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.

Dadas as circunstâncias atuais, o projeto consistiria numa *web app* para informar os seus utilizadores registados acerca do estado do COVID-19 e seu devido acompanhamento. A ideia desta *web app* seria focar-se na região geográfica do utilizador, no sentido de o colocar a par de toda a informação e prestar a assistência necessária:

- Informações acerca do número de infetados em tempo real;
- Informações acerca do número de recuperados e mortos em tempo real;
- Divulgação de gráficos acerca do estado atual do COVID-19 no mundo e, principalmente, na região em específica;
- Assistência *online* relativamente à compra de medicamentos, comida e outros bens essenciais;
- Esta assistência seria conjugada com o posterior envio à casa do utilizador com todas as medidas de higiene.

Estas seriam as ideias gerais para o projeto, mas para tal acontecer teria de existir a disponibilização de dados por parte do utilizador:

- Nome de Utilizador/Email;
- Morada (tanto para as informações do COVID-19 como para a assistência necessária);
- Dados Bancários (para processar os devidos pagamentos).

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?

- Adquirir os dados numa espécie de *form* no ato de registo;
    - A localização da cidade é a base pedida neste ato, dado que é necessária para fornecer os dados do COVID-19;
    - A morada em si seria apenas pedida a partir da primeira compra. O utilizador podia depois decidir guardar ou não esse endereço para compras futuras, de modo a facilitar o processo;
    - Os dados de pagamento seguem a mesma política da morada, dado que também apenas são necessários neste tipo de atividade.
- O uso destes dados é apenas destino para identificar a localização do utilizador e com isso oferecer uma experiência totalmente adaptada a si;
- Não existiria partilha de dados com outras entidades externas;
- Os processamentos de dados identificados como sendo de alto risco estão precisamente no fornecimento do endereço específico e dados de pagamento.

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 seriam fornecidos pelo utilizador devidamente registado e autenticado no sistema;
- Como dito anteriormente, alguns dados seriam pedidos no ato do registo e outros no decorrer de uma compra na *app* em si;
    - Nome Utilizador/Email seriam pedidos no ato de registo;
    - Morada e Dados de Pagamento seriam pedidos no ato da compra, com as devidas possibilidades.
- Estes dados seriam mantidos até ordem contrária do utilizador – encerramento da conta;
- Apenas a informação geográfica seria "usada" várias vezes ao dia para poder dar *updates* da situação ao utilizador;
- Apenas os utilizadores registados seriam o "público-alvo";
- A área abrangida corresponderia aos utilizadores registados.

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 com os utilizadores registados na *web app*;
- O controle dado aos utilizadores focar-se-á em pequenas decisões como por exemplo a possibilidade de escolher manter na base de dados as suas informações de pagamento e respetivo endereço;
- Não é permitido o uso a menores de idade, dada a ideia geral da *app*;
- Existem assim evidentes preocupações sobre todo o processamento de dados pessoais por parte dos utilizadores e possíveis falhas de segurança/privacidade que possam eventualmente surgir.

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 objetivo deste processamento é fornecer aos utilizadores toda a informação necessária para uma constante atualização sobre o COVID-19, para consciencializar e com isso reduzir mais cadeias de transmissão;
- Este processamento é benéfico para obter estatísticas acerca da população no geral, das suas preocupações e acima de tudo o cumprimento correto da quarentena.

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?

- O sistema em si será autónomo por natureza;
- Apenas o processo de compra e posterior entregue em casa necessitará de intervenção humana - pessoas completamente prevenidas e preparadas para tal.
- Será necessário que o sistema seja pensado e desenvolvido por especialistas na área da segurança, dado que precisaremos de lidar com dados que são extremamente sensíveis para o cliente/utilizador em si.

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?

- Dada a natureza da aplicação e tendo em conta que o conjunto de dados em si é muito reduzido e "basilar", torna-se "difícil" avaliar esta necessidade e proporcionalidade.

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
Violação/Divulgação dos Dados do utilizador	Remote	Severe	Medium

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**
Violação/Divulgação dos Dados do utilizador	• Fazer a cifragem dos dados; • Controlar e estabelecer permissões de acesso.	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no Yes

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