# Northern Ireland Policing Board Policy on

# Data Protection Impact Assessments

POLICY

Date to be added

Record No.

1. The GDPR, which became law on 25 May 2018, made it mandatory for public authorities to consider and, if necessary, complete a Data Protection Impact Assessment (DPIA, previously known as a Privacy Impact Assessment) before embarking on any processing operation which will involve personal data. In the UK, this was implemented by the Data Protection Act 2018. In preparation for the introduction of this the Policing Board made it a mandatory requirement to consider the need for a DPIA from January 2018. This brought us in line with the NICS where the practice was made mandatory by the Head of the Civil Service and Permanent Secretaries from July 2017.

2. Staff should be clear that processing, in the context of Data Protection, is a very broad concept, and does not apply simply to IT systems. The Information Commissioner's Office (ICO) has made it clear that it expects a DPIA to be considered, at an early stage, in the planning of any legislation, programme or initiative which will involve personal data and therefore, by implication, a possible risk to the privacy of individuals. This should happen when any new processing operation is being considered, and also if substantial changes are planned to an existing operation (amendments to legislation, major upgrades to IT systems, change of scope, data being put to new uses, and so on.) To help business areas determine if a DPIA is necessary a DPIA Screening Template has been included at Annex A to this policy. If the IAO decides that a DPIA is not necessary, the completed screening template must be retained as evidence of the decision-making process.

   ***N.B.*** *if what you are planning does not involve any personal data, a DPIA is not required; however, this is not always clear, and indirect and unintentional impacts should always be considered*.

3. As with all risk management methodologies, a DPIA provides a clear, comprehensive and structured way to identify and document the sensitivity of your data, any possible risks to privacy in what you are planning, and how you will deal with these. In the event of a data breach or a complaint to the ICO, the DPIA will be our first line of defence in attempting to prove that we carried out appropriate due diligence. (IAOs should note that GDPR legislation gives the ICO the power to fine public authorities for not having completed a DPIA, if they feel this should have been done; this would be separate from, and in addition to, any fine for the breach itself.)

4. The ICO has produced guidance which sets out in detail the format for a DPIA, and how / when[1] they expect one to be conducted. It also provides a sample DPIA template. As this guidance is the standard against which the ICO will judge us in the event of a data breach or regulatory investigation, it is Policing Board policy that all DPIA's produced in the organisation will conform to it.

[1] Annex C provides a list of processing operations that the ICO deems require a mandatory DPIA.

5. A key principle of risk management is proportionality; the purpose of completing a DPIA is not to generate paper or impose an unnecessary additional burden on the business. While all sections of ICO guidance / sample template should be completed, the depth of detail and the scale of the overall exercise will be directly proportionate to the volumes of data involved, the sensitivity of the information, and the potential impact of any breach. A copy of the ICO's sample DPIA template has been included at Annex B to this policy.

6. Information Asset Owners and ICT staff should also note that the DoJ Accreditation Authority Panel will require a completed DPIA to be presented as part of the Risk Management Accreditation Document Set (RMADS) when an IT system which processes personal data is submitted for accreditation or re-accreditation.

7. To provide assurance to the Accounting Officer all completed DPIA's and screening templates must be signed off by the Data Protection Officer.

8. While technical support may be useful to IAOs when completing a DPIA it is not likely that an outsider will be best placed to carry out this work, which requires detailed knowledge of the business, the proposed action, and the implications of any decisions. Answering the questions at Annex A during the DPIA screening process will help you to identify where there is a risk that the project will fail to comply with the data protection legislation or other relevant legislation, for example the Human Rights Act.

9. To ensure consistency across the Policing Board; to ensure a rapid response to any ICO queries, and to provide a knowledge base for the assistance of IAOs, the Data Protection Officer will retain a record of all DPIA's and DPIA Screening Templates completed.

**N.B**. *It is recommended practice for public authorities covered by the Freedom of Information Act (FOIA) to include DPIA reports in their publication scheme under section 19 of FOIA.*

Annex A

## DPIA Screening Template

| | |
| --- | --- |
| Project Name: | |
| Business Area: | |
| Information Asset Owner: | |
| Date Completed: | |

| Summary of project: |
| --- |
| |

| Stakeholders: |
| --- |
| |

| Description of Personal Data involved: |
| --- |
| |

# Data Protection Impact Assessment - screening questions

Before answering these screening questions refer to Annex C. This outlines a list of processing operations that the ICO has deemed require a mandatory DPIA.

These questions are intended to help you decide whether a DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA is required.

| Question | Yes | No | Notes |
|---|---|---|---|
| Is this a major project involving the use of personal data or will the project involve the:<br>• Collection of new information about individuals or<br>• Information collected in a new way (eg move to on-line forms)? | | | |
| Will the project compel individuals to provide information about themselves?<br><br>For example a change to existing policy, process or system that involves personal information that makes it compulsory to collect or disclose information. | | | |
| Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information (eg sharing or matching personal data held by different organisations or in different datasets)? | | | |
| Are you planning to use previously collected personal information about individuals for a purpose it is not currently used for, or in a way it is not currently used? | | | |

| | | | |
|---|---|---|---|
| Does the project involve:<br>• Evaluation or scoring<br>• Automated decision-making with significant effects<br>• Systematic monitoring<br>• Processing of sensitive data or data of a highly personal nature (Special category data or criminal offence data). For example, the use of biometrics or facial recognition.<br>• Processing on a large scale<br>• Processing of data concerning vulnerable data subjects<br>• Innovative technologies or organisational solutions<br>• Processing that involves preventing data subjects from exercising a right or using a service or contract<br>• A change in location of business area or branch (eg move to centralised service or office move).<br>• A change in how personal information is stored or secured (eg Personal information being transferred offshore (Cloud storage)). | | | |
| Will the project involve a change in how sensitive information is managed (eg information migrated to a new database). | | | |
| Will the project require you to contact individuals in ways which they may find intrusive? | | | |
| Will the project lead to keeping personal data for a longer or shorter period than before (ie a change to the Retention & Disposal Schedule? | | | |

Following completion of this screening template it has been determined that a DPIA is / is not required*[2].

Information Asset Owner: _____

Print Name:_____

Date:_____

Data Protection Officer:_____

Print Name:_____

Date:_____

[2] Delete as appropriate

ANNEX B

This template must be used to record the DPIA process and results.

# Data Protection Impact Assessment template

## Submitting controller details

| | |
| --- | --- |
| Name of controller | |
| Subject/title of DPO | |
| Name of controller contact /DPO (delete as appropriate) | |

## Step 1: Identify the need for a DPIA

| Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA. |
| --- |
| |

# Step 2: Describe the processing

| **Describe the nature of the processing:** how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved? |
| --- |
| |

| **Describe the scope of the processing:** what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover? |
| --- |
| |

| **Describe the context of the processing:** what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)? |
|---|
| |

| **Describe the purposes of the processing:** what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly? |
|---|
| |

## Step 3: Consultation process

| **Consider how to consult with relevant stakeholders:** describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts? |
|---|
| |

## Step 4: Assess necessity and proportionality

| **Describe compliance and proportionality measures, in particular:** what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers? |
|---|
| |

# Step 5: Identify and assess risks

| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risks as necessary. | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
|---|---|---|---|
| | Remote, possible or probable | Minimal, significant or severe | Low, medium or high |

# Step 6: Identify measures to reduce risk

| Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5 | | | | |
|---|---|---|---|---|
| **Risk** | **Options to reduce or eliminate risk** | **Effect on risk** | **Residual risk** | **Measure approved** |
| | | Eliminated<br>reduced<br>accepted | Low<br>medium<br>high | Yes/no |

# Step 7: Sign off and record outcomes

| Item | Name/position/date | Notes |
|---|---|---|
| Measures approved by: | | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by: | | If accepting any residual high risk, consult the ICO before going ahead |
| DPO advice provided: | | DPO should advise on compliance, step 6 measures and whether processing can proceed |
| Summary of DPO advice: | | |
| DPO advice accepted or overruled by: | | If overruled, you must explain your reasons |
| Comments: | | |
| Consultation responses reviewed by: | | If your decision departs from individuals' views, you must explain your reasons |
| Comments: | | |
| This DPIA will kept under review by: | | The DPO should also review ongoing compliance with DPIA |

Annex C

## What does the ICO consider likely to result in high risk?

The ICO is required by Article 35(4) to publish a list of processing operations that require a DPIA. This list complements and further specifies the criteria referred to in the European guidelines. Some of these operations require a DPIA automatically, and some only when they occur in combination with one of the other items, or any of the criteria in the European Guidelines referred to above:

1. **Innovative technology**: processing involving the use of innovative technologies, or the novel application of existing technologies (including AI). A DPIA is required where this processing is combined with any of the criteria from the European guidelines.

2. **Denial of service**: Decisions about an individual's access to a product, service, opportunity or benefit that is based to any extent on automated decision-making (including profiling) or involves the processing of special category data.

3. **Large-scale profiling:** any profiling of individuals on a large scale.

4. **Biometrics:** any processing of biometric data. A DPIA is required where this processing is combined with any of the criteria from the European guidelines.

5. **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 where this processing is combined with any of the criteria from the European guidelines.

6. **Data matching:** combining, comparing or matching personal data obtained from multiple sources.

7. **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. A DPIA is required where this processing is combined with any of the criteria from the European guidelines.

8. **Tracking:** processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment. A DPIA is required where this processing is combined with any of the criteria from the European guidelines.

9. **Targeting of children or other vulnerable individuals:** 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.

10. **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.

You should also be aware that the data protection authorities in other EU member states will publish lists of the types of processing that require a DPIA in their jurisdiction.