Rescon Ltd
Data Protection Impact Assessment (DPIA) Procedure

Revision History

Version	Revision Date	Summary of Changes	Author
1.0	23/08/2018	Document creation	Tom Dawson

Table of Contents

1. Introduction

Data Protection Impact Assessments (DPIA) help to identify and minimise the data protection risks of a project. DPIAs must be completed for all processing that is likely to result in a high risk to individuals including:

- Use systematic and extensive profiling with significant effects;
- Process special category or criminal offence data on a large scale; or
- Systematically monitor publicly accessible places on a large scale;
- Use new technologies;
- Use profiling or special category data to decide on access to services;
- Profile individuals on a large scale;
- Process biometric data;
- Process genetic data;
- Match data or combine datasets from different sources;
- Collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- Track individuals' location or behaviour;
- Profile children or target marketing or online services at them; or
- Process data that might endanger the individual's physical health or safety in the event of a security breach.

Failure to embed appropriate data protection measures may breach data security and protection laws.

This document will help to identify and address data protection concerns at the design and development stage and details the process for conducting a DPIA to ensure risks are identified and mitigated appropriately.

2. Scope

This document sets out the DPIA process which is required for all processing that is likely to result in a high risk to individuals, with the aim to identify new risks that may not have an associated mitigation.

A basic DPIA (see Appendix) must be completed for all developments or platform releases to identify whether a full DPIA is needed. DPIAs must be completed alongside Privacy Impact Assessments (PIA) and Change Control documentation.

3. Responsibilities

The person responsible for delivering the proposed project or change to the system is response for completing the DPIA.

The Data Protection Officer (DPO) must be involved and consulted when a DPIA is carried out.

The Information Governance Committee are responsible for overseeing the completion, assessment and outcomes of the DPIA.

The Caldicott Guardian is responsible for filing the completed DPIAs.

4. DPIA

A basic DPIA must be completed to identify whether there may be a high risk to individuals. If the basic DPIA identifies a potential area of risk, a full DPIA must be completed.

The basic DPIA involves initial screening questions and must be completed by the person responsible for delivering the proposed project or change to the system (see Appendix). The basic DPIA will be reviewed and will result in one of the following:

1. The screening process has not identified any DPIA concerns – the process is complete
2. If the answer to any question if 'yes', a full DPIA must be completed

The full DPIA helps to identify and address data protection concerns and ensure risks are identified, assessed, mitigated and of acceptable risk. There are seven stages to the full DPIA (see Appendix). All stages must be completed.

The DPO must be consulted as a matter of routine when a DPIA is carried out.

The Information Commissioners Office (ICO) must be consulted where a DPIA indicates high risk to individual rights and freedoms that cannot be mitigated. The ICO will provide advice within eight weeks, or 14 weeks for complex cases.

DPIAs must be published as part of transparency material, with any sensitive information redacted prior to publication.

Completed and reviewed DPIAs must be sent to adie@rescon.eu for filing.

5. Review & Monitoring

This policy must be reviewed and approved at least annually. Compliance with the DPIA will be monitored through audits and review by the Information Governance Committee.

6. Approval

This DPIA procedure has been reviewed and approved by the Information Governance Lead.

Name: Tom Dawson

Position: Managing Director and Information Governance Lead

Date: 06/09/2018

Signature:

Appendix A: DPIA

Basic DPIA

Answering yes to any of these questions represents a potential risk that requires full DPIA completion to ensure risks are identified, assessed, mitigated and of acceptable risk.

Stage 1 – Basic Assessment

Does this data processing activity:

	Yes	**No**
Use systematic and extensive profiling with significant effects		
Process special category or criminal offence data on a large scale		
Systematically monitor publicly accessible places on a large scale		
Use new technologies		
Use profiling or special category data to decide on access to services		
Profile individuals on a large scale		
Process biometric data		
Process genetic data		
Match data or combine datasets from different sources		
Collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')		
Track individuals' location or behaviour		
Profile children or target marketing or online services at them		
Process data that might endanger the individual's physical health or safety in the event of a security breach		

If you have answered yes to any of these questions a full DPIA must be completed.

Full DPIA

Stage 1 – Identify need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. Summarise the need for a full DPIA.

Stage 2 – Describe the processing

Describe the nature of the processing. How will it be collected, used, stored and deleted? What is the source of the data? Will the data be shared with anyone? Use a data flow diagram where possible. What types of processing are identified as high risk?

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 be collected and used? How often? How long will it be kept? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing. What is the nature of the relationship with the individuals? How much control will they have? Would they expect the data to be used 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 should be factored in? Are there any approved code of conduct or certification schemes that have been applied to?

Describe the purposes of the processing. What do we want to achieve? What is the intended effect on individuals? What are the benefits of the processing?

Stage 3 – Consider consultation

Consider how to consult with relevant stakeholders. Describe when and how to seek individuals views – or justify why it is not appropriate to do so. Who else needs to be involved? Do processors need to assist? Do information security experts or any other experts need to be consulted?

Stage 4 – Access necessity and proportionality

Describe compliance and proportionality measures. What is the lawful basis for processing? Does the processing achieve the purpose? Is there another way to achieve the same outcome? How will function creep be prevented? How will data quality and data minimization be ensured? What information will be given to individuals? How will we help to support their rights? What measures will be taken to ensure processors comply? How will international transfers be safeguarded?

Stage 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** Remote, possible or probable	**Severity of harm** Minimal, significant, severe	**Overall risk** Low, medium, high

Stage 6 – Identify measures to mitigate risk

Identify additional measures that could be taken to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk** Eliminated, reduced, accepted	**Residual risk** Low, medium, high	**Measure approved?** Yes/No

The Information Commissioners Office (ICO) must be consulted where a DPIA indicates high risk to individual rights and freedoms that cannot be mitigated

Stage 7 – Sign off and record outcomes

Item	**Name/Date**	**Notes**
Measures approved by:		Integrate actions 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

DPI advice provided:		DPO must advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, explain reasons why
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Are there unmitigated risks? If yes, have the ICO been notified?		The Information Commissioners Office (ICO) must be consulted where a DPIA indicates high risk to individual rights and freedoms that cannot be mitigated
Comments:		
This DPIA will be kept under review by:		The DPO must also review ongoing compliance with DPIA

Please send the completed DPIA to adie@rescon.eu