

# 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.

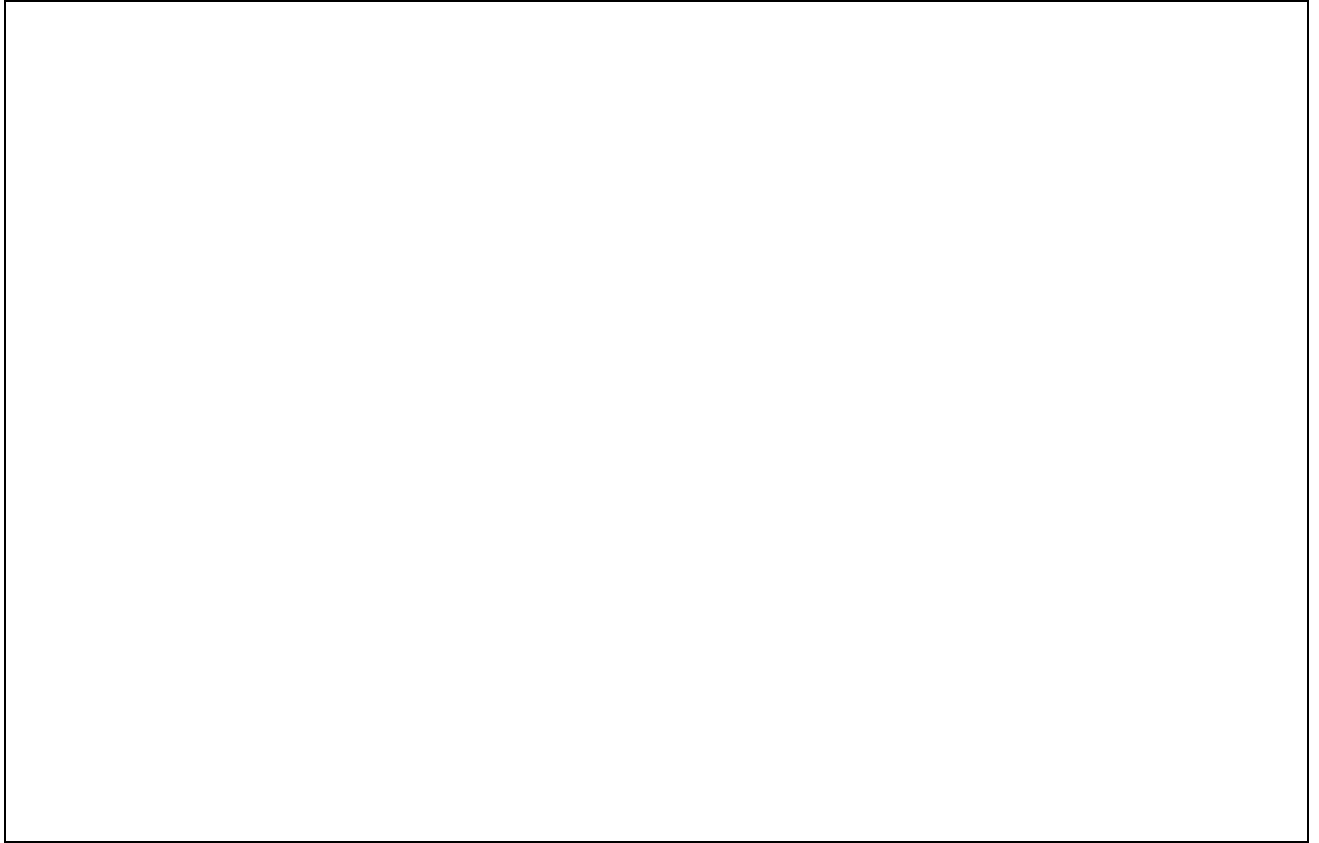
You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

## 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.

Imaginemos que estávamos a iniciar um projeto que tinha como principal intuito desenvolver um site que envolvia a utilização de dados pessoais cujo processamento resulta num risco elevado. O objetivo deste site seria informar os utilizadores que estivessem registados no mesmo sobre os estados da meteorologia. Para tal existem alguns dados que seriam necessário para o fornecimento da informação meteorológica, nomeadamente:

- Nome do utilizador;
- Morada do utilizador (região geográfica);
- Endereço de email;
- Dados bancários (A informação enviada iria ter custos);
- Pagamentos mensais através de paypal ou cartão de crédito



## 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?

- Vamos adquirir os dados através de um formulário, no ato de registo.
- Uso será destinado à identificação da localização geográfica do utilizador;
- Os dados não serão partilhados com mais nenhuma identidade;
- Os tipos de processamento identificados como provável alto risco estão no facto no formulário de introdução de dados de pagamento (pode alguém ler os dados) e no processamento de pagamentos mensais.

**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?

- Dados pedidos: nome, email, informação geográfica e dados de pagamento;
- Estes dados só são pedidos no momento do registo;
- A informação geográfica é consultada todos os dias;
- A informação de pagamento é consultada mensalmente;
- O número de indivíduos são o número de pessoas que se registarem;
- A área que é abrangida correspondente aos utilizadores que se registam;
- Todos os dados serão mantidos na base de dados até o cliente decidir terminar a conta.

**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)?

- Não existe nenhuma relação com os clientes, desde que sejam com idade superior a 18 anos, qualquer pessoa pode-se registar no site;
- Existem preocupações sobre este tipo de processamento de dados e eventuais falhas de segurança;

**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?

- O efeito pretendido sobre os indivíduos é que seja uma entrega diária informativa sobre as condições meteorológicas.

## 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?

- Todo o sistema será autónomo sem intervenção humana;
- Vai ser necessário que o sistema seja desenvolvido por especialista na área de segurança devido a dados sensíveis de cliente, achando assim desnecessário de uma entidade externa para análise de segurança.

## 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?

- Os dados usados no processamento tanto como o processamento em si são demasiado simplistas para considerar.



## 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
<ul style="list-style-type: none"> <li>● Data Breach</li> </ul>	<p>Remote, possible or probable</p> <ul style="list-style-type: none"> <li>● Remote</li> </ul>	<p>Minimal, significant or severe</p> <ul style="list-style-type: none"> <li>● Severe</li> </ul>	<p>Low, medium or high</p> <ul style="list-style-type: none"> <li>● medium</li> </ul>

## 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
<ul style="list-style-type: none"> <li>● Data Breach</li> </ul>	<ul style="list-style-type: none"> <li>● Datos cifrados</li> </ul>	Eliminated reduced accepted  <ul style="list-style-type: none"> <li>● Eliminated</li> </ul>	Low medium high  <ul style="list-style-type: none"> <li>● Low</li> </ul>	Yes/no  <ul style="list-style-type: none"> <li>● YES</li> </ul>

## Step 7: Sign off and record outcomes

Item	Name/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
--------------------------------------	--	---