Data Protection Impact Assessment

# Step 1: Identify the need for a DPIA

Explain broadly what the 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 aims to efficiently identify steel beams to allow the operator to correctly locate its placement.**

**The only piece of information needing processing in accordance with DPIA is the operator’s login information (employee ID).**

**We can also review the requirements documentation in the project folder for further information.**

# 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 another way of describing data flows. What types of processing identified as likely high risk are involved?

**No data will be collected nor shared, however the employee’s login data will need to be stored in the clients cloud database for access of the scanner.**

## 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?

**Data encompasses personal information such as employee ID number. Data will only be used to access the scanner application and stored on client’s cloud servers.**

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)?

**No processing of data.**

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?

**No processing of data.**

# 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?

**Since no data is being used or stored or processed the client will handle everything in house.**

# 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?

**Full compliance given as no data is processed.**

# Step 5: Identify and assess risks

Describe the source of risk and nature of potential impact on individuals in the description box. This includes associated compliance and corporate risks as necessary.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk ID | Description | Likelihood of harm *(remote, possible or probable)* | Severity of harm *(minimal, significant, or severe)* | Overall risk *(low, medium or high)* |
| 001 | Server is stolen | Possible | Minimal | Low |
|  |  |  |  |  |

# 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 ID | Options to reduce or eliminate risk | Effect on risk  *(eliminated, reduced or accepted)* | Residual risk *(low, medium or high)* | Measure Approved  *(yes/no)* |
| 001 | Encrypt data | Low | Low | Awaiting |

# Step 7: Sign-off

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | | **Name/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 | |