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 a marcação de consultas num posto médico, que permite aos utentes, para além do agendamento de consultas, ter acesso ao histórico de consultas realizadas, bem como as prescrições médicas receitadas em cada consulta e um breve resumo sobre as suas consultas, onde consta o que foi falado.

As credenciais para os médicos são disponibilizados pelo respetivo posto médico em que trabalha, enquanto os utentes tem que registar na aplicação e indicar nome completo, nome de utilizador, idade, data de nascimento, posto médico que frequentam, doenças, password. Por outro lado os médicos tem apenas a si associado nome completo, nome de utilizador, password, posto médico atual e os respetivos utentes a si associados.

Os postos médicos podem apagar a conta de um médico, caso este mude de estabelecimento, sendo neste caso gerado novas credencias pelo novo estabelecimento frequentado. Os utilizadores uma vez registados na aplicação não podem nunca apagar a sua conta.

Posto isto, este projeto proposto respeita os critérios 3 e 7 a cima 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 serão inseridos na aplicação pelos utentes (informações pessoais, agendamento de consultas), pelo gerente do posto médico (informação relativa ao médico) e pelo médico (informação relativa às consultas). Todos os dados inseridos na aplicação serão armazenados numa base de dados, sendo que não é possível a remoção de utentes. Não haverá também partilha dos dados com terceiros, uma vez que cada utente tem acesso apenas à sua informação e os médicos tem apenas acesso às informações 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 que será armazenada depende da adesão dos postos médicos e dos utentes à aplicação. A informação contida na aplicação será armazenada para sempre, havendo apenas remoção dos médicos, caso estes mudem de estabelecimento. À medida que se vão sendo realizadas as consultas existe a inserção das mesmas na aplicação.

A área geográfica coberta por esta aplicação será em princípio todo o território português.

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 relação alguma entre os os utilizadores e as pessoas que desenvolveram a aplicação.

Os utilizadores da aplicação sabem o uso que será dado aos dados lá inseridos, sendo que alguns dados incluem grupos vulneráveis tais como doentes, idosos.

No caso das preocupações públicas, existe a necessidade da parte da equipa de desenvolvimento de Proteger as informações pessoais dos utentes, de forma a que terceiros não tem acesso às doenças do mesmo entre outras coisas.

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 estatísticos, de por exemplo, a frequência com que se vai ao posto médico, que tipo de consultas são. Serve ainda para extrair dados estatísticos de quais as doenças mais comuns nos cidadãos portugueses, quais os medicamentos mais receitados para cada doença específica bem como quais os médicos mais requisitados.

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**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
1. Existe o risco de terceiros terem acesso à informação dos utentes	remota	severa	alto

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
1.	Cifrar todos os dados inseridos na aplicação de maneira, para apenas ter acesso cada utente à sua própria 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