Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

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	Takki Sulaiman
Title of DPO	Chief Executive
Name of DPO	Takki Sulaiman

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.
The project is intended to be an online tool for Third Sector Organisations to record digitally purchasers of raffle tickets name and contact details. This involves collecting name and telephone numbers and storing them in an encrypted database for the duration of the raffle. There is a need for a DPIA due to collecting personal data and storing for a set amount of time.

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?
Third Sector Organisations will collect the data and using the online interface, will load it into the database in an encrypted format. The data is stored until 1 month after the raffle has closed to provide ample time to contact winners and is then automatically deleted. Third Sector Organisations have the ability to purge the data prior to this if required. The data will not be shared with anyone out with the initiated organisation. We have identified this as low 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 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 consist of the purchasers name and telephone number or email based on preference. There is no special category data recorded. The amount of data collected is dependent on the amount of raffle tickets purchased, not likely to be more than 3000 individuals and will depend on the organisations fundraising activity. The data is stored until 1 month after the raffle has closed to provide ample time to contact winners and is then automatically deleted. This online tool has been created for the use of organisations in Argyll & Bute.

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)?
The Argyll & Bute Third Sector Interface (the provider of the service) will hold a third party relationship with the individuals in that we hold the database but organisations control the data. The purchasers are providing their information and are aware of the purpose when doing so. They are given the option to approve the data being held in this way prior to purchase. It is possible that children and vulnerable groups will have access to the raffle tickets but the risk is low due to the data being encrypted and a time of deletion being set. There are no concerns with the processing as the site being used has SSL and encrypted data. The Argyll & Bute Third Sector Interface are members of the ICO.

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?
There are no benefits for the TSI in processing the data, we are providing a service only. The intended effect on individuals is that they are entering a raffle to win a prize and support the local third sector organisations.

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?
There will be bery low level impact on stakeholders so this is not required.

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?
As mentioned above, the TSI is only the provider of the service and will have nothing to do with the collection of the data only the storage and this data will not be available to anyone other than the winning details from the raffle. The organisations will not have access to the full data which will prevent function creep.

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**
Risk of website security – mitigated by the site having SSL	Remote	Minimal	Low
Data security – mitigated by encryption of data	Remote	Minimal	Low
Length of storage of the data – automatic deletion of all data 1 month post raffle end with option to delete prior.	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**
Risk of website security	mitigated by the site having SSL	reduced	Low	Yes
Data security	mitigated by encryption of data	reduced	Low	Yes
Length of storage of the data	automatic deletion of all data 1 month post raffle end with option to delete prior.	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	Takki Sulaiman, CEO, 13/12/22	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Takki Sulaiman, CEO, 13/12/22	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Takki Sulaiman, CEO, 13/12/22	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Ensure site has security and data is encrypted.		
DPO advice accepted or overruled by:	Lauren Martin and Phil Ashby	If overruled, you must explain your reasons
Comments: This was actioned.		
Consultation responses reviewed by:	N/A	If your decision departs from individuals' views, you must explain your reasons
Comments:N/A		
This DPIA will kept under review by:	Takki Sulaiman	The DPO should also review ongoing compliance with DPIA