

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	
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.

O projeto proposto consiste no desenvolvimento de uma aplicação para o agendamento de consultas numa clínica. Nesta aplicação é possível agendar consultas, ver o histórico e resumo de consultas, consultar as receitas médicas e ver o historial dos utentes.

Para os utentes se registarem na aplicação têm de indicar o seu nome completo, idade, data de nascimento, número de utente e password. Aos médicos são fornecidas credenciais para posteriormente associarem o seu nome, password e especialidade.

A clínica pode apagar a conta de um médico, no entanto a conta de um utente não poderá ser apagada.

Portanto, este projeto proposto respeita os critérios 3 e 7 acima mencionados, pelo que seria necessário efetuar uma DPIA.

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?

Os dados são inseridos na aplicação pelos utentes e pelos médicos, sendo estes inseridos numa base de dados onde não é possível eliminar informação relativamente aos utentes. A partilha de dados não será possível visto que os utentes apenas têm acesso à sua informação, e os médicos apenas têm acesso à informação dos seus utentes. Os processamentos com mais riscos associados são a inserção de informação pessoal e sensível dos utentes, bem como a gestão da mesma.

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?

Os dados armazenados terão uma natureza pessoal e médica.
A quantidade de dados armazenados dependerá da quantidade de utentes e da quantidade de especialidades que a clínica disponibilizará. A informação contida na aplicação será armazenada para sempre, exceto a informação removida dos Médicos.
A área geográfica coberta por esta aplicação dependerá da quantidade de clínicas que a usarem.

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 entre os utilizadores e os programadores que desenvolveram aplicação. Os utilizadores terão conhecimento sobre o uso dos seus dados pessoais. No caso das preocupações públicas, existe a necessidade de proteger os dados dos utentes de maneira a que os dados sejam confidenciais.

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 armazenamento dos dados da aplicação, tem como objetivo extrair dados para obter dados Estatísticos, como por exemplo, a frequência da clínica, o tipo de doenças mais comuns, relacionado Com as idades, as especialidades mais procuradas, etc.

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?

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
<p>Existe o risco de terceiros conseguirem aceder à informação dos utentes.</p>	<p>Remote, possible or probable</p> <p>Remota</p>	<p>Minimal, significant or severe</p> <p>Severa</p>	<p>Low, medium or high</p> <p>alto</p>

Step 5: Identify and assess risks

--	--	--	--

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
	Cifrar todos os dados inseridos na aplicação de maneira de maneira a que cada utente só tenha acesso à sua informação.	Reduzido	Baixo	sim

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