

**Data Protection Impact Assessment**

**Guidance Document**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Description | Author | Date |
| 1 | Initial version. | Nora Qamar | 30/06/2020 |
| 1.1 | Minor amendments. | Paul Smallcombe | 02/02/2024 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Prepared by: Nora Qamar

Version: 1.1

**Contents**

[Introduction to Data Protection Impact Assessments 3](#_Toc42261861)

[Step 1: Identify a need for a DPIA 4](#_Toc42261862)

[Step 2: Describe the processing 6](#_Toc42261863)

[Step 3: Consultation process 9](#_Toc42261864)

[Step 4: Assess necessity and proportionality 10](#_Toc42261865)

[Step 5: Identify and assess risks 11](#_Toc42261866)

[Step 6: Identify measures to reduce risk 12](#_Toc42261867)

[Step 7: Sign Off and Record Outcomes 13](#_Toc42261868)

[Step 8: Integration of Risk Mitigation Measures 14](#_Toc42261869)

[1 Appendix A – Definitions 15](#_Toc42261870)

[2 Appendix B – Special Category PERSONAL Data 16](#_Toc42261871)

[3 Appendix C – Legal Bases 16](#_Toc42261872)

# Introduction to Data Protection Impact Assessments

## What is a Data Protection Impact Assessment?

## ‘Data protection by design and by default’ is an approach mandated by the General Data Protection Regulation (GDPR) at Article 25. A Data Protection Impact Assessment (DPIA) is a key component of this. A DPIA is a process designed to help an organisation to identify and minimise the privacy and security risks that may arise when systems, services, procedures or policies are changed or introduced. A DPIA can also be used for research projects.

## These risks include mainly risks to individuals, in terms of damage and distress caused when personal data is mishandled, and organisational risks, such as financial and reputational damage resulting from personal data breaches or other misuse. Recital 75 of GDPR expands on the implications on the rights and freedoms of individuals to be considered i.e. processing which could lead to

## physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage;

## where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data;

## where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures;

## where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;

## where personal data of vulnerable natural persons, in particular of children, are processed; or

## where processing involves a large amount of personal data and affects a large number of data subjects.

## The outcome of a DPIA should be a reduction in risk to the rights and freedoms of individuals whose personal data is to be processed and improved compliance with data protection legislation. In certain circumstances, it is a legal requirement to carry out a DPIA. Consideration of whether a DPIA is required is therefore an important stage in any project plan.

##  The template for a DPIA at QMUL can be found on this page: <https://www.qmul.ac.uk/governance-and-legal-services/governance/information-governance/data-protection/data-protection-impact-assessments/>

# Step 1: Identify a need for a DPIA

## This step is important to complete for any project that involves processing personal data as it maps the project aim, what type of processing is involved, allowing you to identify if there is a need to complete the rest of the DPIA. If any of the headings are not relevant, simply mark these as ‘not applicable’ in the DPIA document.

If you decide not to carry out a full DPIA, you must document your reasons within the DPIA or elsewhere, such as a screening checklist, and keep this for future reference.

As your project continues, you may need to reconsider the requirement to undertake a DPIA, for example if it becomes apparent that personal data may be used in a way that was not initially foreseen.

## Project Aim

## What is the aim of your project? What is to be done and what will be the result?

## Processing Involved

## Processing has a broad definition. Personal Data is being "processed" when it is held, collected, maintained, recorded, altered, retained, used, disclosed, shared or destroyed, i.e. any operation on the data. List all the types of processing that may occur within your project. The next step will go into more detail.

## Need for DPIA

## The ICO has set out two sets of criteria to help you decide whether you should or must complete a DPIA for your project involving personal data.

## Does your project involve:

## evaluation or scoring;

## automated decision-making with significant effects;

## systematic monitoring;

## processing of sensitive data or data of a highly personal nature;

## processing on a large scale;

## processing of data concerning vulnerable data subjects;

## innovative technological or organisational solutions;

## processing that involves preventing data subjects from exercising a right or using a service or contract?

## If so, you should complete a DPIA.

## Does your project involve:

* systematic and extensive profiling or automated decision-making to make significant decisions about people;
* processing special category personal data or criminal-offence data on a large scale;
* systematically monitoring a publicly accessible place on a large scale;
* use of innovative technology in combination with any of the criteria in the [European guidelines](https://ec.europa.eu/newsroom/article29/items/611236) (i.e. in this [list above](#criteria));
* use of profiling, automated decision-making or special category data to help make decisions on someone’s access to a service, opportunity or benefit;
* carrying out profiling on a large scale;
* processing biometric or genetic data in combination with any of the criteria in the European guidelines;
* combining, comparing or matching data from multiple sources;
* processing personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;
* processing personal data in a way that involves tracking individuals’ online or offline location or behaviour, in combination with any of the criteria in the European guidelines;
* processing children’s personal data for profiling or automated decision-making or for marketing purposes, or to offer online services directly to them;
* processing personal data that could result in a risk of physical harm in the event of a security breach?

## If so, you must complete a DPIA.

More information can be found on the ICO website [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/) and in Article 35 of the GDPR.

We have developed a screening checklist to help assess the above criteria. There is one for research projects incorporated in the JRMO’s SOP 16a. There is another for everything else [here](https://www.qmul.ac.uk/governance-and-legal-services/media/arcs/governance/information-governance/data-protection/Data-Protection-Impact-Assessment-screening-checklist-v1.1.docx).

# Step 2: Describe the processing

This is where you need to go into more detail about data processing. Not all headings will be relevant to your project.

## Describe the Nature of Processing

**Data Collection:** How will you gather personal data and where from? Does it all come directly from data subjects? Does any come from QMUL or third parties?

**Data Use:** How will it be used in line with the project aims?

**Data Storage:** Where will data be stored and how will it be secured? Consider where the data storage facility is and ensure that the data is secured in its transition to the storage location.

**Data Deletion:** Will the data be deleted inline with existing QMUL policy and the Record Retention Scheme?

**Sources of Data:** Are you collecting from a primary source? How are you ensuring the secondary source data is correct? Linked to Data Collection.

**Sharing of Data:** Will you be sharing the data with parties external to QMUL? How will you ensure this sharing is GDPR-compliant? Do you have an Information Sharing Agreement?

**High Risk Types of Processing:** The GDPR details high risk processing as processing which leads to a high risk to the rights and freedoms of natural persons by virtue of the nature, scope, context and purposes of the processing. Below is a non-exhaustive list of High Risk types of processing.

|  |  |
| --- | --- |
| **Innovative technology** | Processing involving the use of new technologies, or the novel application of existing technologies (including AI).A DPIA is required for any intended processing operation(s) involving innovative use of technologies (or applying new technological and/or organisational solutions) when combined with any other criterion from WP248rev01[[1]](#footnote-2) |
| **Denial of service** | Decisions about an individual’s access to a product, service, opportunity or benefit which are based to any extent on automated decision-making (including profiling) or involves the processing of special- category data |
| **Large-scale profiling** | Any profiling of individuals on a large scale |
| **Biometric data** | Any processing of biometric data for the purpose of uniquely identifying an individual.A DPIA is required for any intended processing operation(s) involving biometric data for the purpose of uniquely identifying an individual, when combined with any other criterion from WP248rev01 |
| **Genetic data** | Any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject.A DPIA is required for any intended processing operation(s) involving genetic data when combined with any other criterion from WP248rev01 |
| **Data matching** | Combining, comparing or matching personal data obtained from multiple sources |
| **Invisible processing** | Processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort (as provided by Article 14.5(b).A DPIA is required for any intended processing operation(s) involving where the controller is relying on Article 14.5(b) when combined with any other criterion from WP248rev01 |
| **Tracking** | Processing which involves tracking an individual’s geolocation or behaviour, including but not limited to the online environment.A DPIA is required for any intended processing operation involving geolocation data when combined with any other criterion from WP248rev01 |
| **Targeting of children/other vulnerable individuals for marketing, profiling for auto decision making or the offer of online services** | The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children |
| **Risk of physical harm** | Where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals |

Describe the Scope of Processing

**Nature of Data:** There are 3 types of data

* [standard] personal data
* special category data
* criminal offence data.

Personal Data: Information about a living individual (Data Subject) from which that individual can be identified, either directly, or indirectly by using other data accessible to the Data Controller (QMUL).

Special Category Data: Personal data that needs more protection because it is sensitive, as defined in Article 9. You can see a full list in [Appendix B](#_Appendix_B_–).

Criminal Offence Data: Personal data about criminal convictions or offences (Article 10 GDPR). This data is covered by the Data Protection Act 2018.

You need to identify which types of data will be processed.

**Amount of Data Collected and Used:** How much data will be collected and used? How many types of data on each Data Subject?

**Data Collection Frequency and Retention:** How often will you collect data and what is the retention period?

**Number of Individuals Affected:** How many Data Subjects are there in your project? How many people are affected, which could be indirectly as well as directly?

**Geographical Area:** What geographical area does it cover?

Describe Context of Processing

**Nature of Relationship with Data Subjects:** What is the nature of your relationship with the individuals? For example, are they all our students?

**Individuals’ Control:** How much control will they have? For example, to withdraw from a project or object to certain uses?

**Individuals’ Expected Use of Data:** Would they expect you to use their data in this way? Will you or have you explicitly informed the individuals?

**Children and Other Vulnerable Groups:** Do they include children or other vulnerable groups?

**Prior Concerns and Security Flaws:** Are there prior concerns over this type of processing or security flaws?

**Novelty of Processing:** Is this a new way of processing data?

**Relevant Processing Technologies:** What is the current state of technology in this area? What systems are to be used?

**Potential Current Issues of Public Concern:** Are there any current issues of public concern that you should factor in?

**Approved Code of Conduct and Certification:** Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the Purpose of Processing

**Desired Outcome of Processing:** What do you want to achieve? Are there benefits identified in the Business Case document?

**Effects on Participants:** What is the intended effect on individuals? What are the impacts, if any? Could there be any detrimental effects?

**Benefits of Processing:** What are the benefits of the processing – for you, and more broadly? Do the Data Subjects get anything out of the processing?

# Step 3: Consultation process

The consultation process is important in understanding stakeholder opinions. Not all headings will be relevant to your project.

## Consultation with Individuals

## Describe when and how you will seek individuals’ views – or justify why it’s not appropriate to do so. Identify whose views you will be collecting. Looking at the type of data you are processing and your project aims, you should be able to identify the appropriate lawful basis. Remember, special category personal data and criminal offence data have extra steps when identifying the appropriate legal basis.

## Individuals Involved Within Organisation

## Identify stakeholders within QMUL you should consult.

## Assistance from Processors

## Are you working with a Data Processor? Do they have stakeholders to consult? Can they provide assistance about the proposed processing, for example, about any external service or system? Can they provide any input in to this DPIA?

## Consultation with Information Security Experts

## Do you plan to consult information security experts, or any other experts? If so, how will you carry this out? What do you need to ask them?

# Step 4: Assess necessity and proportionality

## This step is designed to implement two key principles of GDPR: Purpose Limitation and Data Minimisation. Not all headings will be relevant to your project.

## Lawful Basis for Processing

## Establishing Lawful Basis is a key part of completing a DPIA and prevents any unlawful processing of data. [Appendix C](#_Appendix_C_–) covers all the legal bases including extra conditions required for special category data. If you are unsure, please contact the Data Protection Officer at data-protection@qmul.ac.uk

## Processing for Purpose

## Explain how the processing will achieve the aim of your project.

## Function Creep

## How will you prevent function creep?

## Data Quality

## How will you ensure that the data is up to date and correct?

## Data Minimisation

## How will you ensure that data collection is minimised? Only process what is necessary to achieve your purpose. You should be able to justify each data point that you intend to process.

## Informing Data Subjects

## How will you keep data subjects informed; what information will you provide to them?

## Supporting Data Subjects’ Rights

## How will you help support their rights? It is possible not all of these rights will be applicable, but you need to check and consider. If someone tries to exercise one of their rights, who will deal with it and will it be possible to fulfil?

## Ensuring Compliance with GDPR

## What measures do you take to ensure processors comply, if using one? Will you have an information sharing agreement? Do you need to take any other actions or put in place any other measures to ensure compliance with the legislation, for example, where informing Data Subjects or security is concerned?

## Safeguarding International Transfers

## How will you safeguard any international transfers, i.e. outside the U.K. or EEA? Such transfers can only be made under certain conditions and may require a Transfer Risk Assessment.

# Step 5: Identify and assess risks

## This step is important in identifying any risks discovered in the project so far, including any compliance and corporate risk.

**Describe source of risk and nature of potential impact on individuals:** Provide a summary of the risk and its effects on the data subject.

## Likelihood: This represents the likelihood of the risk materialising, and is scored on a scale of 1 – 5:

## Rare

## Unlikely

## Possible

## Likely

## Almost Certain

## Impact: This indicates the seriousness of the risk materialising, and is scored on a scale of 1 – 5:

## Negligible

## Minor

## Moderate

## Major

## Catastrophic

## Risk Score: Risk Score represents the estimation of the severity of the risk.

## Impact x Likelihood = Risk Score

## The Risk Key below can help you visual the Risk Score and establish if the risk is low, medium or high.

|  |
| --- |
| **Risk Key** |
| **Likelihood** | **Impact** |
| 1 - Negligible | 2 - Minor | 3 - Moderate | 4 - Major | 5 - Catastrophic |
| 1 – Rare | **Low****1** | **Low****2** | **Low****3** | **Low****4** | **Low****5** |
| 2 – Unlikely | **Low****2** | **Low****4** | **Low****6** | **Medium****8** | **Medium****10** |
| 3 – Possible | **Low****3** | **Low****6** | **Medium****9** | **Medium****12** | **High****15** |
| 4 – Likely | **Low****4** | **Medium****8** | **Medium****12** | **High****16** | **High****20** |
| 5 – Almost Certain | **Low****5** | **Medium****10** | **High****15** | **High****20** | **High****25** |

# Step 6: Identify measures to reduce risk

## This step identifies appropriate measures to mitigate the previously identified risk. If there is any residual risk that has a High risk score, you must consult the ICO before going ahead. This residual risk will then have to be signed off in Step 7.

**Options to reduce or eliminate risk**

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in Step 5**.**

## Effect on Risk

## Identify the effect of the measures on the previous risk score. Is the risk:

## Eliminated

## Reduced

## Accepted

## Residual Risk

## Reconsider the Likelihood x Impact of the risk with the mitigation measures in place. This is called the residual risk score.

## Measures Approved

## Each measure must then be approved and signed off in Step 6 and 7. We recommend having the measures approved by the Data Protection Officer.

# Step 7: Sign Off and Record Outcomes

## This step important in maintaining accountability and transparency. Not all approvals will apply to every project.

**Measures Approved by**

Who approved of the measures in Step 6, we recommend having this signed off by a member of staff who specialises in data protection such as the DPO.

**Residual Risk Approved by**

If there is any High residual risk, you must consult the ICO before going ahead. Once this consultation has happened, this box can be signed off.

**DPO Advice Provided by**

A DPO or a qualified risk assessor should advise on compliance, Step 6 measures and whether processing can proceed. Their advice should be summaries and signed off.

**DPO advice accepted or overruled by**

If the DPO’s advice is overruled, the reason must be explained in the comments and signed off by the party responsible.

**Consultation responses reviewed by**

If the decision on processing departs from individuals’ views expressed during consultation, the reasoning should be explained in the comments section and signed off.

**This DPIA will be kept under review by**

This box should identify who is responsible for keeping the DPIA under review as its aims, processing, risks and mitigation my change during the life cycle of the project and the DPIA must document those changes and reassess the necessary measures. This individual will also be responsible for monitoring the integration of the risk mitigation measures into the project, outlined in the next step.

# Step 8: Integration of Risk Mitigation Measures

## This step oversees whether the risk mitigation methods have been integrated into the project plan and completed.

**Decide who is responsible for the integration of the risk mitigation measures**

Going through each mitigation measure, provide a small summary of the measure that needs integrating.

**Responsibility**

Identify whose responsibility it is to integrate the measure into the project.

**Status**

Record whether the integration of the mitigation measure has been completed.

# Appendix A – Definitions

|  |  |
| --- | --- |
| Term | Meaning |
| **Data Controller** | The organisation which determines how personal data is being processed, and is legally liable for ensuring that Data Subjects are informed of the nature of the processing being undertaken, for data security etc. Queen Mary, as a legal entity is the Data Controller, rather than individual departments or employees. |
| **Data Processor** | An institution or individual which acts under instructions from a Data Controller in processing personal data on its behalf. |
| **Data Subject** | Person about whom personal data is processed. (A Data Subject must be a living individual ('natural person'); data relating to the deceased is not covered by the provisions of data protection legislation). |
| **Lawful Basis** | The lawful bases for processing are set out in Articles 6 and 9 of the GDPR. At least one of these must apply whenever you process personal data. See Appendix C to learn more. |
| **Personal Data (Personally Identifiable Information)** | Information about a living individual (Data Subject) from which that individual can be identified, either directly, or indirectly. |
| **Processing** | Processing has a broad definition. Personal Data is being "processed" when it is held, collected, maintained, recorded, altered, retained, used, disclosed, shared or destroyed – any operation/transaction on personal data. |
| **Special Category Data** | Types of personal data defined by GDPR likely to be more sensitive therefore given extra protection; see Appendix B. |
| **International Transfers** | There are rules around restricted transfers, i.e. those outside the U.K. |

Most of the above can be found defined in the UK GDPR (<https://www.legislation.gov.uk/eur/2016/679/article/4>)

# Appendix B – Special Categories of Personal Data

**GDPR ‘special category’ data is personal data revealing:**

• racial or ethnic origin

• political opinions

* religious or philosophical beliefs

• trade union membership

• genetic data, biometric data for the purpose of identifying a person

• data concerning health

• data concerning a person's sex life or sexual orientation

In addition, personal data relating to criminal convictions and offences is to be treated in much the same way, although it is not technically special category data.

# Appendix C – Legal Bases

**From Article 6(1) GDPR, applying to ordinary or standard personal data[[2]](#footnote-3):**

1. **Consent** - The individual has given consent to the processing for one or more specific purposes. *NB: The threshold for obtaining consent is high under GDPR. See Recitals 32, 33, 42 and 43 of GDPR.*
2. **Necessary for performance of a contract** - The processing is necessary for the performance of a contract with the individual or in order to take steps at the request of the individual prior to entering into a contract.
3. **Legal obligation** - The processing is necessary for compliance with a legal obligation to which the data controller is subject. Only legal obligations under U.K. law will satisfy this condition. However, that law need not be statutory (e.g. common law obligations are sufficient).
4. **Vital interests** - The processing is necessary in order to protect the vital interests of the individual or of another natural person. This is typically limited to processing needed for medical emergencies.
5. **Public functions** - The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Those functions must arise under U.K. law.
6. **Legitimate interests** - The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Controllers should undertake a legitimate interests assessment which involves a “careful assessment of” the underlying processing to ensure it properly balances the interest of the controller against any potential intrusion to the individual’s privacy. In particular, would the individual “reasonably expect” that processing for that purpose will take place.

These bases do not apply alone to special category personal data. To process that, you need one of the conditions above *as well as* a legal basis from Article 9 GDPR.

**From Article 9(2) GDPR, applying to special category personal data:**

1. the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes, except where U.K. law provides that the prohibition referred to in paragraph 1 [of Art. 9] may not be lifted by the data subject;
2. processing is necessary for **the purposes of carrying out the obligations** and exercising specific rights of the controller or of the data subject **in the field of employment and social security and social protection law** in so far as it is authorised by U.K. law or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; [specific examples are included in the Data Protection Act 2018]
3. processing is necessary to **protect the vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
4. processing is carried out in the course of its **legitimate activities with appropriate** safeguards by a foundation, association **or any other not-for-profit body with a political, philosophical, religious or trade union aim** and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
5. processing relates to **personal data which are manifestly made public by the data subject**;
6. processing is **necessary for the establishment, exercise or defence of legal claims** or whenever courts are acting in their judicial capacity;
7. processing is necessary **for reasons of substantial public interest**, on the basis of domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; [specific examples are included in the Data Protection Act 2018]
8. processing is necessary for the **purposes of preventive or occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of domestic law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3; [specific examples are included in the Data Protection Act 2018]
9. processing is necessary for reasons of **public interest in the area of public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of domestic law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; [specific examples are included in the Data Protection Act 2018]
10. processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes** in accordance with Article 89(1) based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. [specific examples are included in the Data Protection Act 2018]

Conditions with basis in domestic law must also meet a condition of Schedule 1 Part 2 in the DPA 2018.

**Data Protection Act 2018 Schedule 1 Part 2**

1. Statutory and government purposes
2. Administration of justice and parliamentary purposes
3. Equality of opportunity or treatment
4. Racial and ethnic diversity at senior levels
5. Preventing or detecting unlawful acts
6. Protecting the public
7. Regulatory requirements
8. Journalism, academia, art and literature
9. Preventing fraud
10. Suspicion of terrorist financing or money laundering
11. Support for individuals with a particular disability or medical condition
12. Counselling
13. Safeguarding of children and individuals at risk
14. Safeguarding of economic well-being of certain individuals
15. Insurance
16. Occupational pensions
17. Political parties
18. Elected representatives responding to requests
19. Disclosure to elected representatives
20. Informing elected representatives about prisoners
21. Publication of legal judgments
22. Anti-doping in sport
23. Standards of behaviour in sport

**Note the *necessity* in these conditions.**

1. <http://ec.europa.eu/newsroom/document.cfm?doc_id=47711> [↑](#footnote-ref-2)
2. i.e. is not special category data or data relating to criminal offences [↑](#footnote-ref-3)