

Data Protection Impact Assessment Policy

**CONTENTS**

 **Page**

1. Introduction 3
2. What is Information Risk 3

2.1 What is Privacy? 3

2.1.1 Why is Privacy Important? 4

2.1.2 Privacy by Design 4

1. What is a Data Protection Impact Assessment (DPIA)? 4
2. Benefits 4
3. When is the Best Time to Conduct a DPIA? 5
4. DPIA – Who is Responsible? 5
5. DPIA Process, Assessments and Templates 6
6. Monitoring 7
7. What Types of Processing Automatically Requires a DPIA? 8

9.1 What Other Factors Might Indicate Likely High Risk? 9

1. How Do We Identify and Assess Risks? 10
2. How Do We Identify Mitigating Measures 11
3. Further Information 12

Appendix 1 – Data Protection Impact Assessment – Part 1 Screening Questions 13

Appendix 2 – Data Protection Impact Assessment Template 15

# Introduction

East Ayrshire Leisure recognises that individuals have a right to **privacy** and that they expect personal and confidential data held regarding them to be processed and handled within legislative boundaries and good practice.

Guidance and policy documents to support the protection of privacy and confidentiality of information are located within the Information Governance pages on the council intranet [here.](http://eacintranet/Services/DemocraticServices/InformationGovernance/Information-Governance.aspx)

This procedure is based on the guidance produced by the UK **Information Commissioner**.

The **European General Data Protection Regulation (2016)** (GDPR) stipulates it is a legal requirement in certain circumstances to undertake a Data Protection Impact Assessment (DPIA).

The UK **Information Commissioner** (ICO) promotes the use of Data Protection Impact Assessments (previously known as Privacy Impact Assessments) as an integral part of demonstrating and understanding information risk and to ensure a **Privacy by Design** approach is considered by organisations.

Conducting a DPIA ensures:

* Risk can be managed through the gathering and sharing of information with stakeholders.
* Systems can be designed to avoid unnecessary privacy intrusion.
* Features can be built in from the outset to reduce privacy intrusion.

Where the success of delivering an initiative depends upon people accepting, adopting and using a new system or process, failing to address or recognise privacy concerns can be a significant risk factor.

In areas of high risk processing where risk cannot be mitigated the assessment allows for the organisation to consider the risks and balance these against the business objectives. In certain cases it may be necessary to involve the ICO.

# What is Information Risk?

Institute of Risk Management defines information risk management as “*the policies, procedures and technology one adopts in order to reduce the threats, vulnerabilities, and consequences that could arise if data is not protected.”*

A risk matrix is detailed at page 11 of this procedure.

## **2.1 What is Privacy?**

Article 8 of the Human Rights Act (1998) provides everyone with the right to respect for both private and family life including home and correspondence. Invasion of privacy is defined as an intrusion into personal life of another without justification. Privacy is about maintaining a sense of control of an individual or group over their own information and how that information flows.

## **2.1.1 Why is Privacy Important?**

Public Authorities are responsible for carrying out their business according to government legislation and obligations. Data sets are an important corporate asset that need to be safeguarded. Data protection legislation controls the way in which information is handled and to give legal rights to individuals who have information stored about them.

Privacy is about respecting individuals. It refers to freedom from intrusion and relates to all information and practice that is personal or sensitive in nature to an individual.

## **2.1.2 Privacy by Design**

Privacy by Design is an approach that promotes privacy and data protection compliance from the very start. It is a legal requirement for organisations to ensure that Privacy by Design is a key consideration in the early stages of any project, and then throughout its lifecycle.

GDPR imposes a general obligation upon organisations to implement technical and organisational measures to show that you have considered and integrated privacy and data protection into your processing activities.

A Privacy by Design approach will help to inform and improve operational processes. It will ensure the rights and freedoms of individuals (our customers, employees and service users) are respected by

* keeping their data safe
* ensuring those that have access to their data is proportionate and justified
* building trust and confidence with our customers
* protecting our reputation

# What is a Data Protection Impact Assessment (DPIA)?

It is an assessment framework which can anticipate and address the likely privacy risks and impacts from collecting, using and disclosing personal information of new initiatives or changes in business processes.

## **Why undertake a DPIA?**

DPIAs are an essential part of our data protection accountability obligations. Conducting a DPIA is a legal requirement for any type of processing that is likely to result in high risk. Failing to carry out a DPIA in these cases may leave our organisation open to enforcement action, including a fine from the UK **Information Commissioner.**

# Benefits

Notwithstanding the legal obligation, the DPIA also brings broader compliance benefits, as it can be an effective way to assess and demonstrate our compliance with all data protection principles and obligations.

However DPIAs are not just a compliance exercise. An effective DPIA allows us to identify and fix problems at an early stage, bringing broader benefits to both individuals and our organisation.

# Best Time to Conduct DPIA

DPIAs are most effective when they are started at an early stage of a project or change process, when:

* The project is being designed;
* You know what you want to do;
* You know how you want to do it; and
* You know who else is involved.

But ideally it should be started before:

* Decisions are set in stone;
* Systems have been procured;
* Contracts/Memorandum of Understanding (MOU)/ agreements have been signed;

# DPIA – Who Is Responsible?

Conducting a DPIA usually requires a range of expertise and interests. These are not normally undertaken by one person. It is best that DPIAs are conducted by a small team who together have expertise in a number of areas:

* Knowledge of the overall initiative;
* Knowledge of the relevant stakeholders and customer segments from the services;
* Knowledge of the Data Protection Legislation;
* Expertise in project management;
* Expertise in records, information and data management;
* Ability to assess and communicate organisational risks;
* Expertise in ICT security processes, technologies and cyber risk ;
* Ability to assess which privacy solutions are feasible for the relevant project;
* Knowledge of appropriate representatives of and advocates for the stakeholder group and consultation techniques.

You should seek the advice of the Data Controller. The Data Controller will provide advice on:

* Whether you need to do a DPIA;
* How you should do a DPIA;
* What measures and safeguards you can take to mitigate risks;
* Whether you’ve done a DPIA correctly; and
* The outcome of the DPIA and whether the processing can go ahead.

The DPO’s will review and provide advice which should be recorded on the DPIA. If you don’t follow their advice, you should record your reasons and ensure you can justify your decision.

**A DPIA must be finally approved and signed at Senior Manager level or above.**

If you have carried out a DPIA that identifies a high risk, and you cannot take any measures to reduce this risk, you need to consult the UK Information Commissioner’s Office (ICO). East Ayrshire Council’s Data Protection Officer acts as a contact point for the ICO.

The ICO will provide a written response advising whether the risks are acceptable, or whether you need to take further action. In some cases they may issue a formal warning or take action to ban the processing altogether.

# DPIA Process, Assessment and Templates

DPIAs are required in circumstances where a change occurs that impacts on personal data such as: projects, new systems implementations, changes to business processes etc.

DPIAs are most effective when they are conducted at the initial stage of a project or at the development stage of a new business practice to ensure that potential privacy concerns are identified. Identified privacy concerns can be addressed and safeguards built in rather than bolted on as an expensive afterthought. It is recommended that:

* DPIA should be commenced as part of the initiating a project stage within East Ayrshire Leisure’s project management framework so that risks can be identified and appreciated before the problems become embedded in the design.
* If the project is already underway, conduct a DPIA as soon as possible so that any major issues are identified with the minimum possible delay.

The DPIA framework at Appendix 1is a structured process which looks at all aspects affecting privacy. This includes:

* What should a DPIA include?
* Does the project or initiative need a DPIA?

The templates contain 7 sections and depending on the scope and nature of your project (including identified risks) you may be required to complete all sections.

The forms are designed to:

* Provide general guidance to identify and analyse privacy impacts at an early stage of a project, change or initiative.
* Facilitate the recording of results and recommendations from the assessment process.
* Monitor the progress of implementations of actions identified to mitigate the risks of likely impacts
* Provide lessons learned to other projects, changes or initiatives

|  |
| --- |
| **DPIA – Framework**  |
| **Part 1 – Identify the need for a DPIA - screening questions**  | The screening questions will identify whether or not the proposed initiative will impact on privacy and whether or not you need to complete the full assessment process. Where you answer **“yes” or “unsure”** you will need to progress to undertake the full assessment.  |
| **Part 2 – Describe 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 another way of describing data flows. What types of processing identified as likely high risk are involved? |
| **Part 3 – Consultation Process** | 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? |
| **Part 4 – Assess necessity and proportionality** | What is your lawful basis for processing? Does the process actually achieve your purpose? How will you ensure data quality and minimisation? What information will you give to individuals? How will you support their rights? What measures do you take to ensure processors comply?  |
| **Part 5 – Identify and assess risks** | Describe the source of risk and nature of potential impact to individuals.  |
| **Part 6 – Identify measures to reduce risk** | Identify additional measures to reduce or eliminate risks identified as medium or high risk in Part 5. |
| **Part 7 – Sign off and record outcomes** | Detail DPO advice, record outcomes and sign off by Senior Manager or above. |

#

# Monitoring

It is the responsibility of the Senior Manager to instruct the Project Manager (PM) (or the lead person handling the change) to start an Initial Assessment and examine whether a DPIA should be conducted.

It may be that the PM and/or team have already considered privacy impacts however using the formal DPIA process ensures that potential privacy concerns are recorded, risk identified and mitigation controls where possible, are recorded and documented in a formal manner.

This is particularly important in areas of high risk processing activities or when there has been an information rights complaint. Examples of high risk processing can be found in Section 9.

Where the identified risks are high and it is not possible to mitigate the level of risk to an acceptable level, it will be necessary to consult with the ICO.

In such cases there must be consultation with East Ayrshire Council Data Protection Officer who will review ahead of making a submission to the ICO.

# 9. What Types of Processing Automatically Require a DPIA?

Article 35(3) of the GDPR sets out three types of processing which always require a DPIA:

1. **Systematic and extensive profiling with significant effects:**

**Quote**

“(a) any 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”.

1. **Large scale use of sensitive data:**

**Quote**

“(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10”.

1. **Public monitoring:**

**Quote**

“(c) a systematic monitoring of a publicly accessible area on a large scale”.

The ICO is required by GDPR Article 35(4) to publish a list of the kind of processing operations that are likely to be high risk and require a DPIA. The current list includes a further ten types of processing that automatically require a DPIA:

1. **New technologies:** processing involving the use of new technologies,or the novel application of existing technologies (including AI).
2. **Denial of service:** Decisions about an individual’s access to a product,service, opportunity or benefit which 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.
5. **Genetic data:** any processing of genetic data other than that processedby an individual GP or health professional, for the provision of health care direct to the data subject.
6. **Data matching:** combining, comparing or matching personal dataobtained from multiple sources.
7. **Invisible processing:** processing of personal data that has not beenobtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort.
8. **Tracking:** processing which involvestracking an individual’s geolocationor behaviour, including but not limited to the online environment.
9. **Targeting of children or other vulnerable individuals:** The use ofthe 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 apersonal data breach could jeopardise the [physical] health or safety of individuals.

**9.1 What other factors might indicate likely high risk for a DPIA to take place?**

The Article 29 working party of EU data protection authorities has published guidelines with nine criteria which may act as indicators of likely high risk processing:

* Evaluation or scoring.
* Automated decision-making with legal or similar significant effect.
* Systematic monitoring.
* Sensitive data or data of a highly personal nature.
* Data processed on a large scale.
* Matching or combining datasets.
* Data concerning vulnerable data subjects.
* Innovative use or applying new technological or organisational solutions.
* Preventing data subjects from exercising a right or using a service or contract.

In most cases, a combination of two of these factors indicates the need for a DPIA. However, this is not a strict rule. You may be able to justify a decision not to carry out a DPIA if you are confident that the processing is nevertheless unlikely to result in a high risk, but you should document your reasons.

On the other hand, in some cases you may need to do a DPIA if only one factor is present – and it is good practice to do so.

**10. How do we Identify and Assess Risks?**

Consider the potential impact on individuals and any harm or damage that might be caused by your processing – whether physical, emotional or material. In particular look at whether the processing could possibly contribute to:

* inability to exercise rights (including but not limited to privacy rights);
* inability to access services or opportunities;
* loss of control over the use of personal data;
* discrimination;
* identity theft or fraud;
* financial loss;
* reputational damage;
* physical harm;
* loss of confidentiality;
* re-identification of pseudonymised data; or
* any other significant economic or social disadvantage

You should include an assessment of the security risks, including sources of risk and the potential impact of each type of breach (including illegitimate access to, modification of or loss of personal data).

To assess whether the risk is a high risk, you need consider both the likelihood and severity of the possible harm. Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk.

You must make an ‘objective assessment’ of the risks. You might find it helpful to use a structured matrix to think about likelihood and severity of risks:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  ^ ^ | Serious harm | Low risk | High risk | High risk |
|  ^ ^ | Some impact | Low risk | Medium risk | High risk |
| Severity of impact | Minimal Impact | Low risk | Low risk | Low risk |
|  |  | Remote | Reasonable Possibility | More likely than not |
|  |  | Likelihood of harm |  >>>>> |  >>>>> |

You might also want to consider corporate risks such as impact of regulatory action, reputational damage or loss of public trust.

# How do we Identify Mitigating Measures?

Against each risk identified, record the source of that risk. You should then consider options for reducing that risk. For example:

* Deciding not to collect certain types of data;
* Reducing the scope of processing;
* Reducing retention periods;
* Taking additional technological security measures;
* Training staff to ensure risks are anticipated and managed;
* Anonymising or pseudonymising data were possible;
* Writing internal guidance or processes to avoid risks;
* Adding a human element to review automated decisions;
* Using different technology;
* Putting clear data sharing agreement sin place;
* Making changes to privacy notices;
* Offering individuals the chance to opt out where appropriate; or
* Implementing new systems to help individuals to exercise their rights.

This is not an exhaustive list, and you may be able to devise other ways to help reduce or avoid the risks. You should consult East Ayrshire Leisure’s Data Controller for advice.

# Further Information

Further information about this policy or arranging training sessions for your Service or teams should be directed to East Ayrshire Leisure’s Data Controller:

Tel : 01563 554057

Email : EALInformationgovernance@eastayrshireleisure.com

Further information is available from:

The ICO guidance on DPIAs at : <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>

#

**Record of Change**

|  |  |
| --- | --- |
| **Date Reviewed** | **Date of next review** |
| Aug 19 | Aug 20 |

# Appendix 1

# Data Protection Impact Assessment – Part 1 Screening Questions

#

|  |  |  |  |
| --- | --- | --- | --- |
| **Service Area** |  | **Team** |  |
| 1. **Do you plan to uses systematic and extensive profiling with significant effects?**
 | Yes [ ]  No [ ]  Unsure [ ] **Comments**  |
| 1. **Do you plan to process special category data to decide on access to services?**
 | Yes [ ]  No [ ]  Unsure [ ] **Comments**  |
| 1. **Do you plan to profile individuals on a large scale?**
 | Yes [ ]  No [ ]  Unsure [ ] **Comments**  |
| 1. **Do you plan to use new technologies?**
 | Yes [ ]  No [ ]  Unsure [ ] **Comments**  |
| 1. **Do you plan to use profiling or special category data to decide on access to services?**
 | Yes [ ]  No [ ]  Unsure [ ] **Comments**  |
| 1. **Do you plan to profile individuals on a large scale?**
 | Yes [ ]  No [ ]  Unsure [ ] **Comments**  |
| 1. **Do you plan to process biometric data?**
 | Yes [ ]  No [ ]  Unsure [ ] **Comments**  |
| 1. **Do you plan to process genetic data?**
 | Yes [ ]  No [ ]  Unsure [ ] **Comments**  |
| 1. **Do you plan to match data or combine datasets from different sources?**
 | Yes [ ]  No [ ]  Unsure [ ] **Comments**  |
| 1. **Do you plan to collect data from a source other than the individual without providing them with a privacy notice (‘invisible processing’)?**
 | Yes [ ]  No [ ]  Unsure [ ] **Comments**  |
| 1. **Do you plan to track individual’s location or behaviour?**
 | Yes [ ]  No [ ]  Unsure [ ] **Comments**  |
| 1. **Do you plan to profile children or target marketing or online services at them?**
 | Yes [ ]  No [ ]  Unsure [ ] **Comments**  |
| 1. **Do you plan to process data that might endanger the individual’s physical health or safety in the event of a security breach?**
 | Yes [ ]  No [ ]  Unsure [ ] **Comments**  |
| **If you have answered NO to all questions you do not need to continue with the DPIA process. Should the scope of the initiative change to incorporate privacy and information risk at a future date you will need to review/amend the screening questions. You must ensure a copy of this is retained within your initiative or project documentation.****Please proceed to Appendix 2 – Data Protection Impact Assessment template if you have answered YES to any of the questions or if you think the processing could result in a high risk to individuals’ privacy. If you are unsure email a copy to East Ayrshire Leisure’s Data Controller with your comments who will provide advice and assistance to you.** |

## **Data Protection Impact Assessment template**

Start to fill out the template at the beginning of any major project involving the use of personal data, or if you are making a significant change to an existing process. Integrate the final outcomes back into your project plan.

|  |
| --- |
| **Step 1: Identify the need for a DPIA** |

|  |
| --- |
| Explain broadly what the 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 to anyone? You might find it useful to refer to a flow diagram or another 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? |
|  |

|  |
| --- |
| **Describe the purpose 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 is 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 the 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, reduced or accepted | Low, medium or high | Yes/no |
| **Step 7: Sign off and record outcomes** |

|  |  |  |
| --- | --- | --- |
| Item | Name/date | Notes |
| Measures approved by: |  | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by the Chief Executive: |  | If accepting any residual high risk, the DPO should be consulted |
| DPIA passed to Data Controller |  | To review and forward to East Ayrshire Council’s DPO |
| 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 be kept under review by: |  | The DPO and Data Controller should review ongoing compliance with DPIA |

|  |  |
| --- | --- |
| DPIA Authorisation (Senior Manager):  |  |
| Name : | Date : |