ABU DHABI GLOBAL MARKET

Sample DPIA template

This template is an example of how you can record your DPIA process and outcome.

You should start to fill out the template prior to the commencement of any major project which involves the processing of personal data, or if you are making a material change to an existing process which involves the use of personal data. Any mitigation strategies identified at Stage 6 of the DPIA should be actioned accordingly when rolling out the project or implementing the change to the existing process.

When completing this DPIA template use plain English and define any industry specific terminology.

Controller Information

Name of controller	
Name of controller contact /DPO (delete as appropriate)	

Stage 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing activities it involves (e.g. Storage, sharing, comparing, combining, matching, cross referencing with third party data sources, using for marketing purposes, etc.). You may find it useful to refer or link to other documents, such as a project proposal, any applicable privacy notices, data flow diagram or third party processor documentation which describes how personal data is used by such a third party and the measures which that third party has in place to mitigate risk. Following that, summarise why you identified the need for a DPIA.

Stage 2: Description of processing

Nature of the processing How will you collect, use, store and delete the personal data in scope? Provide details of any systems used (both internal and third party). What is the source of the data? (e.g. Did you collect it directly from data subjects or did it come from a third party? If a third party, where is that third party located and how did they collect it?) Will you be sharing data with anyone? (Consider both internal and external data sharing) Are any high risk processing activities involved?

Scope of Processing
What is the nature of the data? (e.g. Contact information, financial information, biometric information, etc.) Does it include special category or criminal offence data? How much data will you be collecting and using? (Consider both the number of data subjects and the number of data points in relation to each data subject) How often will data be collected and refreshed? How long will you keep it once collected? Where are the data subjects located?

Context of Processing

What is the nature of your relationship with the individuals? (e.g. are they employees, candidates, customers, supplier representatives?)

How much control will they have over your use of their data?

Would they expect you to use their data in this way or is it an usual use case?

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? For example, will the processing involve AI or Blockchain technologies? What is the current state of technology in this area and where are any third party providers positioned in terms of expertise and experience?

Are there any current issues of public concern that you should factor in?

Are you or any relevant processors signed up to any approved code of conduct or certification scheme (once any have been approved by the Commissioner)?

Purposes of Processing

What are you seeking to achieve? Do you really need all of the personal data in identifiable form?

What is the intended effect on individuals?

What are the benefits of the processing for:

- You
- Data Subjects
- Third Parties
- Society

Stage 3: Consultation process

Stakeholder Consultation Identify stakeholders (e.g. Data subjects, those who will use the systems internally, privacy champions, third party processors, IT security experts, other experts in the field) Detail how and when you will seek their views, or describe why this is not appropriate or possible in each case.

Stage 4: Assess necessity and proportionality

Necessity and proportionality

What is your lawful basis for processing? (Refer to the lawful bases available under the DPR 2021)

Does the processing actually achieve your purpose? If so, is there another way to achieve the same outcome without collecting personal data, collecting less personal data or anonymizing or pseudonymizing personal data post collection?

How will you prevent function creep? (e.g. Will only limited individuals in the organisation have access?)

How will you ensure data quality and data minimisation? (e.g. Is there a self serve function to update personal data for data subjects? Are data collection fields closed rather than open?)

What information will you give individuals? (Does your Privacy Notice need updating?)

How will you help to support their rights? (Are the systems connected to any tools used to give effect to requests, including erasure requests, from data subjects?)

What measures do you take to ensure processors comply? (e.g. Contractual provisions, audits?)

How do you safeguard any international transfers? (e.g. use of Standard Contractual Clauses)

Stage 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Describe any associated compliance and corporate risks as necessary. For examples, please refer to paragraph 4.2 of Part 4 of the Guidance.	**Likelihood of harm (Choose one)**	**Severity of harm (Choose one)**	**Overall risk (Choose one)**
	• Remote • Possible • Probable	• Minimal • Significant • Severe	• Low • Medium • High

Stage 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in stage 5				
Risk	**Potential measures to reduce or eliminate risk** For examples, please refer to paragraph 4.2 of Part 4 of the Guidance.	**Effect on risk (choose one)**	**Residual risk (choose one)**	**Measure approved (Y/N)**
		• Eliminated • Reduced • Accepted	• Low • Medium • High	• Yes • No

Stage 7: Sign off and record outcomes

	Name/position/date	Notes
Mitigation steps approved by:		Integrate actions back into project plan, with date and clear responsibility for action
Residual risks approved by:		If accepting any residual high risk, consult the Commissioner before proceeding
DPO advice provided:		DPO should advise on compliance, Stage 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice reviewed by:		
Comments (including if any element of the advice was not followed):		
Consultation responses reviewed by:		If your decision departs from views expressed by stakeholders during consultation, explain your reasons
Comments:		
This DPIA will kept under review by:		Include a timetable for review The DPO should also review ongoing compliance with DPIA