LINKING THE DPIA TO THE DATA PROTECTION PRINCIPLES

Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with the Law.

Lawfulness, Fairness and Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject

Have you identified the purpose of the project?

How will you tell individuals about the use of their personal data?

Do you need to amend your data protection notices?

Have you established which conditions for processing apply?

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

Purpose Limitation

Personal data must not be collected except for a specific, explicit and legitimate purpose, and once collected must not be further processed in a manner incompatible with the purpose for which it was collected.

Does your project plan cover all of the purposes for processing personal data?

Have you identified potential new purposes as the scope of the project expands?

Have you ensured that appropriate review is undertaken where future changes may be planned to the processing?

Minimisation

Personal data processed must be adequate, relevant and limited to what is necessary in relation to the purpose for which it was processed.

Is the quality of the information good enough for the purposes it is used?

Which personal data could you not use, without compromising the needs of the project?

Accuracy

Personal data processed must be accurate and where applicable, kept up to date, and reasonable steps must be taken to ensure that personal data that is inaccurate (having regard to the purpose for which it is processed) is erased or corrected without delay.

If you are procuring new software does it allow you to amend personal data when necessary?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Who do you direct data subjects to for queries around accuracy? How well is that person supported to deliver on the obligations promptly and effectively?

Storage Limitation

Personal data must not be kept in a form that permits identification of the data subject any longer than is necessary for the purpose for which it is processed.

What retention periods are required for the personal data you will be processing?

Are you procuring software that will allow you to delete information in line with your retention periods? Does this delete all personal data or remove identifying features, retaining the information for other purposes such as statistics?

If identifying features are removed, does that prevent identification in all cases?

Integrity and Confidentiality

Personal data must be processed in a manner that ensures its security appropriately, including protecting it against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Have you reviewed and documented the security of all personal data intended to be processed?

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Accountability

The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles

Have you documented all your personal data processing and associated compliance?

Do you ensure that this documentation is regularly reviewed?

Are these records available to all relevant staff including senior management/board members?
