consent previously given).**

EXPLICIT CONSENT – requires all of the above PLUS a totally unambiguous statement such as:

"I consent to [Company] processing my [healthcare data] for the purpose of [providing me with an estimate for life insurance].

NOTE 2: Legal conditions for processing special categories of personal data

This table lists the conditions for special categories of personal data.

Explicit consent	The data subject has given explicit consent to the processing (see consent box above).
Employment Obligations	To exercise the organisation's legal obligations or rights in connection with employment, social security or social protection law, or a collective agreement (e.g. sick pay administration, or checking that an individual is eligible to work in a country that the organisation operates in).
Vital Interests of Data Subject	Where an individual's medical information needs to be disclosed in a medical emergency or to protect their safety where they cannot give their consent.
Not for profits	Where processing is done by a foundation, association or not-for-profit with a political, philosophical, religious or trade union aim and, on the condition, that the processing relates only to members/former members who have regular contact and personal data is not disclose to any third parties without the data subjects' consent.
Publicly Available Information	The personal data has been made public as a result of steps deliberately taken by the data subject. Be cautious where relying on this condition – information available publicly such as on the internet, may not have been made public by the data subject themselves (in which case this condition would not apply).
Legal Rights	To establish, exercise or defend the legal rights of the organisation.
Public interest	Processing is necessary for reasons of substantial public interest, on the basis of law
Medicine / healthcare	Processing is necessary for preventative or occupational medicine, for the assessment of working capacity of employees, medical diagnosis, provision of health or social care or treatment or management of health or social care systems, or pursuant to a contract with a health professional
Public health	Processing is necessary for reasons of public health, e.g. protecting against serious cross-border threats to health, ensuring high standards of quality and safety of medicinal products or devices
Archiving	Processing is necessary for archiving in the public interest, scientific or historical research, statistical purposes

NOTE 3: International transfers

Personal data cannot be transferred to recipients in "third countries" (i.e. outside of the EEA, which is the EU plus Iceland, Lichtenstein, Norway and Croatia) unless the recipient provides an adequate level of protection through one of the 'approved transfer mechanisms' set out in the GDPR, which are as follows:

Approved mechanism	**Explanation**
Finding of adequacy	The EC has found that some countries do have an adequate level of protection (see list at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm) so transfers to these countries do not require additional protections.
Binding Corporate Rules	These only apply to transfers within a group of companies. These are a set of policies which have been approved by a regulator as ensuring adequate protection. To see a list of companies which have BCRs, see https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/
Standard Model Clauses	These are a set of clauses approved by the European Commission. They are non-negotiable.
Privacy Shield	Only relevant for transfers to companies in the US who have signed up to the scheme and who have self-certified. You can check which companies have self-certified at https://www.privacyshield.gov/list
Approved code of conduct / certification	NOT YET available – no codes/certifications yet approved by the European Commission
Necessary for performance of a contract between controller and data subject	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. The transfer could also be necessary to fulfil a contract made in the *interest* of the data subjects.
Public interest	The transfer must be necessary for important reasons of public interest.
Establishment, exercise or defense of legal claims	The transfer must be necessary for this purpose.
Vital interest of the data subject	Where the data subject is physically or legally incapable of giving consent and the transfer must be necessary to save their life or give significant health benefits or other protections to their physical safety.
Explicit consent of the data subject	Note that 'explicit' consent is a higher standard than 'consent'. See Note 1 above.

	This will only be practical for transfers involving a handful of data subjects due to the requirement for explicit consent, which can be withdrawn.
Legally binding agreement between public authorities	Only available to public authorities.

NOTE 4: Privacy notices

Privacy notices must be provided in a concise, transparent, intelligible and easily accessible form in writing (which includes electronically) or orally if requested by the data subject. Notices must be provided at the time when personal data is obtained.

Required contents of a privacy notice where data is obtained directly from data subjects:

- Identity and contact details of controller
- Identity and contact details of representative (if any)
- Data protection officer details (if any)
- Purpose of the processing of personal data and legal basis of processing
- Where processing is consent based (under Article 6(1)(a) or Article 9(2)(a)), right to withdraw consent at any time
- If processing on basis of Article 6(1)(f) (i.e. legitimate interests of controller or third party), explain (at the latest in the first communication with the data subject):
    - What the legitimate interest is
    - Why on balance those legitimate interests override the rights and freedoms of data subject
- Whether provision of personal data is a statutory or contractual requirement or necessary to enter into a contract
- Whether data subject obliged to provide personal data and possible consequences of not providing
- Recipients or categories of recipients of personal data
- Whether controller will transfer personal data to a 3rd country or international organisation and existence of absence of adequacy decision of Commission or if transferring pursuant to Article 46 (Transfers subject to appropriate safeguards), Article 47 (Binding Corporate Rules) or the second subparagraph of Article 49(1) (transfers necessary for performance of contract with the data subject) reference to appropriate or suitable safeguards and means to obtain a copy of them or where they have been made available
- Existence of automated decision making including profiling and meaningful information about logic involved and significance and envisaged consequences for the data subject
- Period for which personal data stored or if this is not possible criteria to be used to determine this period

- data subject rights to:
    - object to processing of their personal data (must be clearly presented and distinguished from other information). *Not applicable to public authorities in performance of their tasks so need to keep this in mind if personal data received from a public sector).*
    - request (in relation to data subject' personal data), rectification, erasure or restriction of processing
    - request access to their personal data
    - request data portability of their personal data
    - Right to complain to supervisory authority
- If personal data to be used for direct marketing and associated profiling, the right to object to this must be brought to the attention of the data subject at the latest in the first communication with them and must be clear and separately presented from other information.

Required contents of a privacy notice where data is obtained from third parties:

Same as above PLUS:

- Categories of personal data concerned
- the source of personal data (including whether came from publicly accessible sources)

but without:

- Whether provision of personal data is a statutory or contractual requirement or necessary to enter into a contract
- Whether data subject obliged to provide personal data and possible consequences of not

NOTE 5: Data minimisation: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose or purposes for which they are processed.

You must only collect the minimum necessary to fulfil the purposes of the Project and no more. If the Company can use anonymised or pseudonymised data instead of personal data, then it should do so. Data must not be collected "in case" it is useful or because it is "nice to have".

NOTE 6: Accuracy: Personal data shall be accurate and, where necessary, kept up to date.

Company must ensure the personal data it holds is accurate and kept up to date. To achieve this in practice, individuals should be encouraged to check the accuracy of their personal data and to notify Company of any inaccuracies by following a simple procedure which should be set out in Company's privacy notices or available for individuals to self-administer through their accounts. This does not require Company to independently verify information that individuals give to Company.

NOTE 7: Storage limitation: Personal data shall not be kept in a form that permits identification of data subjects for longer than necessary for the purpose for which it is processed.

This means that personal data should be anonymised, pseudonymised, destroyed or erased from Company's systems (including any group company's systems and any third party data processor's systems) when it is no longer required.

To comply with this principle, Company should have a data retention policy that sets out when different types of data are deleted. Refer to Company's data retention/destruction policy. You need to check that these are appropriate for the purpose for which data is collected for the Project, or whether shorter or longer periods are required. You should also consider though whether data can be anonymised or pseudonymised sooner than it is destroyed under the policy.

Retention of personal data for the purposes of defending potential claims should not be used as a justification for retaining large amounts of personal data 'just in case'. The DPIA should consider whether claims are a real risk or not for the Project, i.e. how likely they are and whether in the circumstances, there is a significant enough risk that it would warrant retaining the personal data in question.

Retaining data for archiving purposes in the public interest, scientific or historical research purpose or for statistical purposes is permitted, subject to maintaining appropriate security measures.

NOTE 8: Integrity and confidentiality (security): Appropriate technical and organisational measures shall be taken to ensure appropriate security against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

There are no pre-defined or specific security requirements. Organisations should deploy an appropriate level of security depending on the risks to individuals, i.e. what physical financial or emotional damage or distress could be caused to individuals if there were a security breach such as discrimination, identity theft or fraud. In deciding what is appropriate, bearing in mind the risk, take into account:

- Good industry practice
- Cost of implementation
- Nature, scope, context and purpose of processing i.e. how confidential/sensitive it is, how extensive is the use, how much data is involved etc.

Security needs to consider the following measures which could include (as appropriate):

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measure for ensuring the security of the processing.

Some key recommendations from data protection regulators in terms of security are physical security, e.g. access cards, access control to documents containing personal data (particularly if it is sensitive personal data) and in terms of software/systems, resilience testing and encryption on computers and mobile devices. Other countries or sectors may have specific security requirements prescribed by their data protection regulators, so you should also check if any particular security requirements apply.

NOTE 9: Record keeping

The GDPR requires that records of personal data processing activities are maintained by controllers and processors. These records may need to be shared with relevant data protection regulators on request.

If Company is a controller, the records must contain the following information:

- Name and contact details of data controller (and joint data controllers if any)
- Name and contact details of their representatives
- Name and contact details of Data Protection Officer (if any)
- Purposes of processing
- Description of categories of data subjects and personal data
- Categories of recipients to whom personal data has or will be disclosed (incl. in third countries or international organisations)
- Any transfers to third countries or international organisations and appropriate safeguards
- Envisaged time limits for erasure of different categories of personal data
- General description of Article 32(1) technical and organisation measures

If Company is a processor, the records must contain the following information about processing activities on behalf of the controller, containing:

- Name and contact details of the data processor(s) and data controllers on behalf of which the data processor is acting
- Name and contact details of data controller's or data processor's representatives
- Name and contact details of Data Protection Officer (if any)
- Description of categories of processing on behalf of each data controller
- Any transfers to third countries or international organisations, identity of countries or organisations and appropriate safeguards in place
- Where possible, general description of Article 32(1) technical and organisation measures

NOTE 10: Data subject access right ("DSAR")

Check to see if Company has a policy for responding to DSARs and co-ordinate with the internal teams that deal with DSARs to check that DSARs received in connection with the Project can be handled in the same way.

Individuals have a right to ask controller to give them the personal data that the controller processes and to be informed of:

- what personal data of theirs is being processed by a data controller;
- the purposes for which their personal data is being processed;
- the source of the personal data;
- how any automated decisions taken about them have been made and the logic involved in making any such decisions; and
- to whom their personal data may have been disclosed.

A DSAR does not have to be served in a particular format, or even mention data protection legislation. The only requirement is that it is made in writing and requests information relating to the requesting individual's personal data.

In most cases, a DSAR must be responded to promptly, but in any event within 30 calendar days of receipt (unless you can justify an extension for up to 2 months), and any information must be provided in an intelligible form.

NOTE 11: Automated decision-making and profiling

Individuals have the right to not be subject to automated decision making (including profiling) which has a legal effect or significant effect on them unless it is:

- With consent of the data subject*
- Necessary to enter into or perform a contract with the data subject
- Specifically authorised by EU laws

*If the processing involves special categories of personal data we must obtain consent.

In any event, Company needs to implement measures to safeguard individual's rights and freedoms, which at a minimum means allowing a human intervention into the process and allowing the individual to express their point of view and contest the decision.

NOTE 12: Criminal convictions

Criminal convictions and offences information may only be processed if permitted by laws in the relevant Member State and if the processing is in accordance with requirements in place to safeguard the rights and freedoms of data subjects.

NOTE 13: Right to rectification

Subject to certain exceptions, individuals will have the right to ask Company to rectify inaccurate personal data or complete any incomplete personal data we hold about them. We must comply without undue delay.

NOTE 14: Right to erasure

Subject to certain exceptions individuals will have the right to ask us to erase their data and we must comply without undue delay if one of the following applies:

- The personal data is no longer necessary in relation to purpose for which it was collected or otherwise processed
- The data subject withdraws consent (where we processed based on consent) and there are no overriding legitimate grounds for processing the data
- The data subject objects pursuant to Article 21(1) (processing on basis of legitimate interests or performance of a task in the public interest or exercise of official authority vested in the controller) and there are no overriding legitimate grounds for processing the data
- The data subject objects pursuant to Article 21(2) (right to object to direct marketing)
- The personal data was unlawfully processed
- Erasure is required for compliance with legal obligations of the EU or Member State law
- The personal data was collected in relation to information society services offered to children

NOTE 15: Right to restrict processing

Individuals will have the right to ask us to restrict processing of their personal data if:

- Its accuracy is contested (restriction is then for a period to allow for verification)
- We no longer have a need or lawful reason to process the personal data but the data subject wants us to restrict processing of the data instead of erasing it (for example, the data subject might wish to preserve the data to establish, exercise or defend against a claim)
- The data subject objects to the processing, however, we believe we have overriding legitimate grounds for processing the personal data. In this situation, an individual might ask us to restrict the data pending verification of whether we have overriding grounds which enable us to keep the data

Restricted personal data must:

- be marked as restricted; and
- only be stored and not used for any purpose unless with the consent of the data subject or if we need to establish, exercise or defend legal claims or protect the rights of other people.

NOTE 16: Notifying third parties

If personal data has been shared with third parties (who are controllers or processors), Company must tell them if an individual wants to have their information corrected, erased or restricted, unless it is impossible or involves disproportionate effort to do so.

NOTE 17: Right to portability

Individuals will have the right to ask Company to provide their personal data to them in a structured, commonly used and machine reasonable format.

The data subject may also ask us to transmit their personal data to another data controller (*if technically feasible*), if our processing is:

- Based on consent (i.e. this was a condition we relied on to process their personal data in the first place)
- Based on the condition that it is necessary to enter into and perform a contract with the data subject
- Automated processing

Some exceptions apply where we do not need to do this.

NOTE 18: Right to object

Individuals have the right to object to the processing of their personal data (including profiling) which is based on the legal conditions of public interest or legitimate interest only. If individuals object, Company must stop processing unless it can demonstrate compelling legitimate grounds for processing which override interests and freedoms of the individuals or to establish, exercise or defend legal claims.

Individuals can also object to use of their data for direct marketing (including any profiling related to marketing).

NOTE 19: Security breach notification

Breaches of GDPR likely to result in harm to data subjects need to be notified to regulators within 72 hours of Company becoming aware that the breach has occurred. Note that this is any breach, not just a security breach.

Breached likely to result in a high risk to data subjects must also be notified to data subjects, unless the risk has been mitigated

This means that we need to be prepared for a security breach so that any necessary action to notify the breach can be taken in a swift and organised way.

NOTE 20: Human rights

Article 8: Right to respect for private and family life

Everyone has the right to respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

In the UK, the Human Rights Act 1998 do not apply to private sector organisations, but the principles are included in the PIA because if there was ever any litigation concerning the data processing carried out in the Project, the UK courts being public sector bodies, are subject to human rights laws and will consider whether they apply to the case. If the data processing will potentially affect individuals' right to a 'private life', e.g. if the Project involves some form of monitoring of individuals, the courts may well consider human rights laws in this context.

Version Control

This information will be updated annually.

Document:	Department:	Approved By:
Global DPIA Guidance	Risk & Compliance	General Counsel
Effective Date:	**Last Review Date:**	**Reviewed By:**
25/07/2019	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