BHBIA
ETHICS & COMPLIANCE

Data Protection requirements

Risk and Privacy Impact Assessment

Introduction

All those processing personal data for commercial purposes are required to demonstrate that they comply with the data protection law. This requirement is referred to as 'accountability' and is a critical component of the EU and UK General Data Protection Regulations (GDPR) and the UK Data Protection Act (DPA) 2018.

As the GDPR/DPA 2018 distinguish between higher and lower risk data processing activities and the requirements for these two differ, it is essential that all those processing data can assess the level of risk associated with their activities. In fact, data protection law demands that organisations take a *"risk based approach"* to data protection. So, it's important that BHBIA members understand when and how to go about assessing risk.

Risk

Although 'risk' is regularly referred to within the GDPR/DPA 2018, it is not defined. It is generally associated with the risk of inappropriate access and disclosure that would cause harm. Assessing risk means you have to think carefully about the "likelihood and severity" of any negative impact of your processing on individuals. The level of risk will reflect the nature, scope, context and purpose of your data processing. A negative impact or harm could include: discrimination, identity theft or fraud, financial loss, damage to individual reputation, loss of confidentiality, reversal of pseudonymisation or significant economic or social disadvantage.

The Information Commissioner's Office (ICO) recommends that to examine data processing activities in terms of risk assessment you should take a three-pronged approach, this may be termed a preliminary risk assessment:

1. Identify any potential threats that could do harm e.g. excessive collection of data, inadequate records, inappropriate access, misuse, loss of data, excessive sharing, over-retention
2. Evaluate the severity of the harm – this is likely to involve evaluating how sensitive, valuable and critical the data are
3. Consider the likelihood of the harm occurring.

2 and 3 above will require you to think about (amongst other things):

- Where it will be stored?
- How secure is that?
- Who has control?
- Will it be transferred?
- Who would be responsible for data loss?

The next step is then applying cost-effective actions to mitigate or reduce the risk.

BHBIA
ETHICS & COMPLIANCE

Data protection impact assessments (DPIAs)

Data protection impact assessments (DPIA, also known as privacy impact assessments or PIAs) are the practical tool required by the GDPR/DPA 2018 to assist organisations in the risk assessment process. DPIAs are a tool for identifying, assessing and minimising the data protection risks of your project and identifying and evaluating privacy solutions.

A single DPIA can be carried out covering a set of similar processing operations that present similar high risks e.g. for very similar market research projects.

DPIAs SHOULD be carried out when:

- The data processing *might* result in a high risk to the rights and freedoms of the individuals. Consideration should be given to the status of the data subject e.g. vulnerable individuals as the impact may be considerably greater.
- If you are not sure whether your data processing is high or low risk, you need to carry out a DPIA – **if in doubt, carry one out!**

DPIAs MUST be carried out when:

- Large scale processing of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to their rights and freedoms
- Large scale processing of special categories of data (previously referred to as sensitive data)
- Using new technologies or the novel application of existing technologies (including AI) and the processing is likely to result in a high risk to rights and freedoms
- Automated processing, including profiling, that results in automated decisions having legal effects or similar significant impacts on the data subjects
- The GDPR/DPA 2018 defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual (e.g. personalised targeted direct mailings), profiling is not the same as market research segmentation.
- Systematic monitoring of a publicly accessible area on a large scale.

The GDPR/DPA 2018 does not define 'large scale'. The European Data Protection Board (EDPB) recommends that the following factors are considered when determining whether processing is large scale:

  - The number of data subjects concerned - either as a number or as a proportion
  - 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

The EDPB also provides some examples of large-scale processing which include the processing of patient data in the regular course of business by a hospital. An example that would not be considered large-scale is the processing of patient data by an individual physician.

BHBIA
ETHICS & COMPLIANCE

Who is responsible for Conducting a DPIA

- The DPIA should be carried out by the business area or individual who is leading on the project or process in consultation with stakeholders such as Compliance, IT, any processors and the DPO if you have one.

Organisations should ask themselves:

- Do we carry out potentially high-risk data processing? This might involve sensitive data, processing of personal data on a large scale or automated profiling of individuals.
- If the personal data was disclosed how likely is it that this would have a negative impact and how severe would this be?

The ICO advise that a DPIA should contain:

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller, or the consent provided by the data subject
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An assessment of the risks to individuals
- The measures in place to address risk, including security and to demonstrate that you comply e.g. quarantining data, deletion, redaction, encryption, restricting and controlling access and the technical and organisational measure taken to do these things.
- You can then sign off and record the DPIA outcomes and integrate the outcomes into any project plan.

For further information on how to conduct a DPIA see the ICO's guidance and template at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-impact-assessments/

When a DPIA indicates high risk data processing even after mitigation:

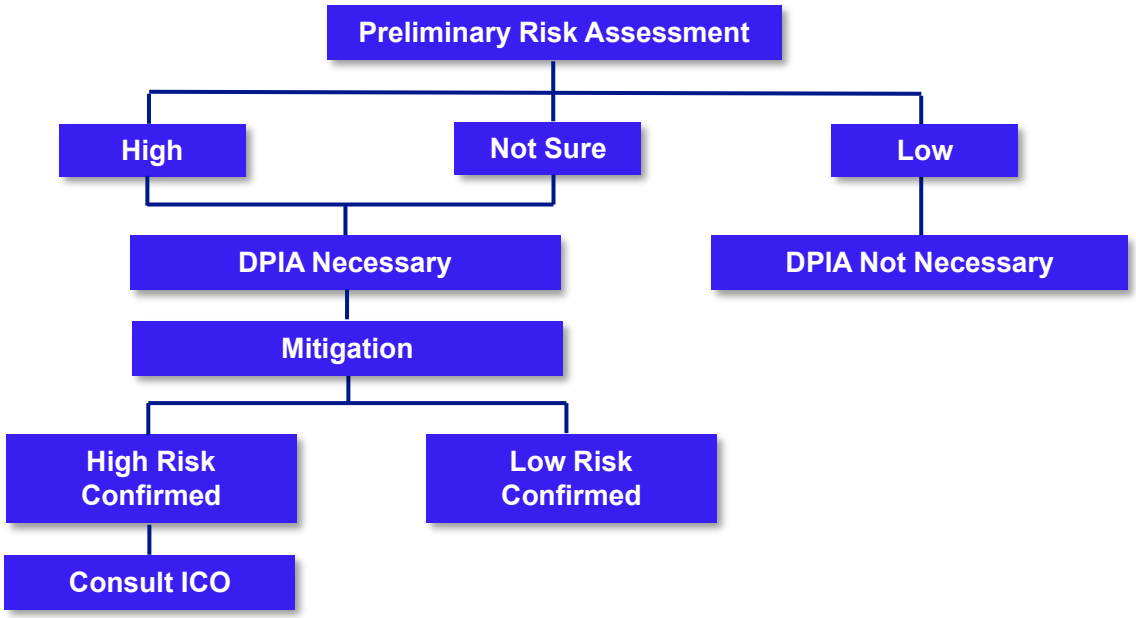
You will have to consult the ICO to seek its opinion as to whether the processing operation complies with data protection law.

Examples

The European Data Protection Board (EDPB) guidelines provide some examples, see below that illustrate how the criteria should be used to assess whether a particular processing operation requires a DPIA:

Examples of processing	Possible Relevant criteria	DPIA likely to be required?
The gathering of public social media data for generating profiles. - Evaluation or scoring. - Data processed on a large scale. - Matching or combining of datasets. - Sensitive data or data of a highly personal nature:	- Evaluation or scoring. - Data processed on a large scale. - Matching or combining of datasets. - Sensitive data or data of a highly personal nature:	YES
A processing of “personal data from patients or clients by an individual physician, other health care professional or lawyer”	Sensitive data or data of a highly personal nature. - Data concerning vulnerable data subjects	No
An online magazine using a mailing list to send a generic daily digest to its subscribers.	- Data processed on a large scale.	No

Overview of the process



Sources and references for further reading

ICO – Overview of the GDPR – Accountability

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/#:~:text=What%20is%20accountability?,guidance%20on%20accountability%20and%20governance

MRS - Adopting a Risk-Based Approach to GDPR Compliance
http://www.fairdata.org.uk/risk_based_GDPR_compliance

ICO's Data Privacy Impact Assessments
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-impact-assessments/

AvePoint Privacy Impact Assessment System
http://www.avepoint.com/privacy-impact-assessment/

EDPB Guidelines on Data Protection Officers ('DPOs')
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

The BHBIA's Ethics & Compliance Committee is providing this guidance as general information for its members. It is not legal advice and should not be relied upon as such. Specific legal advice should be taken in relation to any specific legal problems or matters. Whilst every reasonable effort is made to make sure the information is accurate, no responsibility for its accuracy or for any consequences of relying on it is assumed by the BHBIA.

Updated by the BHBIA's Ethics & Compliance Committee May 2025

British Healthcare Business Intelligence Association
St James House, Vicar Lane, Sheffield, S1 2EX
t: 01727 896085 • admin@bhbia.org.uk • www.bhbia.org.uk
A Private Limited Company Registered in England and Wales No: 9244455