

CMT Exec report template

Data Protection Impact Assessment (DPIA)

Option 1 – no DPIA

As there is no personal data, special categories of personal data or criminal offence data being processed, there is no requirement to complete a DPIA.

This is evidenced by completion of DPIA screening questions.

Option 2 – full DPIA eg DAPIAN/ online tool

Completion of the DPIA screening questions identifies one or more of the below and so requires full DPIA.

Systematic and extensive profiling with significant effects:

“(a) any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.”

Large scale use of sensitive data:

“(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10.”

Public monitoring

“(c) a systematic monitoring of a publicly accessible area on a large scale.”

A DPIA is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of your accountability obligations under the UK GDPR, and when done properly helps you assess and demonstrate how you comply with all of your data protection obligations.

It does not have to eradicate all risk, but should help you minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what you want to achieve.

DPIAs are an essential part of your accountability obligations. Conducting a DPIA is a legal requirement for any type of processing, including certain specified types of processing that are likely to result in a high risk to the rights and freedoms of individuals. Under UK GDPR, failure to carry out a DPIA when required may leave you open to enforcement action, including a fine of up to £8.7 million, or 2% global annual turnover if higher.

By considering the risks related to your intended processing before you begin, you also support compliance with another general obligation under UK GDPR: data protection by design and default.

Option 3 – Short DPIA – template

Completion of the DPIA screening questions identifies some personal data/ special categories of personal data / criminal offence data that does not require full dpia.