

<p><b>2.11.4</b></p>	<p><b>Data Protection Impact Assessment ('DPIA')</b></p> <p>From the previous section it has been determined that the personal data you are collecting requires a Data Protection Impact Assessment ('DPIA').</p> <p>'Data protection by design' means embedding data privacy features and data privacy-enhancing technologies directly into the design of a project at an early stage. This will help to ensure increased protection for individual data privacy throughout the lifecycle of a research project. A key component of data protection by design is the DPIA.</p> <p>The purpose of a DPIA is to assess and demonstrate compliance with data protection legislation.</p> <p>The DPIA also provides evidence that the risks to individuals have been considered and sufficient measures have been taken to protect those individuals.</p> <p>The DPIA assesses the activity to be carried out against all the principles of data protection and determine whether the processing of personal data is both necessary and proportionate or whether changes to the process or additional controls are required.</p> <p><b>What is a DPIA and why may it be required / beneficial for a Research Project?</b></p> <p>A DPIA is a process designed to identify risks arising from of the processing of personal data and to manage these risks from as early as possible during the lifecycle of the project. It also demonstrates compliance with the GDPR.</p> <p>It is a mechanism for assessing the impact of new initiatives or new technologies and implementing measures to minimise or reduce associated risks.</p> <p>DPIA completion is frequently required as a key component of research project design.</p> <p>A DPIA is particularly important in instances where the research utilises new technologies or, taking into account the nature, scope, context and type of processing, <b><u>is likely to result in a high risk to the rights and freedoms of individuals.</u></b></p> <p>The DPIA process and outcomes will help to improve the design of a research project and enhance communication about data protection risks with relevant stakeholders such as research partners, third parties and participants.</p> <p>Please review the <a href="#">Questions</a> and associated <a href="#">Guidance</a> in the section below carefully.</p>		
	<p><b>Question</b></p>	<p><b>Help Text</b></p>	<p><b>Guidance</b></p>
<p>2.11.4.1</p>	<p><i>Why is the processing of personal data (i.e. data relating to an identified or identifiable living individual) necessary for the project?</i></p>	<p>Processing means any activity involving personal data.</p>	<p>It is important to justify the processing of personal data. Explain the rationale which justifies the necessity to process personal data for your research study rather than anonymous data which cannot identify any individual.</p> <p><b>Personal data:</b> Any information relating to an identified or identifiable living individual. In general terms, personal data means information about a particular living individual.</p> <p>'Identifiable' means a living individual who can be identified directly or indirectly in particular by an identifier such as: name, address, identification number (staff ID, participant ID reference code used instead of name), location data, an online identifier such as an internet protocol (IP) address, Internet cookie identifier, or other identifiers such as radio frequency identification tags, or any one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that living individual.</p>

Even when personal data has been replaced by a code (i.e. pseudonymised) it should still be considered as 'personal data' if it is possible to link back to the individual using this code.

Essentially, if someone can be identified directly or indirectly from information then it should be considered as personal data and subject to data protection law.

[Link to Trinity Data Protection handbook](#) for further examples of personal data or information of relevance (see page 8).

**Processing:** Any activity performed on personal data, whether or not by automated means, such as collection, recording, organisation, storage, adaption, retrieval, consultation, combination, sharing, anonymisation, erasure or destruction. Processing can be paper-based and /or electronic.

**Examples of processing:** Collecting potential participant names and contact details, recording interviews, transcribing interviews, storing hard-copy consent forms, storing data electronically, using data, sharing the personal data either internally or externally, conducting surveys. It is important to determine from the outset if it necessary to process personal data to meet the research project's objectives or to decide if there are alternative ways that the same objectives could be achieved without processing personal data. Generally speaking, to be able to pass the necessity test, there should be no equally effective alternative to the use of an individual's personal data.

For instance, could anonymised data be processed instead of data which directly identifies individuals? It is important to note that fully anonymous data is not considered as personal data and is not subject to data protection legislation.

'Necessary' means that processing should be reasonable and proportionate to the aim of the research and could not reasonably be achieved by some other less intrusive means.

[Link to Trinity Data Protection handbook](#) for further examples of personal data or information of relevance.

Personal data that has been replaced by a code (pseudonymised) should be considered as personal data.