2.11.4	**Data Protection Impact Assessment ('DPIA')** From the previous section it has been determined that the personal data you are collecting requires a Data Protection Impact Assessment ('DPIA'). '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. The purpose of a DPIA is to assess and demonstrate compliance with data protection legislation. The DPIA also provides evidence that the risks to individuals have been considered and sufficient measures have been taken to protect those individuals. 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. **What is a DPIA and why may it be required / beneficial for a Research Project?** 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. It is a mechanism for assessing the impact of new initiatives or new technologies and implementing measures to minimise or reduce associated risks. DPIA completion is frequently required as a key component of research project design. 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, **is likely to result in a high risk to the rights and freedoms of individuals**. 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. Please review the Questions and associated Guidance in the section below carefully.		
	Question	**Help Text**	**Guidance**
2.11.4.10	*Who is authorised to access the data and describe how this access is controlled.*	See Guidance - please review carefully before answering Access controls relate to electronic and paper-based personal data.	Access controls relate to electronic and paper-based personal data. Firstly, you should identify where research project personal data is to be stored, who will have access to the research data, either in hard or soft copy format. Consider and document how you will control this access. Is the access restricted to the Research Team or will others have access to the research data in either identifiable or coded format? For hard copy documents state what physical location controls are in place; e.g. swipe card access, locked filing cabinets, security on the premises, log of those who access, how and where data is printed, stored destroyed and transferred.

			For soft copy documents, identify what system(s) will hold personal data. How will you control access to this system? Are users provided with unique user IDs and passwords, multi factor authentication etc. Is there an audit trail/log of those who access research data and the actions taken. Provide detail regarding encrypted laptops, managed VPN access etc. Please provide detail of existing audit trails / logs of those who access and the actions taken in respect of accessed data etc. Provide detail of controls in place.