Sample DPIA template

This template is an example of how Acas needs you to record your DPIA process and outcome. It follows the process set out in DPIA guidance provided by the Information Commissioner's Office, and summarised for you here.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	Advisory Conciliation and Arbitration Service (Acas)
Subject	Analysing Helpline data
Name of controller contact	TBC

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.
Because the supplier will be joint controller and processing Acas data *This project involves a third party supplier sourcing contact data to market to. It also involves some sharing of Acas customer contact data from Acas to the supplier in order to de-dupe records for marketing. Data will be for those contacts signed up to receive Acas comms.*

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?
We will be sharing data with the supplier to de-dupe against new rented lists (to ensure we are not paying for contacts we already have). *Data will be extracted from our databases and stored on the supplier's databases during this project.* *We will periodically (eg monthly/qtly) provide an update on new contacts subscribed to Acas through this process. Again, extracting from our databases and sending to the supplier.*

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?
Email addresses (business) – no special categories apply

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)?
No special categories of data Rented records will include: • Contact Name • Job title • E-mail address • Org size (no of employees) • SIC/Business classification • Permissions for use • List source

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?
Benefits are cost savings – by not rented data we already hold

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?

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?
Acas data is opted-in contacts – agreeing to receive comms from Acas

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**	**Severity of harm**	**Overall risk**
In the event of loss of Acas data we envisage low impact as we will retain records on our system.	Remote,	Minimal,	Low,

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**
Loss of Acas records	Acas will retain records in their systems	accepted	Low	Yes

Step 7: Sign off and record outcomes

Item	**Name/position/date**	**Notes**
Measures approved by:	Mark Faulkner	
Residual risks approved by:	Mark Faulkner	
DPO advice provided:	yes	
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 kept under review by:		The DPO should also review ongoing compliance with DPIA