

# 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 13 EngSeg
Subject/title of DPO	MyMBWay
Name of controller contact /DPO (delete as appropriate)	Grupo 13

## 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.

Este projeto tem como objetivo uma aplicação idêntica ao MB Way, onde os clientes são capazes de consultar o saldo, fazer transferências e pagamentos bancários ou pagar contas em estabelecimentos físicos através da aplicação mobile.

Assim, o projeto fica com os dados bancários dos seus clientes, bem como uma lista de transações por eles efetuadas.

Vai então processar um número elevado de dados pessoais referentes a uma margem considerável da população, já que qualquer proprietário de um cartão de multibanco, crédito ou débito faz parte do alvo da aplicação.

Para apresentar a lista de transferências, o sistema vai também monitorizar automaticamente todas as transações dos clientes.

## 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?

A informação vai ser recolhida automaticamente a partir do momento que alguma Acção é efetuada graças à API do sistema dos bancos. Essa informação vem protegida e fica armazenada no sistema da aplicação, e só é visualizada pelos clientes, que só podem ver a parte recorrente à sua informação.

**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?

A informação guardada vai ser referente a tudo incluído numa conta bancária, seja referências, lista de transações, montante presente na conta e dados sobre o cliente, como nome, morada e idade.

A informação do cliente e da conta vai ser recolhida no momento da criação da conta na aplicação, e a informação das transferências sempre que uma ocorrer.

O sistema deverá guardar todos estes dados até que o cliente decida anular a conta, podendo claro alterar os dados referentes a si próprio.

Em termos de área geográfica, esperamos abranger todo o país, incluindo as regiões autónomas da Madeira e dos Açores.

**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)?

Os elementos que tratarão do sistema do projeto não deverão ter acesso à informação dos clientes, apenas asseguram o bom funcionamento da aplicação.

Toda a informação relacionada com o tratamento dos dados será posta à disposição do público, assegurando o bom tratamento do mesmo. Como a aplicação necessita de um cartão bancário, apenas adultos terão oportunidade de a usar.

Já havendo aplicações que fazem o mesmo que este projeto, mas em separado, a tecnologia não será totalmente inovadora ou inédita.

**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?

Com este projeto espera-se facilitar o acesso e uso de cartões para os mais diversos usos, possibilitando aos clientes evitar deslocações a caixas multibanco ou estabelecimentos semelhantes.

Não haverá benefícios diretos para nós baseados no processamento da informação.

## 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?

Não será preciso obter opinião dos clientes, visto este não ser um projeto de recomendação.

Trataremos de assegurar a segurança das consultas de informação.

## 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?

Sem a extração dos dados das transferências a aplicação perdia uma funcionalidade vital, não havendo alternativa capaz de contornar esse problema.

Encryptando a informação que chega ao servidor asseguramos que apenas aqueles com permissão para ver os dados o fazem. Para além disso, extraímos apenas a informação que interessa para satisfazer as funcionalidades previstas.

## Step 5: Identify and assess risks

<b>Describe source of risk and nature of potential impact on individuals.</b> Include associated compliance and corporate risks as necessary.	<b>Likelihood of harm</b>	<b>Severity of harm</b>	<b>Overall risk</b>
	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