

Data Protection Impact Assessment Stage 2

Briefly explain what the policy/service/project aims to achieve, including benefits to the organisation and individuals

Have you undertaken consultation (internally and externally) and, if so, what were the outcomes?

Who is identified as the Information Asset Owner (i.e. who will be responsible for the personal data collected)?

What personal data will be collected?

Will the personal data be shared and, if so, who will it be shared with?

How will individuals be told about the use of their personal data?

If you are relying on consent to process personal data, how will this be collected and recorded?

What will you do if consent is withheld or withdrawn?

How can you minimise intrusion, particularly if specific concerns have been expressed?

Do you envisage using the personal data for any other purpose in the future? If yes, please provide details

How will you ensure that the personal data is not excessive in relation to the purpose for which it is processed (e.g. asking for date of birth, when you only need an individual's name and postal address)?

How will you ensure the personal data is accurate and remains up to date?

Will information about people be disclosed to third parties (i.e. other organisations or people) who have not previously had access to this data?

What future demands may arise for wider use of the data and how will you address these?

If this involves marketing, have you a process for individuals to opt-out of their information being used for that purpose?

What is the retention period for the personal data you are processing?

How will you ensure the personal data is deleted in line with the retention period set?

Where, and in what format, will the personal data be kept?

Who will have access to the personal data?

Will an IT system or application be used to process the personal data? If so, will it provide protection against any security risks?

What training and instructions are necessary to ensure that employees know how to operate the system securely?

Will employees process the personal data away from the office, for example, paper files, on laptops, tablets, smart phones, etc? If yes, please provide details

What is the risk if this data is breached (e.g. distress to individuals, reputational, financial)?

How will you identify and address any privacy risks?

Will you be required to transfer personal data outside of the EEA? If yes, please provide details

If you will be making transfers, how will you ensure that the personal data is adequately protected?

If a contractor is being used to process personal data, where are they (and their data stores) based?

If a contractor is being used to process personal data, is an agreement in place which defines how they will protect the information?

Any other relevant information:

Outcome of DPIA:

How will you monitor this to ensure there is no adverse effect in the future?