Example risks

Risks to individuals

i. Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
ii. The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
iii. New surveillance methods may be an unjustified intrusion on their privacy.
iv. Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
v. The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
vi. Identifiers might be collected and linked which prevent people from using a service anonymously.
vii. Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
viii. Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
ix. Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
x. If a retention period is not established information might be used for longer than necessary.

Corporate risks

i. Non-compliance with the data protection legislation can lead to sanctions, fines and reputational damage.
ii. Problems which are only identified after the project has launched are more likely to require expensive fixes.
iii. The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
iv. Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
v. Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
vi. Data losses which damage individuals could lead to claims for compensation.

Compliance risks

i. Non-compliance with the Data Protection Act/General Data Protection Regulation (EU) 2016/679.
ii. Non-compliance with the Common Law Duty of Confidentiality.
iii. Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
iv. Non-compliance with sector specific legislation or standards.
v. Non-compliance with Human Rights Act 1998 and Equality Act 2010.