DPIA Form (template)

05 May 2026, 16 min read

> **Operated by:** Nudge Education Ltd · **Owner:** Data Protection Officer

About this template

A Data Protection Impact Assessment (DPIA) is required under UK GDPR Article 35 wherever processing of personal data — particularly children's data — is likely to result in high risk to the rights and freedoms of individuals. NEO uses this template DPIA form whenever a new platform, AI tool, or material change to processing is introduced.

For NEO online provision, a DPIA is mandatory before:

- A new learning, communication, or assessment platform is brought into use.
- An AI tool is introduced into any process that touches learner data.
- Any change to retention, sharing, or location of safeguarding records.
- Any new processing involving learners aged under 13 (ICO Children's Code threshold).

Form template

DPIA Form

Introduction

This form should be read and used in conjunction with the Data Protection Impact Assessment (DPIA) Procedure and has been designed to be used in the UK for compliance with the UK GDPR. Please note that this form is designed to support and record a data protection impact assessment as required by the law. It may not be suitable for any other form risk assessment or project.

How to complete a Data Protection Impact Assessment

Screening

A Data Protection Impact Assessment comes in two parts: the first part is a short screening questionnaire, which requires you to answer a set of questions to establish whether certain data processing operations, activities or processes will impact upon the rights and freedoms of data subjects. A new DPIA must be carried out if there is a change to the nature, scope, context or purposes of existing processing activities which meets any of the criteria below.

Full DPIA Assessment

Where you have answered yes to one or more of the screening questions you must complete the second part of the DPIA to document the assessment of the impact of the processing activities. Please elaborate and provide sufficient details where available.

Part 1 DPIA Screening

Background

*Delete one option Describe the project/processing/system etc. and, if it is new or a variation to existing, explain why it is being introduced. Include the objectives of the processing.

DPIA Screening Questions Complete this section to help determine whether the processing is likely to result in a risk to the rights and freedoms of data subjects. Consider carrying out a DPIA in any major project involving the use of personal data. Consider carrying out a DPIA if you plan to carry out any: ☐ evaluation or scoring; ☐ systematic monitoring; ☐ processing of sensitive data or data of a highly personal nature; ☐ large scale processing activities; You must always carry out a DPIA if you plan to: ☐ process special-category data or criminal-offence data on a large scale; ☐ process personal data that could result in a risk of physical harm in the event of a security breach; ☐ process personal data concerning vulnerable data subjects; ☐ process children's personal data for profiling or automated decision-making or for marketing purposes, or to offer online services directly to them; ☐ process biometric or genetic data; ☐ systematically monitor a publicly accessible place on a large scale; ☐ process personal data without providing a privacy notice directly to those affected; ☐ process personal data in a way that involves tracking

individuals' online or offline location or behaviour; ☐ use systematic and extensive profiling or automated decision-making or special category data to make significant decisions about people including decisions on someone's access to a service, opportunity or benefit; ☐ combine, compare or match data from multiple sources; ☐ use innovative technology or technology in innovate ways; ☐ processing that involves preventing data subjects from exercising a right or using a service or contract.

See further guidance notes below If any of the boxes above are ticked, a DPIA must be carried out. Complete Part 2 of this Form. If none of the boxes above are ticked a DPIA is not required. Sign Part 1 and forward this Form to the Data Protection Officer.

Part 2 Guidance Notes

Consider the following when evaluating whether processing operations are "likely to result in a high risk" to people.

1. Evaluation or scoring, including profiling and predicting, especially using aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements. Examples could include: a financial institution that screens its customers against a credit reference database or against an anti-money laundering and counter-terrorist financing (AML/CTF) database, a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks, a company building behavioural or marketing profiles based on usage or navigation on its website.
2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing legal effects or which similarly significantly affects the natural person. For example, the processing may lead to the exclusion or discrimination against individuals. Processing with little or no effect on individuals does not match this specific criterion. Further explanations on these notions is provided in further guidance on profiling.
3. Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through a systematic monitoring of a publicly accessible area may result personal data being collected in

circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) spaces. “Systematic” should be interpreted as meaning one or more of the following: occurring according to a system; pre-arranged, organised or methodical; taking place as part of a general plan for data collection; carried out as part of a strategy. “Publicly accessible area” should be interpreted as being any place open to any member of the public, for example a piazza, a shopping centre, a street, a market place, a train station or a public library.

4. Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in UK GDPR Article 9, as well as personal data relating to criminal convictions or offences as defined in UK GDPR Article 10. For example a general hospital keeping patients’ medical records or a private investigator keeping offenders’ details would both meet the criteria for a DPIA. Beyond the provisions of the UK GDPR, some categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject’s daily life (such as financial data that might be used for payment fraud). In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion may also include data such as personal documents, emails, diaries, notes from e-readers equipped with note-taking features, and very personal information contained in life-logging applications.
5. Data processed on a large scale: the UK GDPR does not define what constitutes large-scale, but it is recommended that the following factors in particular be considered when determining whether processing is carried out on a large scale: the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; the volume of data and/or the range of different data items being processed; the

duration, or permanence, of the data processing activity; the geographical extent of the processing activity.

6. Matching or combining datasets, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.
7. Data concerning vulnerable data subjects: the processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the data controller, meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable data subjects may include children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data), employees , more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, etc.), and in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.
8. Innovative use or applying new technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control, etc. The UK GDPR makes it clear that the use of a new technology, can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. The personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks. For example, certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy; and therefore require a DPIA.
9. When the processing in itself prevents data subjects from exercising a right or using a service or a contract. including processing operations that aim at allowing, modifying or refusing data subjects' access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

Part 3 DPIA

About the processing

What data being processed?

Name, Address, DOB, Phone, Email Other identifiers e.g. username, twitter handle etc. Financial information Religious Beliefs, Trades Union Membership or Political Opinions Medical/Health information or information about disabilities Criminal offences/convictions Information about behaviour Audio or video recordings (e.g. CCTV images) or photographs Location data Biometric or genetic information Profiling Other (please state): Tick all that apply and elaborate where you have selected “other”:

Who is the data about that is being processed?

Employees, former employees, or prospective employees incl. volunteers etc. Customers, former customers, or prospective customers Suppliers, former suppliers or prospective suppliers Members of the public Tick all that apply. Describe the people whose data is being processed below. Include a description of the nature of the organisation’s relationship with data subjects and whether the processing might include children or other vulnerable groups. Would data subjects expect their personal data to be used in the ways envisaged? Include a Justification if it is within their reasonable expectations.

Purpose of the processing

What are the aims of the processing? What does the organisation want to achieve from it? If the data is pre-existing, how will the new use/processing differ from the current use/processing?

Nature and context of the processing

Describe the processing activities and their purpose. Provide sufficient context to enable the reader to understand how and why the processing occurs. Include information about how data will be collected, used and stored; the scale size and frequency of processing as well as who will use the information and for what purpose(s). If the processing novel in any way please describe how.

Users and uses of the information

Disclosures and Sharing

Will any information be disclosed to or shared with any other organisations including processors, group companies, suppliers, government agencies etc.? If yes please specify which organisations and for what purpose. Please indicate if any recipients are data processors.

Data Processors

Are any data processors involved in the processing? Yes/No

IT Systems

What IT systems including hardware and software will be used for the processing? Include data flows where possible that explain and visualise the processing activities and flow of data.

Responsibility/Beneficiaries

Who in our organisation is taking responsibility for the processing? Who stands to benefit from the processing and how? What are the intended effects on individuals? How will they benefit?

Consultation process

The purpose of a consultation process is to understand the concerns and expectations of the individuals, test appropriate solutions and improve transparency. Will the organisation be seeking the views of staff/customers/residents/other stakeholders regarding this processing? If not, why is this not necessary? If yes, describe the consultation process.

Who else within the organisation will be consulted to ensure that all risks from the envisaged data processing are understood and properly mitigated?

Assessing the processing's necessity and proportionality

Are there alternative solutions which meet the goals without creating the same data processing risks? For example, a high-risk data processing activity which carries minimal benefit for individuals or significantly affects their data

protection rights may not be proportionate. Further, if there is a feasible alternative which is of lower risk (e.g. one that makes less use of personal data), such activity may also not be necessary. If there are no alternative solutions, consider whether the data processing complies with the data protection principles.

Rights

Who is responsible to responding to data subjects' rights requests relating to the processing? Where is the plan or procedure for handling requests?

Data Protection Principles

Privacy Information

What are the arrangements for the provision of privacy information?

Lawful Basis

What is the lawful basis for the processing? *You will need to cite specific conditions from the Data Protection Act 2018 to rely on a substantial public interest condition and have a policy in relation to that condition.

Purpose limitation and minimisation

What measures have been taken to ensure that any personal data collected or created in this processing is not used for any purpose other than that documented in this DPIA? What measures have been taken to ensure that only adequate and relevant information is used in the processing and that it is limited to only that which is necessary to achieve the processing aims?

Accuracy

What measures have you taken to ensure that personal data are accurate? Is there a requirement to keep any personal data up-to-date? Could there be any negative consequences if the personal data are not kept up-to-date?

Storage limitation

What is the envisage retention period for the various types of personal data collected or created during the processing? If you cannot specify a specific retention period, what are the criteria that determine if the information is no longer needed?

How will the information be treated when it reaches the end of its retention period?

Security

Describe the security measures that will be implemented to ensure the confidentiality, integrity, availability and restorability of the data, data systems and processes?

Risk Assessment

In identifying risks consider the potential impact on individuals, in particular whether the processing could possibly contribute to any of the following. Also consider how risks could be mitigated, reduced or eliminated all together.

To assess the level of risk, you should consider both the likelihood and severity of the possible harm that may be caused as a result of the processing activities. In determining the overall risk, use the matrix below:

Risks

In the table below, describe the risk, its source and the nature of potential impact on individuals. Identify as many risks as possible. Against each risk identified, determine the likelihood of the risk arising and the severity of harm caused if it did arise. Then document options for mitigating the identified risk, describe the effect on the risk and rescore it putting your evaluation of the mitigated risk score in the Residual risk score box. add more rows as required.

Decision, approval and documentation

Summary of Privacy Officer’s advice and is it being followed? Explain any variation from the Privacy Officer’s advice.

Mitigation measures

DPIA prepared by

This DPIA has been prepared to the best of my knowledge and ability. I understand that I may be subject to disciplinary action for any false information or negligence in preparing this document.

Privacy Officer approval

I certify that I have reviewed this DPIA and am confident that it has been prepared with sufficient accuracy and diligence.

DPIA Screening carried out by	
Signed	
Date of DPIA Screening	
Result of DPIA Screening	Full DPIA required / Full DPIA not required*

Signed by	Signature
Dated	Signature

Personal Data	Special Category Data
Consent	Explicit consent
Performance of a contract	Employment law purposes
Vital interests	Social security or social protection law purposes
Compliance with a legal obligation	Vital interests
Task carried out by a public authority	Data manifestly made public by data subject
Legitimate interests	Legal defence or claim
	Substantial public interest conditions*
	Preventive or occupational medicine
	Public health interests
	Archiving in the public interest
	Scientific or historical research or statistical purposes

Risks/potential impact	Mitigation
Inability to exercise rights	deciding not to collect certain types of data
Inability to access services or opportunities	reducing the scope of the processing
Loss of control over the use of personal data	reducing retention periods
Discrimination	taking additional technological security measures
Identity theft or fraud	training staff to ensure risks are anticipated and managed
Financial loss	anonymising or pseudonymising data where possible
Reputational damage	writing internal guidance or processes to avoid risks
Physical harm	using a different technology
Loss of confidentiality	putting clear data sharing agreements into place

Risks/potential impact	Mitigation
Any other significant economic or social disadvantage	making changes to privacy notices
	offering data subjects the chance to opt out where appropriate
	implementing new systems to help data subjects to exercise their rights

Describe the risk, its source and the nature of potential impact on individuals. Identify as many risks as possible.	Likelihood of harm (remote, possible or probable)	Severity of harm (minimal, significant or severe)	Overall risk score (low, medium or high)	Describe options to reduce or eliminate risk.	Effect the ris (elimi reduc accep

Mitigation measures approved by:
Mitigation measures to be executed by:

Mitigation measures approved by:
Mitigation measures to be completed by:
This DPIA will be kept under review by:
Residual unmitigated risks documented in the Data Protection Risk Register by:

Signed by	Signature
Dated	Signature

Signed by	Signature
Dated	Signature

Document control

Field	Value
Owner	Data Protection Officer
Status	live
Source file	`5. Nudge Education - Documentation for Commissioning Purposes/Data Protection/F - Data Protection Impact Assessment (DPIA) Form - 1.docx`