**Department of Paediatrics Data Protection Impact Assessment (DPIA) Policy**

A Data Protection Impact Assessment (DPIA) is a process that systematically and comprehensively analyses the processing of data and helps to identify and minimise a project’s data protection risks. The DPIA is a tool that enables you to identify the most effective way to comply with your data protection obligations and meet individuals’ expectations of privacy.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. The outcome of a DPIA does not have to eradicate all risks totally, but rather serves to determine how to minimise risks and whether any assessed remaining risks are justified and acceptable.

Undertaking a Data Protection Impact Assessment is a legal requirement for processing personal data which presents a high risk to the rights and freedoms of individuals under the UK General Data Protection Regulation (UK GDPR)[[1]](#footnote-1). The UK GDPR defines personal data as any data about a living individual who can be identified or who is identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information (pseudonymised data).

**When to carry out a DPIA**

A DPIA should be carried out before any major project that requires the processing of personal data (this includes both administrative and research projects). Processing means ***doing something with someone’s personal data***. It includes collecting, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, using or the destruction of personal data. Processing begins when you collect personal information about someone, and continues until that information has been securely destroyed. If you hold information on someone, it counts as processing even if you don’t do anything else with it.

This assessment should begin while acquisition of the asset is being planned, so that it allows for proper preparation for secure storage and handling of the data, and must occur by the time the asset becomes live. The University has created a series of forms that must be used to carry out the DPIA procedures which can be found on the University’s website[[2]](#footnote-2).

**Research Projects sponsored by the University of Oxford**

The University’s Research Governance, Ethics and Assurance (RGEA) sponsorship process[[3]](#footnote-3) embeds data protection by design into its approval process so a separate DPIA is not necessary for most University-sponsored projects. However, where a project is deemed to be particularly high risk to individuals during the sponsorship process or where a standalone DPIA is necessary for approvals by a third party, the Research Governance team may ask the Principal Investigator to undertake a separate DPIA.

Projects that do not have to undergo research ethics approval do not have data protection by design embedded into the approval process and therefore need to complete a screening assessment and the relevant follow-up assessment. The screening assessment should be completed before the Head of Department or their designated nominee signs the CUREC form.

**Reviewing DPIAs**

DPIAs must be reviewed regularly by the project lead to ensure that the data processing is being carried out in accordance with data protection by design and to safeguard the rights of individuals. Where possible, the Information Governance Unit will regularly prompt project leads to carry out reviews of the DPIA until project completion, but the ultimate responsibility to keep the DPIA under review and up-to-date lies with the project lead. Any proposed changes to processing must be notified to the Information Governance Unit and the project lead must carry out a new screening assessment before the change takes place.

**Further guidance on DPIAs**

Please contact the department’s Information Governance Unit on [infogov@paediatrics.ox.ac.uk](mailto:infogov@paediatrics.ox.ac.uk) if you have any questions concerning the process of undertaking DPIAs.

**Document History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Author** | **Key Changes** | **Date** | **Review By** |
| 1.0 | Obi Udeariry  DOP Senior IG Manager | First published version.  To be reviewed annually | 16 June 2024 | June 2025 |

1. [Data protection impact assessments | ICO](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-impact-assessments/) [↑](#footnote-ref-1)
2. <https://compliance.admin.ox.ac.uk/data-protection-forms#collapse1091641> [↑](#footnote-ref-2)
3. [Where to submit for ethics approval | Research Support (ox.ac.uk)](https://researchsupport.admin.ox.ac.uk/clinical-trials-research-governance/sponsorship-approvals/ethics) [↑](#footnote-ref-3)