DPIA Report

This report is built on the guidelines of GDPR and follows the same format.

Overview

Name of the Organization	Capgemini
Project Name	DPIA
Date	2022-06-06
Name of Data Protection Officer	Smith Williamson
Name of Data Owner	Head

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.
For this scope of service , the project lead defines the purpose of processing the data.The project team analyzes the purpose of processing and then collectively decide the aim of the project.At present , basic research is done before finalizing the method of processing data.Expected benefits from processing data is well defined by the project lead and also documented in the report.The project lead sends a meassage to all the concerned departments about the benefits and documents the list of departments in the report.There is no such process to capture the list of team members involved in this data processing.

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?

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?

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)?

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?

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?
The legal basis for processing are - *** Select all from the list ; separate by comma if more than 1 *** For this scope of service , our organization recommends project lead to define the legality of data processing. No, The data processing will not achieve the desired goals.No, we do not have any alternate approach to achieve the same outcome. We explore a couple of more approaches to achieve the same results. All these approaches are documented in the final report. Project lead decided the list of KPI's which will be used to monitor data quality and integrity for this specific scope of service. Data Subjects are informed about the intent of processing data. Our processes related to data subject rights recommends the data processing team to uphold these rights and aim for complete compliance. We have a robust process to monitor the compliance of the designated processing entitie which aims to achieve full compliance. We make sure that we stick to the decided scope of service and have no deviations from it while processing. We do not accept any out of scope requirements and prevent any function creep.We have a process which ensures that we do not deviate from the decided scope of service while processing data.We have well defined controls in place to ensure that data processors are aware about the scope of service and they comply by them.There is no measures defined to safegaurd any international transfer of the data.

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**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

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**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back 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
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
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