An Garda Síochána (AGS)

Garda National Data Protection Office (GNDPO)

Practical Guidance on

Data Protection Impact Assessments

(DPIAs)

Overview of presentation

- What is a Data Protection Impact Assessment?
- Identify when a DPIA should be conducted?
- Identify when a DPIA is not required
- When in a project lifecycle should a DPIA be conducted?
- Who should be involved in conducting the DPIA?
- What stages are involved in carrying out a DPIA?

What is a Data Protection Impact Assessment?

- A DPIA describes the process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with data protection legislation
- DPIAs are required under Part 5 of the Data Protection Act 2018 (Section 84) and the General Data Protection Regulation (Articles 35 and 36) where a particular processing activity is likely to result in a high risk to the rights and freedoms of individuals
- A DPIA is fundamentally a risk assessment process, designed to show the data controller (AGS) has shown due consideration to the risks associated with a processing activity

When should a DPIA be carried out?

- Article 35 of the GDPR states a DPIA should be administered when “It is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations of the protection of personal data.”

What is a high risk to the rights and freedoms of natural persons?

The GDPR provides some non-exhaustive examples of when data processing is “likely to result in high risks”:

- “A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.”
- Processing of special categories of data or data concerning criminal convictions and offences at a large scale
- “A systematic monitoring of a publicly accessible area on a large scale.”

Examples of when a DPIA should be conducted

- New or untested technology
- Sensitive or special category personal data involved
- The data subjects are vulnerable or in a weak bargaining position
- Large amounts of personal data will be processed
- Individuals may be evaluated or profiled
- Data sets may be consolidated
- Monitoring or surveillance of individuals will be undertaken
- Or when individuals' rights may be restricted

When is a DPIA not required?

Where the processing is not “likely to result in a high risk to the rights and freedoms of natural persons” (article 35(1)).

When the nature, scope, context and purposes of the processing are very similar to the processing for which DPIAs have been carried out. In such cases, results of a DPIA for similar processing can be used (Article 35(1)).

Where a processing operation has a legal basis in EU or Member State law and has stated that an initial DPIA does not have to be carried out, where the law regulates the specific processing operation and where a DPIA, according to the standards of the GDPR, has already been carried out as part of the establishment of that legal basis (Article 35(10)).

DPC guidance states that a DPIA is not required in circumstances where:

- Processing operations do not result in a high risk to the rights and freedoms of individuals;
- Processing was previously found not to be at risk by DPIA;
- Processing has already been authorised by the DPC;
- Processing already has an existing clear and specific legal basis in EU or Member State law and where a DPIA has already been carried out as part of the establishment of that legal basis or where the legal basis states that a DPIA is not required; or
- Where the processing is listed by the DPC as one that does not require a DPIA.
- DPIAs are not required where the purpose of processing is outside of the scope of either the GDPR or Part 5 of the Data Protection Act 2018. This includes, per Section 8(1)(a) of the Data Protection Act 2018, where processing is for the purposes of safeguarding the security of the State. The Data Protection Act of 1988 (as amended) continues to apply for processing of personal data for this purpose and the other purposes listed under Section 8.

When in a project lifecycle should a DPIA be conducted?

It is good practice to carry out a DPIA as early as practical in the design of the processing operation. For some projects the DPIA may need to be a continuous process, and be updated as the project moves forward.

The DPIA should be carried out “prior to the processing” (GDPR Articles 35(1) and 35(10), recitals 90 and 93).

If a project is already underway, a DPIA can still be undertaken, on the basis it is better to carry out an assessment than ignore the data protection risks altogether.

Also to note, significant changes to implemented projects may also require a DPIA.

Who should be involved in conducting the DPIA?

- AGS overall is the **Data Controller** for processing activities for which it determines to purpose and means
- **Business owner** - responsible for determining the need for processing and for the initial draft DPIA
- **ICT** – responsible for advice on technical safeguards and processes.
- **Internal/External stakeholders** (e.g. contracted processors) – can also provide input/advice
- **DPU** – responsible for giving advice to business area/ICT on data protection considerations/safeguards
- **DPC** – provides independent feedback on draft DPIAs (where required)

Eight Stages of DPIA

Stage 1 provides an initial screening exercise to summarise the processing activity and assess whether or not a DPIA is required;

Stage 2 is where a detailed description of the processing activity should be outlined;

Stage 3 is where the features of the processing activity should be documented, including the technical and organisational measures in place to safeguard the data being processed, to confirm the activity is in compliance with the key principles of data protection;

Stage 4 is where the specific controls for ensuring data subject's rights are protected are documented alongside the procedures for notifying any data breaches to the DPC;

Stage 5 is where the approach to stakeholder engagement and consultation on the given processing activity can be documented;

Stage 6 is the risk assessment where all risks related to the processing activity are documented along with relevant safeguards and mitigations to provide an assessment of their impact, likelihood, and overall risk score;

Stage 7 is where consultation with the DPC is considered and documented, including a summary of any feedback provided by the DPC on the draft DPIA; and,

Stage 8 is where the final sign off for the processing activity and DPIA is documented and review arrangements outlined.

Stage One: Identify the need for a DPIA

Provide a General Description of the Processing Activity and consider the following.

- Is personal data being processed?
- Are Special Categories of Personal Data Being Processed?
- Is it High Risk Processing?
- Automated-decision making producing legal or other significant effects
- Systematic monitoring
- Data processed on a large scale
- Datasets that have been matched or combined
- Data concerning vulnerable data subjects
- Includes processing where there is power imbalance between the data subject and the data controller
- Innovative use or applying technological or organisational solutions
- Data transfer across borders outside the European Union
- When the processing prevents data subjects from exercising a right or using a service or contract

Stage Two: A detailed description of the processing activity

The purpose(s) of the processing

- Expand on the summary and outline the purpose of the processing activity that is the subject matter of the DPIA;
- What is the nature of that processing activity, and the relevant legal basis for it? What function does it assist AGS to achieve?
- What are the benefits to the organisation, the public or other interested parties from the processing concerned?
- Who is responsible for the processing within AGS?
- What external stakeholders are involved?

Stage Two: A detailed description of the processing activity

A systematic description of the envisaged processing operations

- Detail the full life cycle of the processing activity (collection, retention, consultation and use, procedures for review and deletion/destruction of records when no longer required);
- If available, include a flow diagram to clearly outline and explain data flows and how data is kept secure at each stage of the processing activity;
- Detail the control mechanisms in place to govern each stage of the processing activity's life cycle. Reference any relevant policies/procedures/manuals applicable to the processing activity, along with arrangements for logging and audit/review mechanisms for AGS personnel involved in the processing of personal data as part of the activity.
- Note in respect of logging that for automated processing systems, it is a requirement under Section 82 of the Data Protection Act 2018 for the data controller to create and maintain a data log of operations carried out by that system.

Stage Three: Compliance with key principles of Data Protection

1. Lawfulness and fairness of processing, and transparency
2. Necessity and proportionality of the proposed processing
3. Purpose limitation
4. Data Minimisation
5. Accuracy
6. Storage Limitation
7. Integrity & Confidentiality – Electronic, Physical and Organisational security controls
8. Accountability

Stage Four: The Rights of Data Subjects

Exercising Data Subjects Rights

Common to Part 5 of the DPA 2018 and the GDPR are the following rights:

- The right to information (Section 90 DPA 2018, Articles 13 and 14 GDPR);
- The right of request access (Section 91 DPA 2018, Article 15 GDPR);
- The right to request rectification of inaccurate data (Section 92 DPA 2018, Article 16 GDPR);
- The right to request erasure (Section 92 DPA 2018, Article 17 GDPR);
- The right to request restriction of processing in certain circumstances (Section 92 DPA 2018, Article 18 GDPR); and
- Rights in relation to automated decision making that produces a decision based solely on automated processing, including profiling that produces legal or otherwise significant effects (Section 89 DPA 2018, Article 22 GDPR).

Data subjects also have additional rights specific to personal data processed under GDPR:

- The right of data portability (Article 20 GDPR) and,
- The right to object to processing (Article 21 GDPR).

The rights of data subjects may be restricted only where it is necessary and proportionate to do so and in accordance with data protection legislation, with due regard for the fundamental rights and legitimate interests of the data subject.

Section 94 of the Data Protection Act 2018 refers in respect of restrictions that may be applied to the rights of data subjects for processing activities for law enforcement purposes and subject to Part 5 of the Data Protection Act 2018. Section 60 of the Act refers in respect of restrictions that may be applied to the rights of data subjects for processing activities subject to GDPR.

Stage Four: Data Breaches

Managing Data Breaches

- The AGS Data Protection Unit manages notification of personal data breaches to the Data Protection Commission

- Where a data breach or suspected data breach in relation to the processing activity that is the subject of the DPIA occurs, it will be reported immediately to the Data Protection Unit (GDPR.dataprotection@garda.ie) in order for the Data Protection Unit to advise on next steps in respect of notification of the breach to the Data Protection Commission and recommended measures to mitigate against the impact of the breach on affected data subjects and the An Garda Síochána as a data controller.

- The DPIA template includes the information that should be included in a breach notification to the Data Protection Unit

Stage Five: Stakeholder Consultation

- Stakeholder consultation is an important part of the DPIA process and can reveal risks that may otherwise have gone unnoticed. For the processing activity that is the subject matter of this DPIA, determine the key consultees (internal and external) for the project. You can use consultation at any stage of the DPIA process, and it may be of benefit to return to stakeholders for further consultation throughout and prior to finalising the project

- In this section summarise the key stakeholders for the project, and why it is necessary or appropriate to consult with them. A table included in the DPIA template can be used (if needed) to record the outcome of stakeholder consultation, including the purpose of the consultation and any issues/risks associated with the processing activity identified by the stakeholder

Stage Six: Risk Assessment

- The identification of data protection and other related risks is the **most important aspect of the DPIA**
- All identified risks related to the processing activity (to data subjects, An Garda Síochána as the data controller, and any other relevant stakeholders) should be documented here, along with the proposed solutions and safeguards designed to reduce or eliminate the identified risk
- All risks should be scored before and after the implementation of the identified mitigating safeguards according to impact, likelihood, and the resulting combined risk score, and in line with the risk matrix guide. Impact and likelihood are assessed on a scale of 1-5. The overall Risk Rating is the product of Impact and Likelihood of the identified risk, before and after mitigation (1-25)
- Where a risk remains rated as high following mitigation, consultation with the Data Protection Commission (DPC) on the draft DPIA is **mandatory**

		Consequence				
		Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood	5 Almost certain	Moderate 5	High 10	Extreme 15	Extreme 20	Extreme 25
	4 Likely	Moderate 4	High 8	High 12	Extreme 16	Extreme 20
	3 Possible	Low 3	Moderate 6	High 9	High 12	Extreme 15
	2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
	1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5

Stage Seven: Consultation with the DPC
Stage Eight: Final Sign-Off and Review

Stage Seven: Consultation with the DPC

If the DPIA outcomes suggest that any identified risks remain high following mitigation, it is a legislative requirement under Section 84 of the Data Protection Act 2018 and Article 36 GDPR to consult with the Data Protection Commission before the commencement of the processing activity

Depending on the nature of the processing activity, the Data Protection Unit may recommend informal consultation on a draft DPIAs to seek their expertise and feedback on the processing activity and the safeguards identified

In this section:

- Document the consultation feedback from the DPC (whether from formal or informal consultation) and the changes made to the DPIA to account for the DPC's feedback; or
- Document the rationale, on the basis of the processing activity and the risks identified for why consultation with the DPC is not required for this DPIA

Stage Eight: Final Sign-Off and Review

This section can be updated as required to:

- Document the sign off and finalisation of the DPIA by the business owner responsible for the processing activity;
- Document that the Data Protection Officer has been consulted on the DPIA and their feedback incorporated; and,
- Document the consent to the processing as outlined in the DPIA by any other key stakeholders (e.g. ICT, external partner data controllers) involved in the project, as required.

Scenarios – Is a DPIA required?

Scenario 1

- AGS is considering a new technology platform for its recruitment process. It receives approximately 70,000 job applications each year
- The platform will enable it to specify minimum screening criteria to applications each year.
- If an applicant does not meet the criteria, they will not proceed to the next stage of the process, and will receive a notification that their application has been rejected
- If the applicant does meet the criteria, their application will be passed to the recruitment team for further consideration
- This means that the recruitment does not need to spend time reviewing any applications which do not meet the criteria
- Applications processed on the platform will include, name, address, previous work history, qualifications, contact information for the candidates and referees

Scenarios – Is a DPIA required?

Scenario 2

- AGS has a website that attracts approximately 1,000 visitors a day.
- The Communications team wishes to analyse the information about website visitors
- The website platform collects data on the IP addresses of individual visitors, the time they visited the website and what pages they viewed
- The analysis will be used to assess and improve how it communicates information about its services

Contact information for the Data Protection Unit (DPU)

- The DPO and Data Protection Unit (DPU) sit within the responsibility of the **Chief Information Officer, Andrew O'Sullivan** and under the **Deputy Commissioner, Policing and Security, Anne Marie McMahon**

- The DPU is based on the **Third floor, 89-94 Capel Street, Dublin 1**.
  - **Public Facing Mailbox (external correspondence) -** Dataprotection@Garda.ie
  - **DPU Section Mailbox (internal queries – including DPIA queries) -** GDPR.DataProtection@Garda.ie

  - **Telephone -** 01 666 9521
  - **DPIA Template** available on our portal page