# 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. |
| --- |
| A título de exemplo consideremos um projeto que consiste numa aplicação de orientação médica para pacientes poderem marcar a sua consulta. Esta aplicação permite o agendamento de consultas, bem como ter acesso ao histórico das consultas pendentes, canceladas ou realizadas, bem como as prescrições médicas de modo a impulsionar uma melhoria no desenvolvimento do processo médico e de vida dos pacientes.<br>As credenciais de acesso dos pacientes são disponibilizadas pelos seus médicos de família, que aderem à presente aplicação, e as credênciais de acesso dos especialistas sãos disponibilizadas pelos mesmos.<br>Cada paciente terá o seu perfil, acompanhado de informações básicas como: nome completo, morada, identificação completa do cartão de cidadão (número, NIF, número de utente de saúde), idade, sexo, doenças, nome de utilizador, endereço de email, foto, password. Cada especialista será caracterizado por: nome completo, nome de utilizador, endereço de email e password.<br>Todos estes testes serão armazenados de acordo com o nome do paciente, morada, idade, sexo, ano decorrente e especialista responsável pelo seu acompanhamento. Os testes são analisados e acrescentados ao respetivo histórico. Este, por sua vez, apenas está acessível ao paciente e ao seu especialista, tendo este último ainda acesso aos relatórios e medicação.<br>O paciente pode optar por eliminar a conta solicitando pedido ao especialista, sendo que o histórico anónimo é conservado para fins estatísticos. |

# 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 correspondentes ao registo que se teve em conta na abordagem anterior, serão introduzidos pelo paciente, pelo especialista na aplicação. Esta aplicação será renovada habitualmente pelo gerência do posto médico. Todos os dados são inseridos numa base de dados e não é possível a eliminação dos pacientes. Não existe partilha de dados entre terceiros e só o especialista (médico de família) poderá ter acesso aos dados do paciente. Os processamentos mais arriscados e associados são a introdução de dados pessoais bem como a gestão da aplicação. |

| **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 têm uma natureza médica e nível pessoal. A quantidade proporcionada depende da adesão dos pacientes à aplicação. A informção médica que a aplicação suporta será armazenada permanentemente, existindo apenas remoção dos especialistas (médicos de família) caso deixem o cargo. A área geográfica coberta por esta aplicação será imposta em Portugal. |

| **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)? |
| --- |
| A natureza da relação entre os pacientes e os desenvolvedores da aplicação é inexistente. Existe somente relação a nível do médico e do paciente onde são descritos os dados. Os desenvolvedores possuem conhecimento dos dados que foram inseridos sendo que são distribuidos por faixas etárias. No caso das preocupações públicas, existe a necessidade da parte da equipa de desenvolvimento proteger as informações pessoais dos pacientes, de forma a que terceiros não tenham acesso a quaisquer dados. |

| **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 na aplicação tem como objetivo extrair dados para fins estatísticos para, por exemplo, saber informações concretas como a frequência do paciente ao posto médico, as doenças mais comuns em geral bem como a medicação. |

## 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? |
| --- |
| Os principais intervenientes nesta organização são os especialistas (médicos de família) envolvidos no ramo da sua formação (saúde) e o especialista na manutenção da aplicação que são os desenvolvedores desta.<br>No desenvolvimento da aplicação, planeia-se uma consulta aos especialistas de manutenção para uma melhor proteção e segurança da aplicação dos dados dos pacientes.<br>Adicionalmente, os dados são anonimizados de forma ao paciente e ao médico associado serem os únicos a poderem aceder. |

## 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? |
| --- |
| Outra forma de alcançar o mesmo resultado seria através da obtenção de dados por parte do paciente ao médico de família, de forma a ter um acompanhamento mais assertivo. No entanto, a aplicação fornece uma explicação estruturada e facilitada para um paciente de qualquer idade poder aceder. |

# 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** |
|---|---|---|---|
| - Perda de informações para entidades terceiras.<br><br>- Perigo inerente de uma troca de informação entre pacientes. | 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** |
| | - Responsáveis pela manutenção da segurança e o tratamento da informação de forma adequada.<br><br>- Encarregado de proteção dos dados (DPO).<br><br>- Encriptação dos dados preenchidos pelos pacientes e dos especialistas.<br><br>- Utilização da pseudominização que define uma substituição dos dados do paciente por códigos. | 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 |