Data Protection Impact Assessment Protocol

|  |  |  |
| --- | --- | --- |
| Policy Title / Reference | Author | Owner |
| Data Protection Impact Assessment Protocol | Emma Cooper, Cluster DPO (Kafico) | Practice Manager |

|  |  |  |
| --- | --- | --- |
| Version | Revision author | Version comments |
| 1 | Emma Cooper, Kafico Ltd | Jan 19 New Draft |
| 1.1 | Emma Cooper, Kafico Ltd | Jan 19 Jan 19 Replaced 1998 DPA with 2018 Act.  Added DPIA Trigger Checklist Updated from ICO Guidance 2018 |
| 1.2 | Hannah Calway, Kafico Ltd | Aug 19 added information regarding what an DPIA is and when it is needed. Provided new checklist. |

Contents

[2. Scope 2](#_Toc17888271)

[3. Definitions 2](#_Toc17888272)

[4. Introduction 3](#_Toc17888273)

[5. Statutory Mandatory Framework 3](#_Toc17888274)

[6. What is a Data Protection Impact Assessment? 3](#_Toc17888275)

[7. When is a DPIA needed? 3](#_Toc17888276)

[8. How is a DPIA carried out? 3](#_Toc17888277)

[9. Do the ICO need notifying each time a DPIA is carried out? 4](#_Toc17888278)

[10. Accountable Parties 4](#_Toc17888279)

[11. What Processing Elements Should Prompt ***Consideration*** of a DPIA? 4](#_Toc17888280)

[12. What Processing Elements Will Automatically Trigger a DPIA? 5](#_Toc17888281)

[13. Which Elements Will Trigger a DPIA When Combined with One Another? 6](#_Toc17888282)

[14. DPIA Trigger Checklist 6](#_Toc17888283)

[15. Information Incidents 6](#_Toc17888284)

[16. Associated Protocols 6](#_Toc17888285)

[17. Audit Schedule 7](#_Toc17888286)

[18. Review 7](#_Toc17888287)

# Scope

This protocol has been drafted for use by customers of Kafico Ltd across Suffolk.

At the time of writing and unless alternative protocols have been adopted locally, the protocol applies to;

|  |  |  |
| --- | --- | --- |
| Barrack Lane | Martlesham | Mendlesham |
| Burlington Road | Ravenswood | Wickhambrook |
| Framlingham | Stanton (west) | Church Farm Surgery (Aldeburgh) |
| Botesdale Health Centre | The Birches | Framfield |
| Felixstowe Road | Mount Farm | Saxmundham |
| Hawthorn Drive | Swan and Forest | Guildhall & Barrow |
| The Surgery, Leiston | Glemsford | Peninsula |
| Victoria Surgery | Lakenheath | Little St John Street |
| Ivry Street | Ixworth | Grove Medical Centre |

# Definitions

**Personal Confidential Information** This term is intended to cover information captured by the Data Protection Act 2018 / GDPR (identifiable information about the living), information covered by the Common Law Duty of Confidence / Tort of Misuse of Private Information and finally, information covered by Article 8 European Convention for Human Rights.

# Introduction

This protocol intends to support **Practice** staff in managing the impact of change on the privacy of patients, employees and other stakeholders by providing a systematic process by which the complex legislation might be navigated and documented. This protocol should be embedded into The **Practice**’s Change Management Process.

# Statutory Mandatory Framework

Data Protection Impact Assessments are required by law in accordance with the General Data Protection Regulations for certain activities deemed to have an impact on the rights and freedoms of the individuals concerned.

The process of completing a DPIA can be complex and require specialist skills and so will usually be completed by the Data Protection Officer. This protocol acts as a precursor to a full DPIA and allows The **Practice** to determine whether the change being considered warrants a full DPIA and gives an indication of the types of risks involved and mitigations to be put in place.

# What is a Data Protection Impact Assessment?

A Data Protection Impact Assessment (DPIA for short) is used as a living document that ensures any new process being considered that is likely to result in a high risk to the rights of data subjects has gone through a thorough screening that aids in mitigating risks and weighing the risks against the outcome.

# When is a DPIA needed?

There are different times when a DPIA is needed. Both the ICO and the European Data Protection Board (EDPB) have issued guidance on this. We have outlined a table below that should be used as an initial determination of whether a DPIA is needed. If the answers are inconclusive an initial DPIA should be conducted to make a determination.

# How is a DPIA carried out?

A DPIA must start before the processing begins to ensure there is a legitimate gateway to be able to process the data. If the DPIA highlights mitigations these must be considered before starting the projects, if they cannot be mitigated or the risk is still too high a risk to the data subjects then the project cannot go ahead until the ICO are consulted. Your DPO, if you have one, must be involved in the DPIA and even once the project is up and running the DPIA should sit beside it and update as the project updates to ensure continuous compliance with the data protection legislation and ICO guidance.

# Do the ICO need notifying each time a DPIA is carried out?

No, the ICO only expect to be notified when there is a high risk to individuals and there are no measures that can be taken to mitigate these risks. Where the ICO must be consulted the DPIA would be sent to them, this is one of the reasons it is important to ensure a complete and comprehensive DPIA is completed from the outset. It will help to avoid delays and requests for more information whilst they make a decision. The processing cannot begin until the ICO have responded. They either advise that the risks are acceptable, suggest further action or advise that carrying out the processing would put you in breach of GDPR. In some cases they are able to issue formal notices and / or take action to ban the processing altogether.

# Accountable Parties

See Information Governance Policy for key roles.

All staff, whether management or administrative, who create, receive and use Personal Confidential Information have responsibilities to ensure effective reporting and management of information risk for The **Practice** . Employees have a contractual and legal obligation to read and comply with all company policies and to attend mandatory training to support the appropriate management of information.

# What Processing Elements Should Prompt ***Consideration*** of a DPIA?

* 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

# What Processing Elements Will Automatically Trigger a DPIA?

The following activities, without needing to be combined with other risk factors, should always trigger a Data Protection Impact Assessment;

 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]](#footnote-1)

 Processing on a large scale[[2]](#footnote-2) of special categories of data or of personal data relating to criminal convictions and offences

 Systematic monitoring of a publicly accessible area on a large scale

 Use profiling, automated decision-making or special category data to help make decisions on someone’s access to a service, opportunity or benefit

 Processing on a large scale

 Combine, compare or match data from multiple sources

 Process children’s personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them

 Process personal data that could result in a risk of physical harm in the event of a security breach

# Which Elements Will Trigger a DPIA When Combined with One Another?

* processing biometric or genetic data[[3]](#footnote-3)
* use innovative technology[[4]](#footnote-4)
* Process personal data without providing a privacy notice directly to the individual
* Process personal data in a way that involves tracking individuals’ online or offline location or behaviour

# DPIA Trigger Checklist

Before embarking on a new project, initiative or change, staff should complete the checklist at Appendix A andsend to the Data Protection Officer for review.

Please be aware that the DPO is required to apply pseudonymisation techniques were possible to satisfy Privacy by Design requirements.

The checklist should be completed as fully as possible to allow the DPO to make the necessary determinations.

The trigger checklist is informed by the ICO Guidance and the European Data Protection Board decision.[[5]](#footnote-5)

# Information Incidents

Any suspected or actual incidents involving Personal Confidential Information must be reported immediately in line with the Information Incident Protocol.

# Associated Protocols

This protocol should be read in conjunction with;

* Risk Management Policy
* Change Management Policy
* Information Governance Policy
* Information Rights and Access Protocol
* Information Sharing and Privacy Protocol
* Information Lifecycle and Data Quality Protocol
* Information / Cyber Security Protocol
* Information Incident Protocol
* Information Risk and Audit Protocol
* Freedom of Information Protocol

# Audit Schedule

Outcomes of the Data Protection Impact Assessment will be fed into the Plan, Do, Check, Act cycle as referenced in the Information Risk and Audit Protocol.

# Review

This protocol will be reviewed every year or sooner where necessary

**Appendix A**

|  |  |
| --- | --- |
| If you tick **any** of the sections below, the DPO should ***consider*** a DPIA. |  |
| 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 you tick **any** of the sections below, the project requires a DPIA. |  |
| 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 on a large scale of special categories of data or of personal data relating to criminal convictions and offences |  |
| Systematic monitoring of a publicly accessible area on a large scale |  |
| Use profiling, automated decision-making or special category data to help make decisions on someone’s access to a service, opportunity or benefit |  |
| Combine, compare or match data from multiple sources |  |
| Process children’s personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them |  |
| Process personal data that could result in a risk of physical harm in the event of a security breach |  |

|  |  |
| --- | --- |
| If you tick **TWO** of the sections below, the project requires a DPIA. |  |
| Processing biometric or genetic data[[1]](file:///C:/Users/etz/Downloads/IG06%20Data%20Protection%20Impact%20Assessment.docx#_ftn1) |  |
| Use of innovative technology[[2]](file:///C:/Users/etz/Downloads/IG06%20Data%20Protection%20Impact%20Assessment.docx#_ftn2) |  |
| Processing personal data without providing a privacy notice directly to the individual |  |
| Processing personal data in a way that involves tracking individuals’ online or offline location or behaviour |  |

1. the decision must have a serious negative impact on an individual. A legal effect is something that adversely affects someone’s legal rights and significant effects would include automatic refusal of an online credit application, and e-recruiting practices without human intervention. [↑](#footnote-ref-1)
2. Large scale processing is not defined within GDPR but some examples are given within WP243 ANNEX. Processing of patient data in the regular course of business by a hospital ***would*** be considered large scale however, processing of patient data by an individual physician ***would not*** be considered large scale. [↑](#footnote-ref-2)
3. DNA, facial images, fingerprints, tissue samples [↑](#footnote-ref-3)
4. Artificial intelligence, machine learning and deep learning; connected and autonomous vehicles; intelligent transport systems; smart technologies (including wearables); market research involving neuro-measurement (e.g. emotional response analysis and brain activity); some ‘internet of things’ applications, depending on the specific circumstances of the processing. [↑](#footnote-ref-4)
5. https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion\_2018\_art.\_64\_gr\_sas\_dpia\_list\_en.pdf [↑](#footnote-ref-5)