Data Protection Impact Assessment

Under GDPR there is a greater focus on actively managing the risks around processing personal data. Part of this management is the completion of Data Protection Impact Assessments (DPIAs). These act rather like most risk assessment exercises; encouraging people to look carefully at what they are doing, why they are doing it, the risks involved and controlling those risks to an acceptable level.

It is a good idea to do DPIAs for higher risk processing activities in any event, not waiting for GDPR!

Under GDPR DPIAs must in accordance with Article 35 be completed where the use of the data "is likely to result in a high risk to the rights and freedoms of natural persons". The risks can arise from the activity and the category and quantity of the data to be used.

Step 1

Identify if a DPIA is needed

1) It might be helpful to answer screening questions to identify a proposal's potential impact on privacy, consider in particular:

- Are new technologies being used?
- Will the proposal involve automated decision making or profiling?
- Are special categories of personal data being processed?
- Is a large volume of personal data being processed?
- Will the proposal involve the systematic surveillance of large public spaces?
- Are datasets being merged?
- Is the personal data of vulnerable individuals being processed?
- Is data being transferred outside the EU?
- Will personal data be processed in ways which individuals might not reasonably expect?

2) If you think it likely that a DPIA is required contact the Data Protection Officer who can provide guidance.

Step 2

Determine that the processing is necessary and proportionate

3) Describe the processing that is being proposed and why it is being proposed; this will include an analysis of how the data will be obtained, used and retained.

4) Assess the necessity and proportionality of the processing in relation to the purpose, i.e. can it be done another way that requires less processing of personal data?

5) Always consider whether you can anonymise or at least pseudonymise the data you wish to process. You may be able to anonymise at a later date, safely destroying the original identifiable data. Also consider whether you can conduct the activity with less data either in terms of quantity or quality – only take what you need.

Step 3

Identify the risks associated with the processing

6) You will need to assess the risks to the rights and freedoms of the individuals whose data is being processed, i.e. what would happen if the data was lost or misused in some way? This needs to include consideration of the rights afforded to individuals under the GDPR. (See ICO guidance https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/)

7) Also consider the risk that the processing poses (if any) to compliance with the GDPR and to the University more broadly.

   This might helpfully be done in a tabular format e.g.

Proposed processing	Risk to individual	Compliance risk	Associated organisation risk

Step 4

Identify solutions/mitigations to the risks

8) Describe safeguards and security measures put in place, privacy by design, use of data processing and data sharing agreements.

9) Consider seeking the views of the data subjects, or their representatives and other interested parties (i.e. data processors, sector specialists).

Step 5

Document the findings

10) This is often helpfully done in a tabular format e.g.

Risk	Solution	Result (is the risk eliminated, reduced or accepted?)	Evaluation: is the final impact on individuals justified, compliant and proportionate?

Step 6

Feed the results into the proposal

11) Assess if there are changes that need to be made to the proposal, and define how the risks will be monitored.

12) Make sure that the solutions proposed deal with the risk. If you are not sure about acceptable levels please contact the Data Protection Officer.

Step 7

Implementation

13) Once you have completed the above findings and it is safe to proceed make sure that all those involved in the processing are aware of the necessary solutions.

14) Regularly review processing activity to make sure it is still compliant with the acceptable position and be responsive to any necessary changes.

ICO Guidance

We are presently waiting on specific ICO guidance to deal with DPIAs. However there is guidance on generally doing impact assessments see

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Rebecca Messenger-Clark
Dec 2017