ARK- Guidance on when to complete a Data Protection Impact Assessment (DPIA)

A DPIA is a process to help you identify and minimise the data protection risks of a project or piece of work. You **must** complete a DPIA for processing that is **likely to result in a high risk to individuals**. Examples include where we plan to:

- Process special category data (racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, sex life and sexual orientation) or criminal offence data, on a large scale;
- Use new technologies;
- Carry out profiling on a large scale;
- Process personal data without providing a privacy notice directly to the individual;
- Process personal data in a way which involves tracking individuals' online or offline location or behaviour; or
- Process personal data which could result in a risk of physical harm in the event of a security breach.

It is also good practice to complete a DPIA for any other major project or big piece of work which requires the processing of personal data. Examples include where we plan to carry out:

- Any major project involving the use of personal data or processing on a large scale;
- Processing of sensitive data or data of a highly personal nature;
- Processing of data concerning vulnerable data subjects;
- Innovative technological or organisational solutions; or
- Processing involving preventing data subjects from exercising a right or using a service or contract.

In practice, if you are planning a new piece of work which will involve processing personal data, or you are reviewing a policy/ procedure and you think that there may be potential risks associated with the policy area in relation to personal data, please contact ARK's Data Protection Officer to discuss, and to obtain advice on how to proceed: dataprotection@arkha.org.uk or Kelly.Patterson@arkha.org.uk, 0131 478 8177.

Once you have discussed the issue, the Data Protection Officer will, if necessary support you to complete a DPIA, using the template on the following pages.

ARK Data Protection Impact Assessment (DPIA)

This template is based on the template produced by the Information Commissioner's Office.
Where you identify the need to complete a DPIA, you should start to fill out the template at the **start** of any project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes and any actions should be integrated back into the relevant project/ action plan.

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.
This activity involved the development of a Policy and Procedure to support ARK to comply with the requirements of the Freedom of Information (Scotland) Act 2002 ('FOISA') and the Environmental Information (Scotland) Regulations 2004 ('EIR'). In order to meet the requirements of FOISA and EIR, we will require to: • Publish information in a Guide to Information, in accordance with the Model Publication Scheme set out by the Scottish Information Commissioner • Respond to information requests from members of the public ARK has identified the need for a DPIA on the basis that, in relation to our Guide to Information publications, or as part of an information request, it may be necessary to process personal data, and there may be risks associated with sharing or publishing personal data without lawful basis.

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?
The personal data processed in relation to ARK's duty to publish, and responding to information requests, will be data which ARK already processes. The source will potentially be any data subject associated with ARK's RSL function. It is not proposed that any of the data processed in relation to ARK's guide to information, or requests for information, will be shared with third parties, other than senior employee and Board member data, which specifically requires to be published in order to meet the relevant legal requirements.

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?
The data will be personal data and potentially special category data. It is anticipated that there would be a low to medium volume of data processed in order to meet ARK's responsibilities in relation to the duty to publish, and to respond to requests for information.

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)?
In terms of context, a proportion of the personal data ARK processes in relation to FOISA/EIR may relate to those in vulnerable groups (ie adults with learning disability) and the expectation of these individuals would be that ARK would not publish or share such personal data without an appropriate lawful basis.

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?
The purpose will be to support with ARK's legal obligation to comply with FOISA/ EIR, whilst balancing those obligations with ARK's responsibilities under GDPR.

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?
Notwithstanding that potential risks have been identified in relation to this processing (see below), ARK will not publish or share personal data under any circumstances without lawful basis, and therefore it is not proposed that consultation should be undertaken in this case.

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?
Processing will only take place to the extent required to comply with ARK's responsibilities in relation to FOISA/EIR whilst ensuring that ARK also acts in accordance with data subjects' rights in terms of the GDPR, and more particularly the lawful basis of meeting ARK's legal obligations in relation to FOISA and EIR.

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: Remote, possible or probable**	**Severity of harm: Minimal, significant or severe**	**Overall risk: Low, medium or high**
1. Risk that personal data will be published in ARK's Guide to Information with no lawful basis	possible	significant	Medium
2. Risk that personal data will be released in relation to a request for information with no lawful basis	Possible	significant	Medium

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: Eliminated reduced accepted**	**Residual risk: Low medium high**	**Measure approved: Yes/no**
1.	Ensure that all relevant functions are clear that personal data should not be published. Ensure involvement by ARK's DPO in reviewing materials for publishing in terms of the Guide to Information.	Reduced	Low	Yes
2.	Ensure oversight and review by ARK's DPO in relation to information requests, and that specific advice and guidance is obtained where a request potentially involves the release of information which contains personal data. Where personal data is included in information which will require to be released as part of an information request, and there is no lawful basis for sharing that personal data, the relevant information will be redacted prior to sharing.	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	John Rankin (03.10.19)	Integrate actions back into any relevant project plan, with date and responsibility for completion
Residual risks approved by:	John Rankin (03.10.19)	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Kelly Patterson (03.10.19)	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: DPO has reviewed the draft DPIA and is in agreement with its terms.		
DPO advice accepted or overruled by:	Accepted by John Rankin (03.10.19)	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	n/a	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	John Rankin and Kelly Patterson	The DPO should also review ongoing compliance with DPIA