

**GDPR TEMPLATE:**

**EMPLOYEE DATA PROTECTION IMPACT ASSESSMENT**

**Points to note**

* Before using this template Employee Data Protection Impact Assessment (DPIA), it is essential that you read these ‘Points to note’, together with the separate document, ‘Make UK Essential GDPR Templates for HR – Points to note’, which provides important information applicable to all of the template documents, including the DPIA.
* To comply with data protection law in respect of the personal data of Employees (as defined in the body of the document), you must conduct a DPIA before beginning data processing in certain circumstances if that processing is likely to result in a high risk to the rights and freedoms of the data subject. The UK GDPR specifically identifies some examples of situations in which a DPIA will be required – namely, where you:
  + systematically or extensively use automated techniques such as profiling which produce legal effects for individuals or similarly significantly affect them (e.g. a recruitment aptitude test which uses pre-programmed algorithms and criteria to determine which candidates pass to the next stage of the process);
  + process special category personal data on a large scale; or
  + conduct systematic monitoring of publicly accessible areas on a large scale (e.g. if a you were proposing to install CCTV to monitor your premises – including the reception area and visitors’ car park – for security purposes).
* Note that, for ease of reference, this DPIA includes criminal convictions/offences data within the definition of special category personal data (see Appendix); even though this is not technically special category data under the UK GDPR, the DPA 2018 applies similar restrictions to its processing and the circumstances in which a DPIA will be required for processing criminal convictions/offences data are similar to those where a DPIA will be required for processing special category data.
* In addition to the situations identified in the UK GDPR, the Information Commissioner’s Office (ICO) has published a list of ten additional circumstances in which a DPIA is required. These are reproduced in the Appendix to the template DPIA for ease of reference. However, both the UK GDPR list and the ICO list are non-exhaustive so a DPIA may well be necessary even if the processing falls outside one of these categories.
* This template DPIA begins with a series of screening questions to help you decide whether you are legally required to conduct a DPIA in respect of a particular project/processing operation. The benchmark we have suggested is that you should conduct a DPIA if you answer “yes” to two or more of the screening questions. However, even if you answer “yes” to fewer than two of the screening questions, we advise you to consider the situation in the round and apply your mind to the question of whether the proposed processing is likely to result in a high risk to the rights and freedoms of data subjects, such that you should conduct a DPIA. The guidance we have included in the template DPIA then advises that, even if you take the view that the proposed processing does not, or is unlikely to, result in a high risk to the rights and freedoms of data subjects, you should nonetheless consider whether it would be beneficial to conduct a DPIA. It refers to the fact that European and ICO guidance on data protection law consider employees to be ‘vulnerable’ data subjects in view of the imbalance of power in the employment relationship – and this is a factor pointing towards the need to conduct a DPIA. (Although the UK has now left the EU, the ICO expressly acknowledges the continuing relevance of the European level guidance in relation to DPIAs.)
* If you are required to conduct a DPIA, this must be done before the proposed processing has begun. Even if you are not caught by the legal requirement to conduct a DPIA for a particular processing activity, it can be a helpful tool to enable you to identify, assess and address data protection risks. There too, it is best to conduct a DPIA before you begin processing, e.g. at the design stage of a new project, as this will help you to build in data protection by design and by default. This template DPIA is therefore drafted on the basis that it will be completed at that early stage, although it could also be used to assess the impact of any data processing activities on individual rights and freedoms at any time.
* The UK GDPR imposes certain minimum requirements for the content of a DPIA, and there is guidance that expands on this. The questions in this template DPIA have been drafted to ensure that these points are covered and to focus your attention on key data protection issues, such as the security of the processing, whether the processing involves any external disclosure of Employees’ data and the need to ensure Employees have been properly informed about how you will be processing their data. This necessarily means that the questions are quite detailed. However, if there is a question that simply does not apply to the particular project you are considering, it is fine to enter “N/A” in the answer box.
* One of the requirements imposed by the UK GDPR is to consult with data subjects or their representatives about the processing “where appropriate”. Unfortunately, there is no explanation in the legislation as to when consultation will be considered appropriate. However, the ICO guidance on DPIAs recommends consulting affected individuals ‘unless there is a good reason not to’ and states that, ‘in most cases’, it should be possible to consult individuals in some form. Where you are conducting a DPIA covering the processing of existing Employees’ personal data, the ICO guidance indicates that ‘you should design a consultation process to seek the views of those particular individuals, or their representatives’. While consultation may be administratively burdensome, we recommend that you try to undertake it wherever possible, in line with the ICO guidance. In our view, consultation will be particularly important where the data processing that is envisaged will have a significant impact on Employees’ rights, e.g. if you decided to introduce a system of profiling/automated decision-making whereby Employees’ eligibility for a contractual attendance bonus would become dependent on their use of an automatic system for clocking in and out, whereas previously their eligibility was determined on the basis of sickness and holiday records only. It is also likely to be beneficial to consult where consultation would actually help you to identify or resolve any risks involved in the proposed processing. The ICO guidance acknowledges that you might decide it is not appropriate to consult individuals in a given case, but emphasises the importance of documenting your reasons for such a decision, and this is reflected in this template DPIA.
* Section 5 of the DPIA contains a table where you should identify and record privacy risks, from the perspective of the individual, assessing the likelihood and severity of the risk in each case and indicating what measures you propose to take to mitigate it. We have included detailed instructions on how to go about this, as well as an Appendix listing possible risks and suggested mitigating actions, drawn from the ICO guidance on how to conduct a DPIA.
* At the end of the DPIA is a section in which you should identify action points that have come out of your assessment and assign responsibility for them to specific individuals involved in the data processing project. There is space to record deadline dates and confirm once actions have been taken. This is part of the principle of data protection by design and default – data protection should be built into your processing operations and completing a DPIA at the start of a project should not be a “tick box” exercise to be forgotten about as soon as the questionnaire has been completed. Rather, you should come back to the DPIA responses as you work to implement a project to check that no new or increased risks have arisen and that any actions to mitigate risk have been taken.
* Note that, while it may seem like an administrative hassle, a DPIA can be a very helpful means of enabling you to identify, assess and address any risks that may arise from your proposed data processing activities. Where you decide not to conduct a DPIA, you will still have to keep a record of that decision and your reasons for it.
* This template DPIA makes reference to the possibility of publishing a completed DPIA, either in full or in summary/redacted form. The ICO guidance notes that it is good practice to publish DPIAs as a means of assisting transparency and accountability and helping to foster trust in your data processing activities. The guidance acknowledges that DPIAs may contain confidential commercial or otherwise sensitive information and suggests either redacting such details, or publishing the DPIA in summary form. For an Employee DPIA, one practical method of publication is likely to be via the company intranet.

**Employee Data Protection Impact Assessment**

To comply with the UK GDPR, you must conduct a DPIA where the processing of personal data is likely to result in a high risk to the rights and freedoms of data subjects. If you are required to conduct a DPIA under the UK GDPR, this must be done before such processing has begun. Even if you are not caught by the legal requirement to conduct a DPIA for a particular processing activity, it can be a helpful tool to enable you to identify, assess and address data protection risks. There too, it is best to conduct a DPIA before you begin processing, e.g. at the design stage of a new project, as this will help you to build in data protection by design and default.

This Employee DPIA assumes that your organisation is at the outset of a new project which involves the processing of personal data belonging to employees, workers, [contractors, agency workers, consultants, interns, volunteers, partners and directors], together referred to as ‘Employees’. Note that the term ‘project’ does not necessarily imply a major initiative; it can include any type of activity that involves the processing of personal data.

If the project involves processing of personal data by a third party data processor, they should provide any relevant information to assist you to complete the DPIA.

See Appendix for definitions of key terms used in this document.

**Project outline and DPIA screening questions**

|  |
| --- |
| *Explain what the project involves and who the key parties are. Describe the project aims, including the benefits to the company, to individuals and to other parties. Provide links to any relevant documents related to the project, e.g. a project proposal, any existing policies to which the project is subject. Identify whether any similar projects have been done previously and, if so, whether a DPIA was conducted for those projects.* |
|  |

The UK GDPR identifies three situations in which a DPIA is mandatory, and the ICO has produced a list of ten more. These are reproduced in the Appendix, for your reference.

In circumstances that do not fall within either of these lists, assessing your project outline against the following screening questions should help you to identify whether or not the processing of personal data involved in your proposed project is likely to result in a high risk to individual rights and freedoms – and thus whether a DPIA will be necessary.

|  |  |  |
| --- | --- | --- |
| **Question** | **Yes** | **No** |
| Will the project involve the collection of new personal data? |  |  |
| Will the project compel individuals to provide personal data about themselves? |  |  |
| Will you be using personal data that you already hold for a purpose it is not currently used for, or in a way it is not currently used? |  |  |
| Will personal data be disclosed to organisations or people who have not previously had routine access to the information? |  |  |
| Does the project involve you using new technology which might be perceived as being privacy intrusive e.g. biometrics or facial recognition? |  |  |
| Is the personal data that will be processed likely to raise privacy concerns or expectations e.g. special category data such as health data or criminal records data, or other information that people would consider particularly private? |  |  |
| Will the project result in you evaluating or scoring individuals, making decisions or taking action against them in ways which can have a significant impact on them? |  |  |
| Does the project involve the systematic monitoring of individuals? |  |  |
| Will you be processing the personal data of large numbers of individuals? |  |  |
| Will the processing prevent individuals from exercising a right, or using a service or contract? |  |  |

If you answer “yes” to two or more of the above questions, this indicates that you should conduct a DPIA in respect of the proposed processing – see next section.

If you answer “yes” to fewer than two of the screening questions, you must still consider the situation in the round and apply your mind to the question of whether the proposed processing is likely to result in a high risk to the rights and freedoms of data subjects, such that you should conduct a DPIA.

Even if you take the view that the proposed processing does not or is *unlikely* to result in a high risk to the rights and freedoms of data subjects, you should nonetheless consider whether it would be beneficial to conduct a DPIA. When doing so, you must bear in mind that both European and ICO guidance on data protection law consider employees to be ‘vulnerable’ data subjects in view of the imbalance of power in the employment relationship. In addition, the ICO guidance on artificial intelligence (‘AI’) flags that the vast majority of uses of AI will involve a type of processing that is likely to result in a high risk to individuals’ rights and freedoms, thus triggering the legal requirement to conduct a DPIA, and its guidance on monitoring employees strongly recommends carrying out a DPIA before you begin any such monitoring, even if there is no specific high risk. Remember also that a DPIA can be a very helpful means of enabling you to identify, assess and address any risks that may arise from your proposed data processing activities.

If you decide *not to conduct a DPIA*, you must document this decision and your reasons for it in the box below.

***Reasons for not conducting DPIA:***

**DPIA Questions**

1. **Personal data to be processed, purposes of processing**

|  |
| --- |
| *Identify the individuals or types of individuals to whom the personal data relates and the nature of your relationship with them (NB – if individuals are located outside the UK, seek legal advice about any additional local data protection law requirements.)* |
|  |
| *List the categories of personal data (e.g. names, dates of birth, etc.) and the reason why each category of personal data must be processed for this project* |
|  |
| *Specify whether the project involves the processing of special category personal data or other information that people would consider particularly private. If so, specify what types of data and the reason why they must be processed for this project* |
|  |
| *Data minimisation – are all categories of personal data listed above really necessary for this project or are there some that you could exclude?* |
|  |
| *Consider the necessity and proportionality of the processing in relation to the purposes described above, i.e. is there a practicable way to achieve those purposes that involves processing less personal data?* |
|  |

1. **Information flows and prior experience**

|  |
| --- |
| *Describe the collection, use and deletion of personal data – including any creation, access and sharing that will be involved for each data processing activity in the project. It may be useful to include a flow diagram or other way of explaining data flows. Include information about the volume of data involved, and/or the number of individuals likely to be affected by the project, as well as the extent, frequency and duration of the processing, and the geographical area covered by it.* |
|  |
| *Have you conducted processing of a similar nature in the past? If so, are there any lessons to be learnt e.g. in relation to data security? Have there been relevant technological advances since then? Are there any current security concerns in relation to the systems you are proposing to use in this project?* |
|  |

1. **Compliance considerations**

|  |
| --- |
| *For each category of personal data identified at (1) above, specify the legal grounds for processing. For special category data, you must specify both an ordinary legal ground and a special category legal ground. (Refer to the Appendix for a list of the ordinary and special category legal grounds that are most commonly applicable when processing personal data in the employment context).* |
|  |
| *It is important that individuals whose personal data will be processed as part of the project are informed as to what is happening with their data. Is this covered by existing privacy notices already provided to the affected individuals or is a new or revised privacy notice needed?* |
|  |
| *Does the project involve the use of existing personal data for new purposes? If yes, is the new purpose compatible with the original purpose for which the personal data was collected (consider, for example: – any link between the new and old purpose; context of data collection and relationship between the parties; nature of the data – ordinary/special category data; consequences of processing/impact on individual; safeguards in place)?* |
|  |
| *Are you able to amend the personal data when necessary to ensure it is up to date, or ensure that individuals update their own information? To what extent will individuals retain access to and/or control of their personal data in the context of the project?* |
|  |
| *What are the retention periods for the personal data and how will these be implemented, i.e. how will data be deleted? (If the retention periods differ between the various categories of personal data to be processed as part of the project, provide details of each period).* |
|  |
| *Are there any exceptional circumstances for retaining certain data for longer than the retention period set out above and how will you identify whether these apply in individual cases?* |
|  |
| *How will you action requests from individuals (or someone acting on their behalf) to exercise their individual rights, e.g. Subject Access Request, right to be forgotten, objection to processing, etc.? Does the project structure/design enable you to access personal data quickly and easily so that you can respond to such requests in a timely manner and, where relevant, within the one month deadline?* |
|  |
| *How will you ensure that all staff with access to the personal data have adequate training on data protection compliance requirements?* |
|  |
| *Will any new or updated policies or procedures be required to implement the project?* |
|  |
| *What security measures are built into the project structure/design?* |
|  |
| *Will personal data be disclosed internally or externally and, if so, to whom, how and why?* |
|  |
| *If personal data will be disclosed to a third party, are they a processor? If so, have you put in place an appropriate contract to ensure GDPR compliance? If the third party is a controller, have you put in place an appropriate data sharing agreement?* |
|  |
| *Will personal data be transferred to a country outside the UK? If yes, what arrangements will be put in place to ensure compliance with the rules on overseas transfers?* |
|  |

1. **Consultation**

|  |
| --- |
| *If your organisation has a Data Protection Officer (DPO), have you sought their advice on this project? If your organisation does not have a DPO, have you discussed the project with the [HR Data Protection Lead/Data Protection Team]? Summarise any advice given.* |
|  |
| *Is there anyone else within the organisation who should be involved in this DPIA (e.g. IT, legal, etc.)? If so, ensure that you integrate their input into your responses across this form, and summarise any additional comments they have here.* |
|  |
| *The UK GDPR requires you to consult affected data subjects (or their representatives) about the project “where appropriate”. ICO guidance recommends consulting individuals “unless there is a good reason not to” and states that consultation in some form should be possible “in most cases”.*  *Have you consulted and, if so, with whom (e.g. individual data subjects/employee representatives/recognised trade union)?* |
|  |
| *If you have decided not to consult affected data subjects/their representatives about the project, you must document your reasons for this decision.* |
|  |
| *If you have consulted affected data subjects/their representatives, what was their view on the project? If the consultees oppose the project and you plan to go ahead anyway, you must document your reasons for this decision.* |
|  |

1. **Identification of privacy risks and solutions**

*Based on your answers to the questions in the above sections, identify and record privacy risks (from the perspective of the individual) in the table below. See the Appendix for examples of possible risks you should consider. You should assess the level of risk to the individual (both in terms of likelihood and severity) as “high”, “medium”, or “low”. This assessment of risk level may influence what is required to address it, e.g. if a risk’s severity is assessed as “high”, you should be taking action to address it even if its likelihood is “low”. By contrast, a risk whose severity and likelihood are both assessed as “low” and for which there is no readily available solution might ultimately be considered acceptable, i.e. the impact on individuals may still be justified and proportionate notwithstanding that residual risk.*

*Remember that risks will differ depending on the nature of the personal data concerned – e.g. a security breach in respect of business contact data will not give rise to the same individual risk as a security breach in respect of bank account details or health data. The nature of the risk will also affect what solution will be appropriate to address it.*

*Describe the actions you could take to reduce the risks, and any necessary future steps. See the Appendix for examples of possible mitigating actions to consider. Evaluate how effective these actions are likely to be and determine whether any remaining impact on individuals is justified and proportionate in view of the aims of the project.*

*Note that if there would be a residual* ***high*** *risk to individual rights and freedoms even after solutions are put in place, you must consult with the ICO before going ahead with the project. Details of any such consultation should be entered into the table at 6 below.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Privacy issue:** identify potential risk | **Risk to individual:** include consideration of likelihood of risk occurring and severity of potential impact on the individual | **Compliance risk:** identify GDPR requirement that may be breached | **Other risk: e.g.** enforcement action, reputational damage, etc. | **Mitigating actions:** identify how you plan to remove/ reduce risk and indicate whether each proposed action is accepted or rejected | **Result and evaluation:** is risk eliminated, reduced or accepted? Is final impact on individuals after implementing mitigating action GDPR-compliant, justified and proportionate to the aims of the project? |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. **Consultation with ICO – only if residual high risk**

|  |
| --- |
| *Set out details of information provided to the ICO, advice received, and actions taken based on that advice.* |
|  |

1. **Integration of outcomes into project plan**

*Who is responsible for implementing the solutions that have been approved?*

|  |  |  |  |
| --- | --- | --- | --- |
| **Action** | **Person responsible** | **Date for completion** | **Completed?** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. **Sign-off**

*(To be completed by the person with overall responsibility for the project once DPIA solutions have been implemented)*

|  |  |  |
| --- | --- | --- |
| **Name** | **Position** | **Date** |
|  |  |  |

1. **Publication**

|  |
| --- |
| *Confirm whether you will publish the DPIA* ***(a)*** *in full;* ***(b)*** *in summary/redacted form; or* ***(c)*** *not at all. If (c), note your reasons.* |
|  |

1. **Date for review**

*DPIAs should be reviewed periodically and may need to be repeated if the nature, scope, context or purposes of the processing changes.*

**Review date: ………………………………….**

**APPENDIX**

This Appendix contains: key definitions of data protection law terminology; the UK GDPR and ICO lists of circumstances in which a DPIA is required; a summary of possible legal grounds for processing personal data; and lists of potential risks and mitigating actions to consider.

**Key definitions**

|  |  |
| --- | --- |
| **Controller** | the body which, alone or jointly with others, determines the purposes and means of the processing of personal data. (As an employer, you will be a controller in respect of your employees’ personal data) |
|  |  |
| **Processor** | a body which processes personal data on behalf of the controller. (An organisation that processes personal data only on your instructions, such as a payroll provider, will be a processor) |
|  |  |
| **Data subject** | an identified or identifiable natural person (i.e. the individual to whom personal data relates) |
|  |  |
| **Personal data** | information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, 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 |
|  |  |
| **Processing** | any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction |
|  |  |
| **Special category data** | any personal data about an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sex life or sexual orientation, criminal convictions or offences, biometrics (if used for identification purposes), or genetics. |

**UK GDPR list of circumstances requiring a DPIA**

Under the UK GDPR, you must conduct a DPIA where you are proposing to:

* systematically or extensively use automated techniques, such as profiling, which produce legal effects for individuals or similarly significantly affect them (e.g. a recruitment aptitude test which uses pre-programmed algorithms and criteria to determine which candidates pass to the next stage of the process);
* process special category personal data on a large scale; or
* conduct systematic monitoring of publicly accessible areas on a large scale(e.g. if a you were proposing to install CCTV to monitor your premises – including the reception area and visitors’ car park – for security purposes).

**ICO list of circumstances requiring a DPIA**

In addition, the ICO requires you to conduct a DPIA where your proposed processing of personal data involves any of the following:

* **Innovative technology:** processing involving the use of new technologies, or the novel application of existing technologies (including AI) and any of the additional risk criteria listed below apply.
* **Denial of service:** decisions about an individual’s access to a product, service, opportunity or benefit which are based to any extent on automated decision-making (including profiling) or involve the processing of special category data.
* **Large-scale profiling:** any profiling of individuals on a large scale.
* **Biometric data:** any processing of biometric data for the purpose of uniquely identifying an individual, where any of the additional risk criteria listed below apply.
* **Genetic data:** any processing of genetic data where any of the additional risk criteria listed below apply, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject.
* **Data matching:** combining, comparing or matching personal data obtained from multiple sources.
* **Invisible processing:** processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that provision of a privacy notice to the data subject would prove impossible or involve disproportionate effort, and any of the additional risk criteria listed below apply.
* **Tracking:** processing which involves tracking an individual’s geolocation or behaviour, including but not limited to the online environment, and any of the additional risk criteria listed below apply.
* **Targeting of children or other vulnerable individuals:** the use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.
* **Risk of physical harm:** where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.

The additional risk criteria referred to in the list above are:

* evaluation or scoring;
* automated decision-making with legal or similar significant effect;
* systematic monitoring;
* sensitive data or data of a highly personal nature;
* data processed on a large scale;
* matching or combining datasets;
* data concerning vulnerable data subjects;
* innovative use or applying new technological or organisational solutions; and
* preventing data subjects from exercising a right or using a service or contract.

Note that the above lists are not exhaustive and a DPIA may well be required in respect of processing that does not fall into the above categories. See the screening questions at the start of this template DPIA for assistance in determining whether a DPIA is necessary for your proposed data processing activity.

**Summary of possible legal grounds for processing Employees’ personal data**

**Legal grounds for processing ordinary personal data** *(to be lawful, processing must fall within at least one of these legal grounds)*:

* Necessary for performance of legal obligation to which you are subject (**BUT** not a contractual obligation).
* Necessary for the performance of the individual’s employment contract or to take steps to enter into contract at individual’s request (e.g. processing job applications).
* Necessary for legitimate business interests – yours, or those of a third party to whom you disclose the personal data – **EXCEPT** where those interests are overridden by interests or fundamental rights and freedoms of individual.
* Individual has consented for specified purpose(s) **BUT** UK GDPR/ICO GUIDANCE SAY DO NOT USE IN THE EMPLOYMENT CONTEXT.
* Necessary to protect the vital interests of the individual or another person (generally only appropriate in exceptional ‘life or death’ situations).

**Legal grounds for processing special category personal data** *(to be lawful, processing must meet one of the legal grounds from the ‘ordinary’ list above,* ***and*** *one from the ‘special category’ list below)*:

* Necessary to exercise/perform legal right/obligation connected with employment (**NOT** for contractual rights/obligations; and **NB** need to include additional information in the [Data Protection Policy, Employee Data Retention Process and Employee Record of Processing]).
* Necessary for purposes of establishing, exercising or defending legal claims.
* Information has manifestly been made public by the individual.
* Individual has given explicit consent for specified purpose(s) **BUT** GDPR/ICO GUIDANCE SAY DO NOT USE IN THE EMPLOYMENT CONTEXT.
* Necessary for reasons of substantial public interest, as defined in national law (this permits equal opportunities monitoring in accordance with the DPA 2018).
* Necessary to protect individual’s/someone else’s vital interests and individual cannot consent (generally only appropriate in exceptional ‘life or death’ situations).

Note that the ICO guidance on those of the legal grounds for processing special category personal data that refer to the processing being ‘necessary’ for a particular purpose emphasises the importance of being able to demonstrate such necessity. The guidance states that this does not mean that the processing has to be absolutely essential. However, it must be more than just useful or habitual. It must be a targeted and proportionate way of achieving your purpose and – if you can reasonably achieve your purpose by less intrusive means, in particular if you can do so without using special category data – then the requirements of the special category legal grounds that are based on necessity will not be met.

**Lists of potential risks and mitigating actions to consider**

This section of the Appendix sets out **non-exhaustive** lists of:

* potential risks that may arise from the processing of personal data; and
* actions you could consider taking in order to mitigate such risks.

These lists are drawn from the ICO’s guidance on DPIAs, which is available online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/>. They are intended to help you focus your mind when completing section 5 of the DPIA.

However, the lists are not exhaustive and your project may give rise to risks that are not identified here, and/or there may be further mitigating actions you could take to remove or reduce the risks that arise from your project. You must therefore take care to consider the situation in the round so as to identify and address all potential risks and mitigating actions.

Potential risks

* inability to exercise rights (including but not limited to privacy rights)
* inability to access services or opportunities
* loss of control over the use of personal data
* discrimination
* identity theft or fraud
* financial loss
* reputational damage
* physical harm
* loss of confidentiality
* re-identification of pseudonymised data
* any other significant economic or social disadvantage

Mitigating actions

* deciding not to collect certain types of data
* reducing the scope of the processing
* reducing retention periods
* taking additional technological security measures (e.g. password protection, encryption, data partitioning, etc.)
* training staff to ensure risks are anticipated and managed
* anonymising or pseudonymising data where possible
* writing internal guidance or processes to avoid risks
* using a different technology
* putting clear data sharing agreements into place if any data is to be disclosed to third parties
* making changes to privacy notices
* offering individuals the chance to opt out where appropriate
* implementing new systems to help individuals to exercise their rights