Data Protection Impact Assessments

information commissioner
Barrantagh Fysseree

Determining whether a data protection impact assessment (DPIA) is required should occur as early as practicable in the lifecycle of a project and, in all cases, prior to the commencement of processing.

If it is determined that a DPIA is required then the resources required to do so, the individuals who will need to be involved, and the timeframe for the DPIA, including referral to the Commissioner when required, should also be identified.

The risks to individuals may not be apparent at an early stage of a project; the requirement for a DPIA may, therefore, need to be reconsidered, reviewed or repeated as the project moves forward.

Step 1: Identify whether a DPIA is required.

1.1 To identify whether a DPIA is required you should first document in broad terms what:-

- the project aims to achieve
- the envisaged processing of personal data
- the impact and potential risks to individuals, and
- the outcome and perceived benefits of the processing

This can be achieved by reference to other documents, such as a project proposal.

1.2 A preliminary risk assessment can then be undertaken which should be context specific and take into account whether any processing, either on its own or combined with other factors, is likely to result in a high risk to the rights and freedoms of individuals.

1.3 A DPIA is required where a type of processing is likely to result in a high risk to the rights and freedoms of individuals. To assist in determining whether a DPIA is required, the European Data Protection Board has adopted guidelines on DPIAs and whether processing is likely to result in a high risk for the purposes of the GDPR. The full guidelines are available at: https://edpb.europa.eu/our-work-tools/our-documents/guideline/data-protection-impact-assessments-high-risk-processing_en

In summary, the following criteria are to be considered in assessing the level of risk:

1. Evaluation or scoring, including profiling and predicting, especially "from aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements" (Recitals 71 and 91).

Examples of this could include a bank that screens its customers against a credit reference database, or a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks, or a company

building behavioural or marketing profiles based on usage or navigation on its website.

2. Automated decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or which "similarly significantly affects the natural person" (Article 35 (3)(a)). Such processing with little or no effect on individuals does not match this specific criterion.

   For example, the processing may lead to the exclusion or discrimination against individuals.

3. Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through "a systematic monitoring of a publicly accessible area" (Article 35 (3)(c)). This could include, for example, CCTV, ANPR, body worn video, monitoring staff email and internet use.

   This type of monitoring is included as personal data may be obtained in circumstances where data subjects may not be aware who is collecting their data and how that data will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in public (or publically accessible) space(s).

4. Higher risk data includes special categories of data as defined in Article 9 (for example, information about individuals' political opinions), as well as personal data relating to criminal convictions or offences.

   For example, a hospital or general practitioner maintaining patients' medical records or an investigator processing an offender's details.

Higher risk data also includes data that increases the risk to the rights and freedoms of individuals, such as electronic communication data, location data, financial data (that might be used for payment fraud). In this regard, whether the data has already been made publically available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes.

Higher risk data may also include information processed by a controller on behalf of an individual for their domestic purposes.

For example cloud computing services providing personal document management, email services, diaries, e-readers equipped with note taking features, and various life-logging applications that may contain very personal

information about that individual and unauthorised disclosure could be very harmful to that individual.

5. Data processed on a large scale: the GDPR does not define what constitutes large-scale, although Recital 91 provides some guidance. In any event, the following should be considered when determining whether the processing is carried out on a large scale:
    - The number of data subjects concerned, either as a specific number or as a proportion of the relevant population
    - The volume of data and/or the range of different data items being processed
    - The duration, or permanence, of the data processing activity
    - The geographical extent of the processing activity

6. Datasets that have been matched or combined, for example originating from two or more data processing operations performed for different purposes and/or by different controllers in a way that would exceed the reasonable expectations of the data subject.

7. Data concerning vulnerable data subjects (Recital 75): the processing of this type of data can require a DPIA because of the increased power imbalance between the data subject and the controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data.

    For example, employees would often meet serious difficulties to oppose the processing performed by their employer when it is linked to human resources management. Similarly, young children cannot be considered to be able to knowingly and thoughtfully oppose or consent to the processing of their data. This also concerns more vulnerable segments of the population requiring special protection, such as, for example, the mentally ill, asylum seekers, or the elderly, a patient, or in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.

8. Innovative use or applying technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control, etc.: The GDPR makes it clear (Article 35(1) and Recitals 89 and 91) that use of a new technology can trigger the need to carry out a DPIA. This is because the use of a new technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the controller to understand and to treat such risks.

    For example, certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy and therefore require a DPIA.

9. When the processing in itself "prevents data subjects from exercising a right or using a service or a contract" (Article 22 and Recital 91). This includes processing performed in a public area that people passing by cannot avoid, or processing that aims at allowing, modifying or reusing data subjects' access to a service or entry into a contract.

   For example, a bank screens customers against a credit reference database in order to decide whether to offer them a loan.

1.4 If, following a preliminary assessment, the proposed processing meets more than one of the above criteria, then it is more likely to present a high risk to an individual and a DPIA will be required. In some cases, processing meeting just one of the criteria listed above may result in high risk which requires a DPIA to the undertaken.

1.5 Where a controller determines that the proposed processing, although it includes one or more of the above criteria, is not likely to present a high risk, the reasons for not carrying out a DPIA should be thoroughly documented.

Where a project does not identify a high risk and a DPIA is not initially required, this should be reviewed particularly where any changes or modifications to the project occur.

1.6 If it is determined that a DPIA is necessary then the reasons should be documented.

The documentation should clearly explain why the proposed processing is considered to present a high risk to individuals and, as relevant, should make reference to the criteria set out in 1.3 above.

Step 2: Consultation process

Article 35(9) of the 'Applied GDPR' states:

"*Where appropriate the controller shall seek the views of the data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing.*"

Consultation should commence at an early stage so that the views obtained can be taken into account.

2.1 Consider how to consult with data subjects or their representatives.

Determine who may need to be consulted when and how.

Document the views of the data subject, including what, if any, actions have occurred as result.

2.2 Consider whether any other person should be consulted, including for example:

- other staff
- any processor that will be involved, or
- other experts, such as information security experts**.**

If it is not appropriate to consult with data subjects, justify and document why the reason for not doing so.

Step 3: Describe the proposed processing

The proposed processing, that is the initial concept, should be documented using whatever means are most suitable for your organisation and the project concerned.

Visual aids, such as flow charts, to document how information will be used as part of a project can assist in identifying potential risks. This may also help with internal communication by allowing the project team and others in your organisation to better understand the design of the project.

The documentation should:-

1. Describe the purposes of the processing, including:
   - Why the processing is necessary
   - What the expected outcome is
   - What effects, both positive and negative, upon individuals are anticipated
   - What the perceived benefits of the processing are and whether they are for the controller, the individual or more broadly

2. Describe the context of the processing, including:
   - What is the nature of your relationship with the individuals?
   - What, if any, control will an individual have over the processing?
   - Would an individual reasonably expect their data to be processed for this purpose?
   - Does the processing include children or other vulnerable groups?
   - Are there any issues of public concern?
   - Are there any other concerns, for example, security?
   - Is the processing novel in any way?
   - What is the current state of technology in this area?

3. Describe the scope of the processing, including **:**
   - The nature of the data
   - Whether the data includes special category or criminal offence data
   - The estimated volume of data to be processed
   - The estimated number of individuals that will be affected
   - How long the data will be retained
   - Whether the data will be shared or disclosed to any other controller;
   - What geographical area is covered

4. Describe the nature of the proposed processing, including:
   - The source of the data
   - When it will be obtained
   - How it will be obtained
   - How it will be processed
   - How it will be stored
   - How it will be deleted or destroyed

Step 4: Assess necessity and proportionality

Having established the initial concept, this step provides an opportunity for an objective analysis of the proposed processing and consideration of the proposal against not only data protection obligations but other obligations such as compliance with Article 8: Right to Respect for Private and Family Life under the European Convention on Human Rights.

An objective analysis should:

- Consider whether the proposal will actually achieve the specified purpose(s)
- Consider whether an acceptable outcome can be achieved without processing personal data or by other less intrusive means? (Article 25: data protection by default)
- Identify the lawful basis for the proposed processing – both in general terms and which of the conditions set out in Article 6 of the Applied GDPR are met
- If the proposed processing includes special category or criminal convictions or offences, identify which of the conditions for processing such data, set out in Article 9 and 10, will be met
- Consider whether the proposed processing of personal data is limited to the processing which is only necessary for the purpose
- Consider how the accuracy of the personal data is to be established or ascertained
- Consider what measures are required to ensure the data remains accurate it is must be kept up to date
- Identify what information is to be provided to individuals and when
- Consider the rights of individuals set out in Article 15 to 22 of the Applied GDPR and identify how those rights will be complied with.
- Identify whether any transfers will occur and if so what measures are required to ensure the data continues to be safeguarded and not processed for other unspecified purposes
- Identify whether any international transfers will occur and what measures are necessary to safeguard the personal data
- Identify if a processor is to be involved and what measures are required to ensure any processor complies with its obligations

Step 5: Identify and assess risks

Identify the potential impact and any harm or damage, whether physical, emotional or material, that might be caused to individuals by the proposed processing including:

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

To assess whether the risk is a high risk, you need to consider both the likelihood and severity of the possible harm. Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any possibility of serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk.

The following matrix can be used when considering the likelihood and severity of risks.

Severity of impact				
	Serious harm	**Low risk**	**High risk**	**High risk**
	Some impact	**Low risk**	**Medium risk**	**High risk**
	Minimal impact	**Low risk**	**Low risk**	**Low risk**
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

Other risks to consider

Security risks: including sources of risk, such as unlawful or unauthorised access to, modification of, or loss of personal data, and the potential impact of such risks.

Corporate risks: such as the impact of regulatory action, reputational damage or loss of public trust.

Step 6: Identify measures to reduce risk

Consider ways to reduce or eliminate the risks that have been identified.

For example:

- deciding not to proceed with the proposed project or an element of the proposed project
- reducing the scope of the processing
- deciding not to collect certain types of data
- reducing retention periods
- taking additional technological security measures
- training staff to ensure risks are anticipated and managed
- where possible, anonymising or pseudonymising data
- writing internal guidance or processes to avoid risks
- using a different technology
- putting clear data sharing agreements into place
- making changes to privacy notices
- offering individuals the chance to opt out where appropriate, or
- implementing new systems to help individuals to exercise their rights

This is not an exhaustive list.

Determine whether the measures would reduce or eliminate the risk and whether the costs and benefit of doing so would be appropriate.

Step 7: Consult the Commissioner

Integrate the outcomes of the DPIA into the project plans, identifying any action points and who is responsible for implementing them.

If having undertaken a DPIA there remains a high risk to individuals then the Information Commissioner must be consulted prior to any processing taking place.

Step 8: Review

Keep the DPIA under review and repeat it if there is a substantial change to the nature, scope, context or purposes of the processing.

It is good practice to publish your DPIA to aid transparency, accountability and foster trust.

Published July 2018