

Data Protection Impact Assessment (DPIA) Guidance

Data Protection Impact Assessment (DPIA) Guidance

1 Introduction / Objective

The objective of the document is to provide guidance regarding best practice for establishing when and how to conduct a Data Protection Impact Assessment (DPIA).

It will be maintained and updated sporadically to reflect feedback and appropriate changes in legislation, reflect any enhancements or developments in guidance and to supplement information available from the Information Commissioners Office.

As stated below, it is not legal advice and is aimed to supplement (not replace) other guidance available.

This guidance does not constitute legal advice: individual companies should seek their own and, when using this guidance, AOP member companies will need to take into consideration other relevant laws.

2 WHAT is a DPIA: Overview

2.1 What is a DPIA?

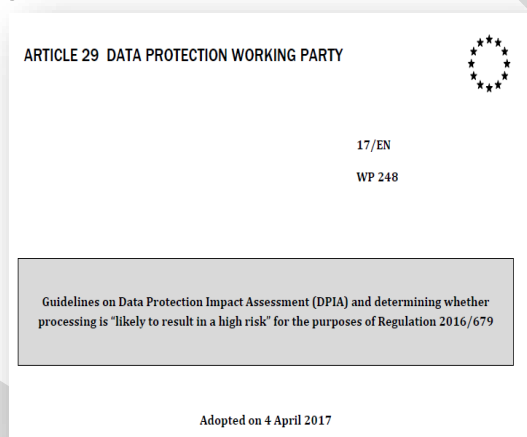
The Data Controller is **Accountable** i.e. bears responsibility for compliance with all the GDPR principles relating to processing of personal data and must be able to demonstrate this.

The Data Controller is defined as the entity that determines the purposes and means of the processing of personal data, alone or jointly with others.

The DPIA is a process aimed at providing assurance that Data Controllers adequately address privacy and data protection risks of 'risky' processing operations, such as those with high, medium, and low risk.

 **Best Practice Tip** A key element of GDPR is the ability of Data Controllers to be able to demonstrate accountability. Integrating the guidance available into your existing development processes will ensure constituency of approach and can provide the capability of documenting any decisions and actions taken.

DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation. In other words, a DPIA is a process for building and demonstrating compliance.



[EDPB Guidelines on Data Protection Impact Assessment \(DPIA\) \(wp248rev.01\) \[Accessed 16-01-20\]](#)

By providing a structured way of thinking about the risks to data subjects and how to mitigate them, DPIAs help organisations to comply with the requirement of 'data protection by design' where it is needed the most, i.e. for 'risky' processing operations.

Question	Response
1. Does the GDPR impose or prescribe a specific DPIA methodology on Data Controllers?	No, Data Controllers are free to use any methodology – However it needs to comply with the Regulation's requirements and the WP29's guidelines on DPIA interpreting the equivalent provisions of the GDPR. (see section 4)

As a result of a DPIA, various documents may be produced **BUT** the objective of the DPIA should not only be a form filing/completion exercise!



Best Practice Tip
Establish a defined process to meet the requirements of a DPIA that fits in with your business's technical build and maintenance procedures

2.2 When is a DPIA Needed?

When processing personal data is likely to result in a high risk to the rights and freedoms of natural persons - 'risky' processing operations!

Article 35 of the GDPR covers Data Protection Impact Assessments and states (emphasis added)

*"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, **is likely to result in a high risk to the rights and freedoms of natural persons**, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data".*

The appropriateness of a new DPIA or a review of an existing DPIA should be considered whenever:

- You are planning to develop a new project, process or activity that involves the more extensive GDPR definition of personal data
- There is a change / alteration that may have an impact upon existing processing activity, such as:
 - Change to a component of the processing such as change of technology supplier
 - Change to the wider environment e.g. legal



Best Practice Tip
It is sensible to set review dates for DPIA's e.g. annually so that internal and external changes in the general operating environment can be reviewed

Question	Response
2. Do we have to conduct a DPIA for all processing operations?	No, only those that are likely to pose a 'high risk to the rights and freedom of data subjects'
3. What is the threshold for determining 'risky' – high risk processing?	There is guidance to determine this, provided • Directly in the GDPR text – Article 35 para3 • By the European Data Protection Board (the band formerly known as The Article 29 Working party) • By local national regulators (UK – The ICO) But ultimately, it is the Data Controller who is accountable for determining: 1. Whether a DPIA is required 2. How the DPIA is carried out and any resulting actions taken to mitigate risk to a 'suitable' level



Best Practice Tip
As a Data Controller, you should maintain an Article 30 Record of Processing Activity (ROPA) Register. This provides a summary of the processing under the control of the Data Controller.

This requires a certain level of detail that will provide an overview of the higher risk activity.

Include a column that records if a DPIA is needed and / or the dates a DPIA was completed and when it should be reviewed.

2.3 Why is a DPIA needed?

DPIAs help organisations to comply with the requirement of ‘data protection by design’ where it is needed the most, i.e. for ‘risky’ processing operations.

- Stage 1: focuses upon helping Data Controllers identify what is classed a ‘risky’ operation.
- Stage 2 (if required): A full DPIA provides a structured way of thinking about the risks to data subjects, options on how to mitigate them, and documents actions proposed or taken by the Data Controller to reduce the risks identified.

 **Best Practice Tip** You should conduct a **Threshold Assessment test** to determine if you should carry out a full DPIA (i.e. Stage 2).

2.4 What is a Threshold Assessment Test?

Article 39 of the GDPR text states

‘(1) Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

[...]

(3) A data protection impact assessment referred to in paragraph 1 shall **in particular** be required in the case of:

- (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- (b) processing on a large scale of special categories of data referred to in Article 10, or of personal data relating to criminal convictions and offences referred to in Article 11; or
- (c) a systematic monitoring of a publicly accessible area on a large scale.’

- However, this list is **non-exhaustive**, as indicated by the use of ‘in particular’.
- The European Data Protection Board and national Data protection Authorities also provide guidance of criteria to consider for determining if processing falls with the “likely to result in a high risk” category
 - [European Data Protection Board Guidance \(wp248 page 7-9\)](#)
 - ICO List : [What does the ICO consider likely to result in high risk?](#)

Ultimately, the Data Controller is responsible for determining the requirement for and the extent of any DPIA activity.

The ICO would always recommend that if in any doubt, you do a DPIA to ensure compliance and encourage best practice.

Question	Response
4. How do we identify whether a DPIA is needed?	The responsibility for conducting a DPIA is the responsibility of the Data Controller but to aid this decision you can use the AOP DPIA pre-qualifier Google sheet as a template available at https://docs.google.com/spreadsheets/d/1cIyX1CEs8sSqWu9IYrXLLuwJIK-OcQtoNgcS32bPceU/template/preview [*Save by clicking on the USE TEMPLATE option.]



Best Practice Tip

- Rather than question “is a DPIA needed?”, instead, **assume a DPIA is needed** unless a Threshold Assessment Test has been conducted and found that a DPIA is not required.
- Your DPIA process documentation should include a simple validation tool to confirm whether you need to proceed to stage 2 using the GDPR text and the guidance from the EDPB and local Data Protection Authority.
- Ensure you document the decision and the rationale behind the decision!

2.5 Who should be involved in the DPIA process?

A DPIA is a process that may / should involve various stakeholders. Depending on the processing operations being considered, you may need to involve other teams, such as your company’s legal unit / service, suppliers etc.

A RACI matrix can provide a summary of the different roles appropriate to a DPIA

Role	Details	Who
‘Responsible’	Having the obligation to act and take decisions to achieve required outcomes i.e. determining whether a DPIA is required, and if so, conducting it effectively	Business unit manager or process owner who is instigating the activity that requires personal data to be processed
‘Accountable’	Be answerable for actions, decisions and performance with regard to GDPR compliance	The Data Controller (the business) is in charge of ensuring compliance and being able to demonstrate the measures decided upon to provide compliance.
‘Consulted’	Being asked to contribute and provide information & comments	• Data Protection Officer *(recommended) • IT Department. • Legal support • Procurement • 3rd party suppliers – joint controllers / data processors. • External parties e.g. data subjects & regulators e.g. ICO** (in specific circumstances)
‘Informed’	Being kept informed of decisions made and the process	

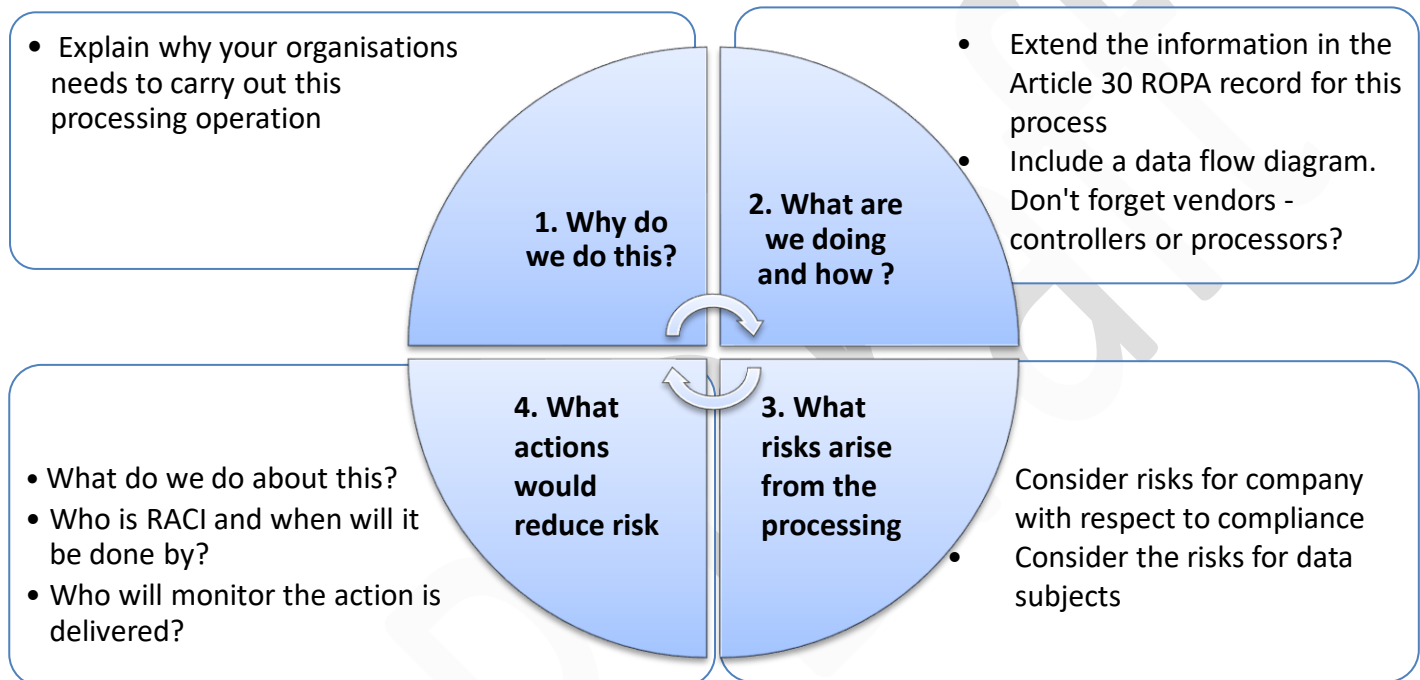
Question	Response
5. Can’t the DPO do this for me?	No - Under Article 39 of GDPR, DPOs have specific tasks regarding DPIAs. The DPO can and should provide advice on: • whether you need to do a DPIA; • how you should do a DPIA; • whether to outsource the DPIA or do it in-house; • what measures and safeguards you can take to mitigate risks; • whether you’ve done the DPIA correctly; and • the outcome of the DPIA and whether the processing can go ahead You must ensure that any responsibilities you give a DPO for your DPIA do not conflict with their requirement under Recital 97 to complete these tasks in an independent manner.

3 HOW to Conduct a DPIA

DPIAs are a **cyclical process**, not a one-off exercise.

- If you are starting a new project / process you start with a description of your processing.
- If the process already exists, you may already have DPIA documentation in place.

The overall process is highlighted in the diagram below



The steps in the process is described in greater detail in the subsections

1. [Describe the processing – FULLY](#)
2. [Conduct Risk Assessment](#)
3. [Identify Mitigating Options – Risk treatments](#)
4. [Agree Action Plan, Monitor and Review](#)

 **Best Practice Tip** To ensure accountability, it is sensible to document the decision points taken within a DPIA's to demonstrate the activity has been undertaken.
This is also to assist anyone who may review the process at a later date.

The output of the DPIA process should be

- 1) A list of risks identified resulting from the proposed processing and an evaluation of the impact and probability of those risk being realised
- 2) Various potential mitigating options to reduce the risks identified
- 3) A plan of agreed defined actions that will reduce the level of risk to acceptable to the Data Controller.

Conducting the Risk Assessment - Describe the processing FULLY

Establishing the context and describing processing operations is the foundation of a solid DPIA process.

In short, you have to describe what you plan to and how you plan to do it.

To create this systematic description of the process, start from the information you already have in your Article 30 record and add the following points:

- Detailed description of the purpose(s) of the processing: explain the process step-by-step and distinguish between different purposes of elements of the processing where necessary
- Data flow diagram of the process (flowchart): what do we collect from where / whom, what do we do with, where do we keep it, who do we disclose it to?
- Description of the supporting infrastructure: filing systems, IT hardware and software, third party suppliers etc
- Description of its interactions with other processes: does this process rely on personal data being fed in from other systems? Are personal data from this process re-used in other processes?

This documentation should allow the reader to quickly understand the scope of the activity.

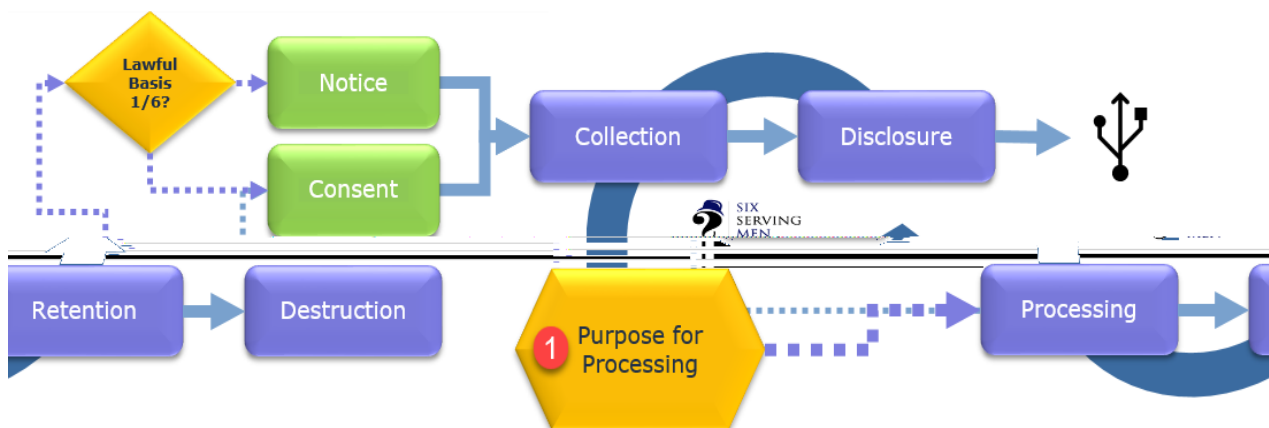


Best Practice Tip

Being specific regarding the purpose of the processing is a key element of the DPIA.

Be careful not to lump processing activities into generic headings e.g. Behavioural Targeting. Each organisation (Data Controller) will implement technical solutions in different configurations.

Establish and confirm the Purpose for Processing



 *"In order to determine whether data processing complies with the law, and to establish what data protection safeguards should be applied, it is a necessary precondition to identify the specific purpose(s) for which the collection of personal data is required. Purpose specification thus sets limits on the purposes for which controllers may use the personal data collected, and also helps establish the necessary data protection safeguards. Purpose specification requires an internal assessment carried out by the data controller and is a necessary condition for accountability.*

[Article29 WP opinion on purpose limitation Page 12 \(wp203\) \[Accessed 16-01-20\]](#)

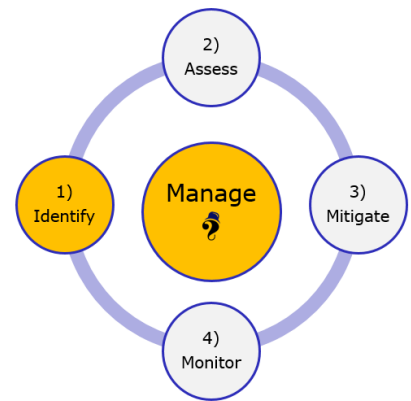
3.1 Risk Assessment – Identify the Threats associated with the Processing

As a Data Controller, you determine of the "purposes" of the processing and the "means" to achieve them i.e. determining respectively the "why" and the "how" of the actual processing activities.

A principle component of the Risk Assessment is to provide suitable protection against risks associated with the processing.

The risks to the rights and freedoms of individuals of “varying likelihood and severity” may result from personal data processing which could lead to “physical, material or non-material damage”

(GDPR Recital 75).



The Risk Assessment is focussed upon confirming that the “means” chosen does not expose the data subject to excessive threat levels regarding their Rights and Freedoms.

It is important to understand that “means” does not only refer to the technical ways of processing personal data, but extends to the “how” of processing, including questions such as:

- “which data shall be processed”,
- “which third parties shall have access to this data”,
- “when data shall be deleted”, etc.

The initial activity focusses upon identifying threats posed so that the potential likelihood and severity of the threat being realised can be considered.



Best Practice Tips

- It is important that the analysis is looked at from the perspective of the data subjects whose personal data is being processed NOT from the company perspective

3.1.1 Areas of consideration to identify Potential Threats to Data Subjects.

To help identify and understand associated risks a **NON-EXHAUSTIVE** list of “threats and associated damage” is provided in GDPR Recital 75 & Article 32.

The below can act as a prompt in the risk assessment to flush out potential threats or specific areas to focus upon:

Might the processing impact the data subject by giving rise to: • discrimination, identity theft or fraud, financial loss • damage to the reputation • loss of confidentiality of personal data protected by professional secrecy • unauthorised reversal of pseudonymisation • any other significant economic or social disadvantage	Might the processing result in the data subjects being: • deprived of their rights and freedoms • or prevented from exercising control over their personal data
Might the processing of personal data reveal: • racial or ethnic origin • political opinions • religion or philosophical beliefs • trade union membership • and the processing of genetic data, data concerning health or data concerning sex life or	Does the activity involve profiling i.e. personal aspects are evaluated, to create or use personal profiles, in particular for analysing or predicting aspects about: • performance at work • economic situation • health

criminal convictions and offences or related security measures	- personal preferences or interests - reliability or behaviour - location or movements, in order to create or use personal profiles
Does the processing of personal data involve: - vulnerable persons, children in particular - a large amount of personal data, affecting a large number of data subjects	Are the technical and organisational measures appropriate so as to not lead to: accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise of the data processed

3.1.2 Review the Proposed activity against compliance with the GDPR principles

Alternatively, the proposed processing can be evaluated against the principles of GDPR laid out in Article 6.

The following questions act as prompts that will help highlight the threat of non-compliance with GDPR.

Principle	Summary	Questions for consideration to identify compliance to the principles
  'Purpose limitation'		- Have you identified all purposes of the component activities to a suitable level of granularity? - Are they all required for the overall purpose of the processing? - Have you confirmed the basis for processing of each of the purposes? - Are all the activities proposed compatible with the initial objective of the processing? - Is there a risk that the data could be reused for other purposes (function creep)? - How can you ensure that data are only used for their defined purposes? - Are third parties / suppliers used to process data acting as Data Controllers or Data Processors?
  Fairness		- Would people expect this to happen, even if they do not read the information you provide them with? - Is it easy for people to exercise their rights to access, rectification, erasure etc? - If reliant upon consent: - Is it really freely given? - How do you document that people gave it? - How can they revoke their consent? - How soon and how do you intend refreshing consent? - Could this generate restrictive effects on data subject's behaviour? - Could this lead to discrimination?
  Transparency		- How do you ensure that the information you provide reaches the data subjects (i.e the individuals) concerned? - Is the information you provide complete and easy to understand? - Is it targeted to the audience? Can you verify this i.e. have you checked / tested this? - Is the information regarding the processing provided at point of interaction / collection as well as easily findable / available to review retrospectively elsewhere? - In case you defer informing people, what is the justification for this approach? - How are data subject's rights met e.g. - Right of access (Article 15) - Right to rectify, erase, restriction of processing (Article 16 to 19)

	• Right of portability (Articles 20): CONTRACT / CONSENT • Right to object, (Article 21); LI Basis • Right NOT to be Subject to Automated profiling, (Article 22) <i>*The rights that data subjects have are dependent upon which one of the six lawful basis are chosen to process data under – Check with your DPO or legal which rights apply!</i>
  Data minimisation	• Are all the data points collected required? • Are there data points you could remove (or mask / hide) without compromising the purpose of the process? • Do you clearly distinguish between mandatory and optional items when data is collected? • In case you want to keep information for statistical purposes, how do you manage the risk of re-identification? • Is there the risk of unjustifiable or excessive collection / storage of data – quantity & retention
  Accuracy	• Is the data of sufficient quality for the purpose? • What could be the consequences for the persons affected of acting on inaccurate information in this process? • How do you ensure that the data you collect yourself are accurate? • How do you ensure that data you obtain from third parties are accurate? • Do your tools allow updating / correcting data where necessary? • Do your tools allow consistency checks?
  Storage Limitation	• For each of the specific purpose(s) and data items? • How long do you need to keep which data – is this excessive? • Can you distinguish storage periods for different parts of the data? • If you cannot delete the data just yet, how can you restrict access to it?
  Security	• What procedures do you have in place to perform an identification, analysis and evaluation of the information security risks potentially affecting personal data and all the IT systems supporting their processing? • What controls are in place to protect against use or storage of inaccurate or outdated data. • What technical and operational measures exist to prevent 'inappropriate use or misuse of data'. • Do you manage your system vulnerabilities and threats for your data and systems?
  Accountability / Governance	• Have you reviewed / considered the impact on people's fundamental rights, freedoms and interests and not only on the risks to the organisation? • Have you taken into consideration the full nature, scope, context and purposes of processing when assessing the risks? • Have staff with assigned roles, appropriate experience and had suitable time to perform the risk assessment? • Are the roles of any 3rd parties fully understood, defined and agreed? • Have all stakeholders been involved in the process?



Best Practice Tips

- The initial threat identification process is not aimed at stopping a proposed processing activity but recognising the potential threats. Once documented, options that mitigate the level of risk posed by the threat can be identified. The Data Controller then has responsibility to implement actions that will reduce the risk level to an appropriate level.

3.2 Assess Identified Risks for Likelihood and Severity

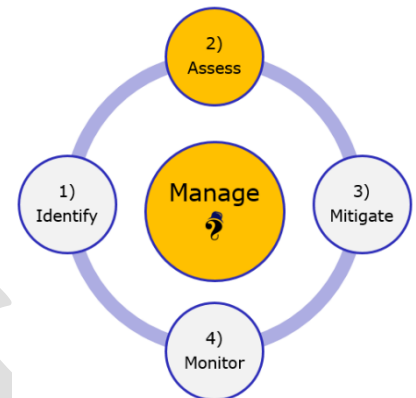
The activity in section 1 will identify a series of threats

- To the Rights and Freedoms of the data subjects
- Or faced by the Data Controller.

For each of the threats identified the Data Controller needs to assess and evaluate

- the likelihood (probability)
- and the severity (impact)

of the threat being realised to determine the associated risk level.



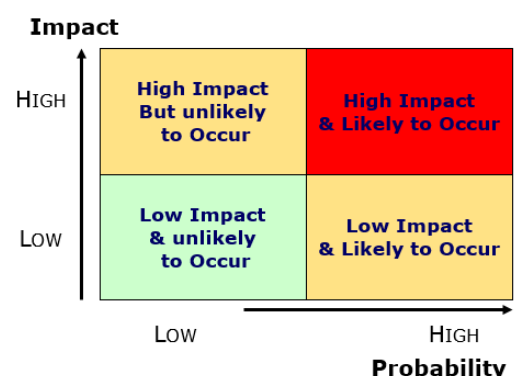
3.2.1 Quantifying the level of Risk Present

Using the two criteria of probability and impact provides a mechanism for quantifying the level of risk associated with the identified threat.

The GDPR does not prescribe the type or number of categories that impact and probability should be measured against

- The diagram uses High and Low as categories on both axes
- The ICO DPIA template uses three categories for
 - Probability i.e. Remote / Possible / Probable
 - Impact i.e. Minimal / Significant / Severe

that determines the level of Overall Risk as Low / Medium / High.





Best Practice Tip

- Each Data Controller will determine this based upon their own risk management approach.
- The objective is to be able to have a consistent method that helps quantify the level of risk. Use your company's current risk evaluation process!

3.3 Identify Options that Mitigate the Risks Impact & Probability

The output from section should be a list of the risks identified and classified according to level of risk.

For risks deemed unacceptable to the Data Controller e.g. High or Medium, measures should be now be identified that would reduce or eliminate those risks.

The options can be technical and / or organisational measures.

It is likely that the mitigating measures identified will impact upon a number of the risks identified.

The impact of the mitigating options should be applied against the identified risks to evaluate the impact.



**Best Practice Tip**

Establish a risk evaluation process and residual risk template.

The template should include columns including:

- A description of the threat identified
- Summary of the output of the risk if the threat is realised
- Initial risk evaluation (e.g. None, Low, Medium, High) based upon
 1. Evaluation of the associated impact
 2. Evaluation of the probability of the risk being realised
- Mitigating options that will reduce the level of risk
- Revised risk evaluation - based upon the mitigating options identified being implemented and their effect upon reducing
 1. The anticipated impact
 2. The anticipated probability of the risk being realised

3.4 Monitor Agree Action Plan, Monitor and Review

Stage 3 will provide:

- A list of options of technical and / or organisational measures and actions that could be implemented that would reduce the risks identified
- An indication of the effect upon the risk if the options are implemented.

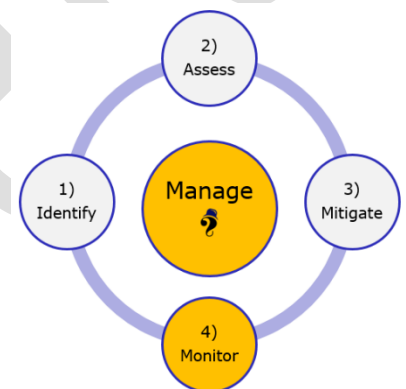
For each of the risks that the Data Controller deems unacceptable, a series of mitigating actions are required to eliminate or reduce the residual risk to a level acceptable to the Data Controller.

The treatment options for the identified risks generally fall into four areas i.e.

- Treat: Actions are required to reduce the risk to more acceptable levels
- Terminate: Stopping the activity eliminate the risk
- Transfer: The associated risks are moved to a third party
- Tolerate: The identified level of risk is deemed acceptable

The Data Controller needs to agree what mitigating actions are appropriate and implement an activity plan that will establish the mitigating measures identified.

The default (do nothing) approach would be to Tolerate the situation so it is important that suitable management controls are put in place to assess that the activity plans are not just started but completed.



Question	Response
6. If we identify a risk as high, does that mean we need to stop the processing?	No – in the first instance you would look to implement technical and / or organisational measures that will mitigate the risk identified. This could include things such as enhanced security to who can access data, greater transparency mechanisms for data subjects, shorter data retention periods etc. The purpose of the activity is to implement measures that will reduce the risk level to a level deemed acceptable to the Data Controller.
7. What if we cannot reduce the risk level to a suitable level?	Before you commence processing you need to provide a copy of your DPIA to the Information Commissioner's office. You need to send the information to the ICO via email

Once the ICO have the information they require, they aim to respond within eight weeks (although this can be extended by a further six weeks in complex cases).



Best Practice Tip

Under the GDPR accountability principle, the Data Controller needs to document and be able to justify the decisions taken.

The action plan should include who is accountable for delivering the mitigating actions and a review process to ensure they are introduced effectively.

4 WHERE to find out more?

4.1 Useful Links

In addition to this guidance, AOP member companies may find the following GDPR sources helpful:

- AOP GDPR FAQs <https://www.ukaop.org/hr-and-legal/the-eu-general-data-protection-regulation-gdpr-faqs-> [NB member log in required]
- UK Information Commissioner's Office (ICO) <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>
- Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
- EU Article 29 Working Party (group of EU regulators): Draft guidance on consent under the GDPR - https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
- EU Article 29 Working Party (group of EU regulators): Draft guidance on transparency under the GDPR https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
- IAB Consent Framework <https://iab europe.eu/> [Accessed – 16-01-20]

5 Document Information

Please treat all documents and other communications issued to AOP Members and all discussions that take place in the Group meetings as STRICTLY PRIVATE AND CONFIDENTIAL and that no disclosure will be made to any person outside the membership of the Association or be published in any journal without first obtaining the permission of the AOP.

Version Information / Control

We use version control to maintain document status – with the version status and the published year and month shown – Current Version: DRAFT - v1.0 20-01

Summary of changes from previous version – Not applicable

Queries / Further Information

The information available relating to GDPR and ePrivacy is evolving and this document reflects the situation and advice available at a point in time.

We will update it to reflect changes post publication with the next update planned for 12months hence. If you have any questions, wished to contribute towards it or have specific queries please contact the AOP via email – stef.elliott@6sm.co.uk or info@aop.uk.com