

<p>2.11.4</p>	<p>Data Protection Impact Assessment ('DPIA')</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>What is a DPIA and why may it be required / beneficial for a Research Project?</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, <u>is likely to result in a high risk to the rights and freedoms of individuals.</u></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 Questions and associated Guidance in the section below carefully.</p>		
	<p>Question</p>	<p>Help Text</p>	<p>Guidance</p>
<p>2.11.4.12</p>	<p><i>Detail how and when you will code / pseudonymise personal data you are using for the project (if applicable).</i></p> <p><i>Detail how the personal data will be archived / anonymised / deleted / destroyed (as applicable).</i></p>	<p>Describe associated archiving / anonymisation / deletion / destruction processes for the data as appropriate.</p>	<p>Pseudonymised/Coded personal data: Information where the individual can only be identified with the use of additional information (which is kept securely and separately). Examples include a code or the use of pseudonyms, where the identity of the individual can be linked back in some way.</p> <p>Personal data that has been replaced by a code (pseudonymised) should be considered as personal data.</p> <p>See the Data Protection Commission's Guidance Note for more information on pseudonymisation techniques: https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf</p> <p>Trinity promotes a privacy by design based approach to any research project which uses personal data, commencing at the design stage and applicable through all phases of the data's lifespan.</p> <p>Researchers are encouraged to create data management plans for any research which uses personal data.</p> <p>This will ensure that the entire research journey from access/collection to deletion/archival has been considered from a data protection perspective.</p> <p>Adoption of this approach should minimise the risk of a data breach or non-compliance with data protection legislation.</p>

			Where possible, research data should be suitably prepared and uploaded to appropriate domain specific repositories or archives for long term preservation. If a domain specific repository does not exist, research data may be uploaded to institutional or appropriate third party repositories. See Good Research Practice Policy .
	<i>Include any additional information in respect of the study which may be relevant.</i>		