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 que se pretende desenvolver consiste numa aplicação educativa para crianças, que permite a disponibilização de informações e testes relacionados com temas de carácter pedagógico, bem como estatísticas de acerto para o utilizador corrente. Para além disso, esta aplicação deverá permitir que professores consultem o desenvolvimento dos seus alunos.

As credenciais de acesso dos alunos e professores são disponibilizadas pela escola. Cada aluno terá associado ao seu perfil os seguintes dados: número de aluno, nome completo, nome de utilizador, password, escola, ano e turma. Cada professor será caracterizado por: nome completo, nome de utilizador, password e escola.

Após a autenticação, os professores podem disponibilizar informações e testes para os alunos de um ano e turma, num determinado ano letivo. Posteriormente, os alunos realizam os testes, que são automaticamente corrigidos e acrescentados ao respetivo histórico. Este, por sua vez, apenas é acessível pelo próprio aluno. Mais ainda, o professor tem acesso às estatísticas dos testes por si efetuados, para os vários alunos.

A escola tem a possibilidade de apagar a conta de um aluno. Nesse caso, são removidos todos os dados associados ao aluno, exceto o respetivo histórico (anonimizado), que é mantido para fins estatísticos.

Desta forma, a aplicação proposta respeita os critérios 3 (monitorização sistemática) e 7 (dados sobre sujeitos vulneráveis) enunciados na pergunta anterior, pelo que é necessário efetuar o 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 pelo administrador (dados pessoais de alunos e professores), professores (testes e correção dos mesmos) e alunos (as respostas aos testes). Os primeiros são utilizados para permitir que os vários utilizadores se possam autenticar e identificar dentro da aplicação. Por sua vez, os testes são utilizados para que os alunos os possam realizar. Por fim, as respostas dadas pelos alunos são corrigidas pelos professores. Estas são utilizadas para manter o histórico dos alunos, assim como na elaboração de estatísticas. Todos os dados referidos anteriormente são armazenados numa base de dados única, sendo que é garantida, ao administrador, a possibilidade de anonimização do histórico dos alunos (remoção dos dados pessoais). Além disso, os dados não serão partilhados com terceiros. O processamento com maior risco está relacionado com a inserção e armazenamento dos dados pessoais do alunos (crianças), bem como a manutenção do histórico das mesmas.

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 naturezas pessoal e escolar.

A quantidade de dados armazenada está dependente do número de alunos/professores de uma dada escola ou, eventualmente, escolas. Para além disso, importa realçar que o número de testes efetuados também influencia a quantidade de dados, uma vez que por cada teste serão adicionadas resoluções e notas do mesmo, dependendo do número de alunos.

No início de cada ano letivo são removidos os dados pessoais de antigos alunos e, adicionalmente, são inseridos os dados dos novos alunos. Além disso, ao longo do ano existe a inserção de novos testes e correções por parte dos professores, bem como a resolução dos mesmos por parte dos alunos.

A área geográfica coberta por esta aplicação envolverá as imediações da escola que a utilize.

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 desenvolvedores e os utilizadores da aplicação.

Qualquer mudança de dados, exceto palavra-passe, deve ser comunicada à escola (administradores), que fará a devida alteração. Ações com inserção e remoção de dados já foram explicitadas anteriormente.

Os utilizadores da aplicação estão cientes do uso que é feito dos dados presentes na mesma. Alguns dados armazenados na aplicação são referentes a crianças.

Para a utilização desta aplicação será necessário que a escola tenha os recursos informáticos suficientes para que os alunos possam realizar os seus testes.

No que toca às preocupações de carácter público, há a necessidade de proteger as informações pessoais dos alunos, de forma a evitar que terceiros tenham acesso à escola que o aluno frequenta. Além disso, torna-se necessário salvaguardar que apenas os administradores, professores e o próprio aluno tenham acesso ao histórico deste último.

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 tem como objetivo permitir extrair estatísticas a partir dos testes realizados pelos alunos para conseguir aprimorar o método de ensino. Além disso, permite aos professores, alunos e encarregados de educação (através da conta do aluno) o acompanhamento do histórico escolar do aluno em questão. Por fim, através da aplicação torna-se possível automatizar a correção de algumas questões dos testes.

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?
No início do desenvolvimento será consultado um perito em segurança de forma a confirmar que os requisitos da aplicação são cumpridos (possível anonimização do histórico do aluno e acesso aos dados apenas após autenticação e validação de permissões). Contudo considera-se desnecessária a consulta dos pontos de vista de outros indivíduos, uma vez que a dimensão do projeto e a dificuldade dos mecanismos de segurança utilizados não o justificam.

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?
O processamento dos dados é necessário, uma vez que é através deste que as classificações são atribuídas aos alunos. Dado que os testes são realizados de forma digital, é imperativo que o tratamento dos dados seja efetuado desta forma. Os dados de cada aluno estarão disponíveis para consulta por parte dos mesmos ou pelos seus professores. Mais ainda, os dados dos professores apenas podem ser consultados pelo próprio e respetivos alunos. Desta forma, os direitos dos utilizadores são salvaguardados. Transferências internacionais de dados não se aplicam.

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 um dado histórico ser associado a um aluno, o que pode levar a situações de discriminação.	possível	significante	médio
2. Existe o risco de terceiros conseguirem descobrir em que escola determinado aluno estuda, o que pode levar a que estes entrem em contacto direto com os menores.	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	Uma possível solução passa por cifrar os dados (a) enquanto os alunos estiverem inscritos. Desta forma apenas os professores e o próprio aluno têm acesso aos seus resultados escolares. Quando forem removidos da aplicação então o respetivo histórico deve ser mantido anonimizado (b).	(a) Reduzido (b) Eliminado	Baixo	Sim
2	Uma possível solução passa por cifrar os dados do aluno. Desta forma apenas se tem acesso aos mesmos depois da autenticação e validação das permissões.	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