BHBIA

BHBIA Ethics & Compliance

Preparing for the General Data Protection Regulation

Risk and Privacy Impact Assessment

Introduction

The General Data Protection Regulation (GDPR) will apply from 25 May 2018. All those processing personal data will be required to demonstrate that they comply with the GDPR. This requirement is referred to as 'accountability' and is a critical component of the GDPR.

As the GDPR distinguishes 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 the GDPR demands that organizations 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, 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 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 involves 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.

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 to assist organisations in the risk assessment process. DPIAs are a tool for identifying, assessing and reducing 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
- 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 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 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 does not define 'large scale'. The Article 29 Working Party (made up of representatives from data protection authorities in each EU Member State, the EU DP Supervisor and the European Commission, and sometimes referred to as the .WP29) 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 WP29 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.

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.

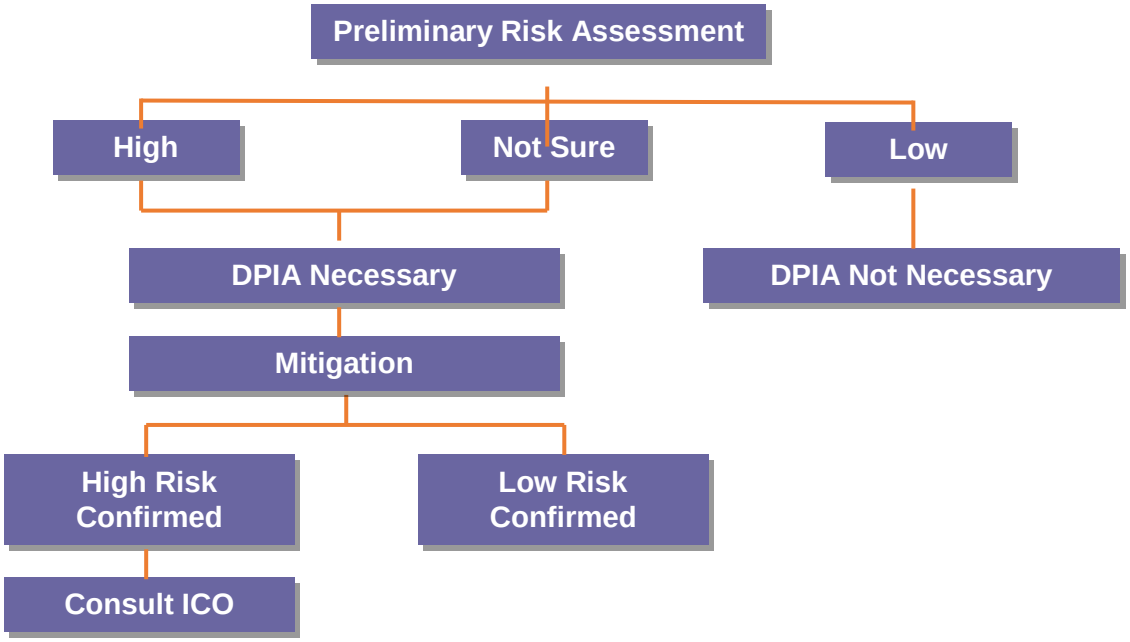
You can then sign off and record the DPIA outcomes and integrate the outcomes into any project plan.

For further information on how to conduct a DPIA see the ICO's *Conducting Privacy Impact Assessments Code of Practice*.

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 the GDPR.

Overview of the process



Sources and references for further reading

ICO – Overview of the GDPR – Accountability
https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/accountability-and-governance/

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

ICO's Conducting Privacy Impact Assessments Code of Practice
https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

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

Article 29 Data Protection Working Party Guidelines on Data Protection Officers ('DPOs')
http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

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 ensure the information is accurate, no responsibility for its accuracy or for any consequences of relying on it is assumed by the BHBIA. We do expect to update our guidance on the GDPR as more information becomes available.

Prepared by the BHBIA's Ethics & Compliance Committee May 2017

British Healthcare Business Intelligence Association
Ground Floor, 4 Victoria Square, St. Albans, Herts AL1 3TF
t: 01727 896085 • admin@bhbia.org.uk • www.bhbia.org.uk

A Private Limited Company Registered in England and Wales