## ico_master_blue_rgb_DPIA – user registration

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](http://ec.europa.eu/newsroom/document.cfm?doc_id=47711) 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 | Alexandra CLOOS |
| Subject/title of DPO |  |
| Name of controller contact /DPO  (delete as appropriate) | acloos@stud.42.fr |

# 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. |
| The project is the creation of a website where users can register and play the game Pong. Stats are kept on the player’s games, such as wins and losses. |

# 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? |
| The processed data is collected on inscription, and used when  - confirming registration on the website  - communication is needed from the website including but not limited to : confirming changes on the user’s password and email address (security measure), any info pertaining to security (if there ever was a breach od data privacy), updates on Privacy Notice/data handling etc  The data is stored on our database.  It is deleted upon the user’s request OR IF WE DECIDE TO END THE ACCOUNT ??  It is not to be shared with any entity, and processing it does not involve any high risk to the rights and/or privacy to the user. |

|  |
| --- |
| **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? |
| The processed data is the user’s email address. It does not fall under any special category, and is not considered a sensitive data.  It is collected once, on registration. All users must supply this data, regardless of their geographic region when registering – the data will not be re-processed if the user accesses the website from a different area. It is used only for security concerns, and kept until the account is deleted. |

|  |
| --- |
| **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)? |
| The individuals are considered customers of the website. While their are logged in to their account, they can see the data and modify it as will (may want to put a max change for a given time? Avoid 10 changes per second?).  EXPECTATION : make sure that processing details are available to users on the email to validate registration, such as what their data (email address) is used for  We do not process the age of our users, therefore cannot know if children use the service. However, most email providers include in their terms and conditions that their user must be at least 13 years of age, or more, to use their services. For instance, Google has a list per country for the minimum age (in France you must be 14 years old minimum) ; Microsoft Services states that their users must have reached the age of majority of their place of residence, or if they are a minor, that their parent/legal gardian accepts to be bound by their terms and conditions. => maybe add in terms of use that the person must be at least 13?  The data is very simple and not directly identifying the user, there is no specific concern or technology tied to it, and no need for certification to use it.  Employees are required to sign a charter regarding data handling/processing. |

|  |
| --- |
| **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? |
| We want to secure the access to user’s profile, to ensure whoever created the account is the only person who can access it. We do not wish to implement 2FA as we feel there is little inherent risk in id’ing the person and we deem that there it would be too mush a hassle for the users  Also, it allows the users to handle and update their data as they wish. |

# 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? |
| As this is a small organization, there is no specific stakeholder – only discussion between members as to how the operations may evolve in any way regarding the handling of users’ accounts. Unless we deem necessary to process more data to expand all and any aspect of account handling, there should be no need to consult 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? |
| The lawful basis for this data processing is based on the fact that some data is necessary to create an account, in order to ensure that whoever accesses an account (and modifies its info) is the person who created it. There is no need for the address to reflect the name (or any identifying piece of information) of the user. The registering process specifically asks for the email address, so the future user can decide to stop the process immediately of they do not want to give an email address. No other data is asked from the user. Data processing info are given in the email sent to complete registration. Also, a Privacy Notice is available on the website, and the data is not shared with external organizations. |

# Step 5: Identify and assess risks

|  |  |  |  |
| --- | --- | --- | --- |
| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risksas necessary. | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
| Privacy-related risks : unauthorized access/modification/deletion of data  threats making it possible :  computer stolen  hacking  human error  threat source:  employee  virus  hacker  impact on user’s life :  inability to access the website  email distributed to others | Remote (if data cannot be accessed by employee)  remote  possible ?  Possible?  Possible?  Possible?  Possible?  Possible?  Probable?  Remote, possible or probable | Minimal  minimal  minimal  Minimal, significant or severe | Low  low  low  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** |
| access/mod/del data  hacking | Minimize access  cannot modify  can only delete after account has been reported/noted to not comply with rules  secure access  data are anonymized (are they ?) | 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 be kept under review by: |  | The DPO should also review ongoing compliance with DPIA |