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	Grupo 1
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

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.

Our project consists in developing an application that, given information about the preferences of a user and his location, suggests the best near spot for a visit.

The application is accessible with a login that asks for a user id, a user password and a user mail.

Having that data processed, the next step for the user is to answer simple questions about his tastes, like food taste, nights club preference, age and hobbies, etc. Beside that, the user will also be asked about his usual locations and to give the current location as well.

There's a need for a DPIA because the app will be dealing with highly sensitive data about the users and a systematic monitoring is important.

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 collection of data is going to be made through some questions in the application.
Data will only be used to give real time advices, suggestions and recommendations of places.
The source of data will be the user itself. And will not be shared with anyone else also than the administrator of the app and the personal user.

The main risk processing this kind of data is in the login and the introduction of the location.

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?

This data has personal nature and only.

It will be collected as much information as the user finds appropriate to have the maximum benefit with the application. All the information that is given by the user will be used to give him the best experience and the best recommendations.

There'll be suggestions of places every time the user is with is Wi-Fi or mobile data on and near places that he might believe useful.

Data will be kept by us – on the application – as long as the user has his account available. That meaning that, once the user doesn't want to use again the application and wants to disable or delete his account, data will no longer be used by us.

The only individual affected will be the user and, geographically speaking, all areas are covered by the application… meaning there's also a map in the app.

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)?

As administrators of the app, we don’t have any kind of relationship with the individuals that sign in the app, other than give advices and let the algorithm do its work.

They’ll only have control in give the preferences and answers or introduce more details about their surroundings.

There’s no limit or low bound of ages, so children and other vulnerable group can access to this application.

Security flaws are plausible and possible, once it’s everything processed online.

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 main propose is to give the users the best accommodation and experience in their daily lives.

As administrators, there’s no type of benefit with this data processing.

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?

The only thing of outsiders we may need is access to maps that are updated, like google maps or something. Given this fact, we will only have a contract whit this company so that we can use their maps. No more information from the outside is needed, nor this company will have access to data that is introduced by user.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing 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?

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

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

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