

# 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 consiste numa aplicação de orientação académica para alunos que estejam numa determinada etapa de transição, seja ensino básico-secundário, ensino secundário-universitário, entre outras.

Esta aplicação permite a disponibilização de informações, de modo a impulsionar reflexão nos alunos, e testes de carácter pedagógico e vocacionais, supervisionados por especialistas qualificados.

Adicionalmente, esta aplicação terá a intervenção de psicólogos e professores, que durante o processo de apoio na tomada de decisão do aluno, têm acesso ao respetivo desenvolvimento do mesmo, com base nos resultados dos testes efetuados por ele.

As credenciais de acesso dos alunos são disponibilizadas pelas escolas, que aderem à presente aplicação, e as credências de acesso dos especialistas são disponibilizadas pelos mesmos, no momento em que se disponibilizam para serem orientadores neste projeto.

Cada aluno terá o seu perfil, acompanhado de informações básicas como: nome da escola, ano, turma, número de aluno, nome completo, nome de utilizador, password; e cada especialista será caracterizado por: nome completo, nome de utilizador, profissão e password.

Após a autenticação dos alunos, estes serão abordados com algumas questões, de modo a efetuar-se uma primeira triagem de opções, tanto vocacionais como de selecção do especialista que melhor o consegue acompanhar. Posteriormente, o aluno será convidado, pelo especialista que lhe foi atribuído, a efectuar determinados testes.

Todos esses testes serão armazenados de acordo com o nome da escola, ano e turma que o aluno frequenta, ano letivo e especialista responsável pelo seu acompanhamento. Mais ainda, estes testes são analisados e acrescentados ao respetivo histórico. Este, por sua vez, apenas está acessível ao aluno e ao seu especialista, tendo este último ainda acesso às estatísticas extraídas dos testes.

A escola possui a capacidade de eliminar a conta de um dado aluno, sendo, nesses casos, removidos todos os dados associados a este, à excepção do respetivo histórico anónimo, que é conservado para fins estatísticos.

Note-se que a aplicação apresentada suporta dois dos critérios enunciados acima: monitorização sistemática (resultante da execução de testes periódicos) e dados relativos a sujeitos de dados vulneráveis (alunos); devendo-se assim efetuar um 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 recolhidos das credenciais dos intervenientes da aplicação e são inseridos pelos mesmos. Os especialistas são responsáveis pelos testes vocacionais propostos e pela respetiva análise e os alunos pelas respostas aos testes mencionados. Note-se que inserção de dados é indispensável para a autenticação e posterior identificação dos intervenientes na aplicação.

Observe-se ainda que os testes são elaborados para que os mesmos possam ser preenchidos pelos alvos da análise vocacional, os alunos, e consequentemente, a fonte de dados para o funcionamento da aplicação consiste assim no preenchimento dos testes que os alunos serão submetidos.

As respostas dadas pelos mesmo são objeto de análise por parte dos especialistas e são mantidas no histórico dos alunos, para que se proceda à elaboração de análises vocacionais, a longo prazo, e ainda se efetue análises estatísticas.

Todos os dados aqui referidos são armazenados numa base de dados única, sendo que é permitido ao administrador anônimizar o histórico dos alunos, através da remoção dos dados pessoais destes.

Adicionalmente, existe partilha de dados apenas entre o aluno e o especialista, mas nunca os mesmos serão divulgados a terceiros.

O tipo de processamento identificado como de alto risco está associado ao facto dos dados pertencerem a sujeitos vulneráveis (menores de idade) e à necessidade de manutenção do histórico.

**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 não pertencem a nenhuma categoria especial ou de ofensa criminal, tendo natureza pessoal e académica.

A dimensão dos dados a serem armazenados é inherente ao número de especialistas (professores e psicólogos) e alunos que aderirem a esta plataforma. Adicionalmente, o facto de existirem escolas a adotar esta aplicação é um factor relevante.

Note-se também que o número de testes necessários para efetuar e finalizar uma análise de um aluno, é variável, sendo isto por si só um factor a ter em consideração, no que diz respeito à quantidade de dados recolhidos. Consequentemente, esses mesmos testes serão acompanhados por análises consecutivas de especialistas.

Serão recolhidos os dados necessários até que o especialista consiga orientar o aluno para uma determinada área, com a frequência igual à da emissão de testes para os mesmos preencherem;

O especialista vai manter os dados consigo até que dos mesmos se retire alguma conclusão confiável, posteriormente serão removidos todos os dados pessoais dos antigos alunos, que já não precisam dos serviços que esta aplicação fornece.

Esta aplicação abrange a área geográfica que engloba as escolas que aderem à aplicação, e ainda alunos individuais que simplesmente aderem à aplicação.

**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 qualquer relação entre os utilizadores da aplicação e os desenvolvedores da mesma.

Os utilizadores da aplicação estão cientes do uso feito aos dados que fornecem.

A necessidade de uma mudança de dados, excepto mudança de password, deve ser comunicada à escola, caso o aluno pertença a um programa escola que tenha aderido a esta aplicação. Já ações como adição e remoção de dados já aqui foram mencionadas.

Para a utilização desta aplicação, aquando de um programa escolar, é necessário que as escolas tenham recursos informáticos e humanos para que a aplicação possa ser bem utilizada e aproveitada.

No que concerne a preocupações de carácter público, existe necessidade de proteger as informações pessoas dos alunos, entidades muito vulneráveis, de modo a prevenir que terceiros tenham acesso a dados comprometedores, como a escola em que o aluno frequenta, a escola que o aluno pretende frequentar no próximo ano letivo, entre outros.

É necessário garantir que apenas os administradores, especialistas e alunos tenham acesso aos históricos, durante todo o processo.

Note-se ainda que o estado atual da tecnologia nesta área é bastante satisfatório.

**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?

Pretende-se alcançar que as escolas aderentes a este programa, possam dispor de um acompanhamento de orientação vocacional de excelência para os seus alunos. Pretende-se ainda que os mesmos sejam de tal maneira bem orientados e acompanhados, que o numero de alunos que ingressam, por exemplo no ensino superior, e mudam de curso ao fim de x tempo seja reduzido.

O objetivo principal passa por ajudar os alunos na tomada de decisão, que é muitas vezes encarada por eles com muita pressão.

O armazenamento dos dados tem como objetivo extrair estatísticas e efetuar uma análise vocacional progressiva, durante um considerável prazo (mínimo 3 meses). Adicionalmente, permite que os intervenientes da aplicação possam consultar o seu acompanhamento.

Por fim, esta aplicação vem possibilitar uma automatização e um acompanhamento muito pessoal aos seus utilizadores, contrariamente ao método tradicional, que para além de impessoal exige a presença física.

## 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 envolventes nesta organização são os especialistas, quer com formação no ramo da educação (professores dos mais variados níveis de escolaridade), quer com formação no ramo da psicologia (psicólogos familiarizados com o acompanhamento dos jovens).

No desenvolvimento da APP planeia-se ainda consultar especialistas em segurança da informação, pois existe necessidade em proteger os utilizadores vulneráveis (alunos) e quaisquer informações relativas aos utilizadores, que possam ser utilizadas para identificar direta ou indiretamente o titular dessa informação. Adicionalmente, estes peritos de segurança permitem confirmar que os restantes requisitos da aplicação são cumpridos, como a possibilidade de anonimizar o histórico do aluno e o acesso à conta apenas após autenticação e validação de permissões.

## 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 maneira para alcançar o mesmo resultado seria o acompanhamento tradicional feito as escolas, em que os especialistas se deslocam às mesmas, e de forma muito imissional tentam orientar os alunos num curto espaço de tempo.

Logicamente, tal não é opção, no entanto, uma adicional vantagem desta aplicação seria o facto de os especialistas poderem agendar reuniões presenciais com os utilizadores interessados.

## 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>
<p>- Perda de informações capazes de serem utilizadas por entidades terceiras para identificar direta ou indiretamente os titulares das mesma, como nome, endereço de email, entre outras. Uma vez descoberta a escola em que o aluno frequenta, facilmente uma entidade consegue ir ao seu encontro.</p> <p>-Perigo inerente ao facto de um dado histórico ser associado a um aluno, o que pode conduzir, por exemplo, a situações em que o mesmo possa ser persuadido a não ir para determinada escola, ou universidade, por entidades que beneficiem com tal escolha.</p>	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

## Step 6: Identify measures to reduce risk

<b>Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5</b>				
<b>Risk</b>	<b>Options to reduce or eliminate risk</b>	<b>Effect on risk</b>	<b>Residual risk</b>	<b>Measure approved</b>
	<ul style="list-style-type: none"> <li>- Contratar um responsável qualificado para o tratamento de informações e um encarregado de proteção de dados: DPO (Data Protection Officer);</li>   <li>- Cifrar os dados enquanto os alunos estiverem inscritos, permitindo que estes apenas tenham acesso aos mesmos depois de efetuada a autenticação e validação de permissões. Deste modo apenas os especialistas e os próprios alunos têm acesso aos seus dados e históricos. Quando removidos os dados dos utilizadores da aplicação, optar pelo anonimato.</li>   <li>-Minimizar os dados recolhidos, o acesso aos mesmos e o tempo de armazenamento associado a estes.</li>   <li>-Optar por usar algum método útil na proteção de todos os dados pessoais envolventes, não só a cifragem mas também, por exemplo, a pseudonimização, que consiste em substituir dados pessoais por códigos.</li> </ul>	Eliminated reduced accepted	Low medium high	Yes/no

## Step 7: Sign off and record outcomes

<b>Item</b>	<b>Name/position/date</b>	<b>Notes</b>
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