

Data

[illegible]

# Protection Impact Assessment (DPIA) Form

[illegible]

[illegible]

## Example Risks to Data Subject

Inappropriate disclosure of personal data internally within your organisation due to a lack of appropriate controls being in place.
Accidental loss of electronic equipment by organisation's personnel may lead to risk of disclosure of personal information.
Breach of data held electronically by "hackers".
Vulnerable individuals or individuals about whom sensitive data is kept might be affected to a very high degree by inappropriate use of data.
Information released in anonymised form might lead to disclosure of personal data if anonymisation techniques chosen are not robust enough.
Personal data being used in a manner not anticipated by data subjects due to an evolution in the nature of the project.
Personal data being used for purposes not expected by data subjects due to failure to explain effectively how their data will be used.
Personal data being used for automated decision making may be seen as excessively intrusive.
Merging of datasets may result in a data controller having far more information about individuals than anticipated by the individuals.
Merging of datasets may inadvertently allow individuals to be identified from anonymised data.
Use of technology capable of making visual or audio recordings may be unacceptably intrusive.
Collection of data containing identifiers may prevent users from using a service anonymously.
Data may be kept longer than required in the absence of appropriate policies.
Data unnecessary for the project may be collected if appropriate policies not in place, leading to unnecessary risks.
Data may be transferred to countries with inadequate data protection regimes.

## Example Risk Mitigation Measures

Deciding not to collect or store particular types of information.

Putting in place strict retention periods, designed to minimise the length of time that personal data is retained.

Reviewing physical and/or IT security in your organisation or for a particular project team and making appropriate improvements.

Conducting general or project-specific training to ensure that personal data is handled securely.

Creating protocols for information handling within the project, and ensuring that all relevant staff are trained in operating in accordance with the protocols.

Producing guidance for staff as reference point in the event of any uncertainty relating to the handling of information.

Assessing the need for new IT systems to safely process and store the data, and providing staff with training in any new systems.

Assessing the portability of using anonymised or pseudonymised data as part of the project to reduce identification risks where anonymised data is suitable.

Ensuring that individuals are fully informed about how their information will be used.

Providing a contact point for individuals to raise any concerns they may have with your organisation.

If you are using external data processors, selecting appropriately experienced data processors and putting in place legal agreements.

Deciding not to proceed with a particular element of a project if the data privacy risks associated with it are inescapable and cannot be reduced to an acceptable level.