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.

**In order to process this information, the companies can choose their preferred level of detail as some users might opt for detailed inputs which** **contain sensitive information while other users may choose to use generalised estimates.**

**The project aims to develop an web based or mobile application to assist the energy companies in evaluating the ROI.**

**The tool will process financial and operational data entered by users to assess metrics such as operational efficiency, decision-making improvements and regulatory compliance**

**The DPIA is necessary due to the sensitise nature of financial and operational data from energy communities. The tool must ensure the data privacy and address potential risks associated with handling of confidential business 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?

**The users will manually input the data such as the cost, projected savings and other investment metrics specific to their digital transformation projects.**

**All the data is provided directly by the users and typically though an input form.**

**Collected data is stored securely in a cloud environment, ensuring that only authorized users can access it.**

**Users would have the option to delete or export their data upon project completion.**

**Data is not shared with third parties.**

## 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?

**Financial and operational data relevant to digital transformation investments, specific to the energy sector.**

**The amount of data will vary by user and project, retention may align with project timelines or user preferences.**

**The affected individuals would primarily be corporate users and energy company decision makers**

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 users are energy sector professionals and have control over the data they input and analyse.**

**The users expect secure handling of sensitive business data and transparency on how it us used within the tool.**

**There are no anticipated vulnerable groups the target audience includes corporate professionals.**

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?

**The tool is designed to help energy companies evaluate the ROI of digital transformation initiatives. By calculating potential financial and operational impacts as it assists the companies in determining if these initiatives are financially viable.**

**Users gain insights into the benefits and transformation, empowering them to make data-driven decision. The tool’s analyses can inform strategic planning, budget allocations and long term investments.**

# 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?

**Engage with stakeholders such as project managers, IT and legal teams to ensure compliance and robust data protection.**

# 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 as data processing is necessary to provide ROI calculations that support users’ strategic decision making.**

**Data collected is limited to the essential information needed for accurate ROI calculations. The tool will avoid collecting unnecessary data.**

**The inputs are user-controlled which allows the users to entre only the data required for specific assessments.**

**Users are informed of data usage policies and have access to their data within the platform.**

# 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 |
| 002 | Inaccurate data inputs leading to misleading ROI results | Possible | Significant | Low |
| 003 | Fake Credentials | Possible | Significant | High |
| 004 | Cloud Storage Shutdown | Probable | 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 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 |
| 002 | Validation Protocols | Reduced | Low | Awaiting |
| 003 | 2FA For Purchases | Reduced | 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 | |