# DPIA for Time Management

This DPIA form is designed to guide the Time Management web application project team in assessing and documenting the potential risks to individuals' privacy posed by the project's processing of personal data.

## 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. Summarize why you identified the need for a DPIA.

The Time Management web application project aims to provide users with a set of tools to manage their time more effectively. The application includes features such as a scheduler, to-do list, anti-procrastination tool, diary, alarm/timer, history, and email notifications. The application will process personal data such as user names, email addresses, and potentially sensitive information such as task details and schedules.

A DPIA is necessary because the project involves processing personal data on a large scale, and therefore carries the risk of infringing on users' privacy rights. Additionally, the project involves the use of potentially sensitive information such as task details and schedules, which could cause harm to users if improperly handled. By conducting a DPIA, we can identify and mitigate potential privacy and security risks before the application is launched, ensuring that users' personal data is handled appropriately and in compliance with data protection regulations.

# 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 Time Management web application involves collecting personal data from users, such as their name, email address, and task information. This data will be used to provide features such as a scheduler, to-do list, and diary, all of which will store user data for later retrieval.

The primary source of data will be the users themselves, who will input their personal information and task details into the application. Data will be stored in a secure database and will be deleted upon the user's request or after a specified period of time has elapsed.

No data will be shared with third parties, except for email notifications, which will be sent to users regarding their tasks and appointments. The email notifications will not contain any personal data beyond the user's email address.

The processing identified as likely high risk includes the storage of personal data, including email addresses and task information, as well as the potential for data breaches or unauthorized access to the application. Additionally, the application's anti-procrastination feature could potentially be seen as intrusive or coercive, which could lead to user privacy concerns.

**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 Time Management web application will collect and process personal data related to its users, including names, email addresses, and time-related information such as scheduled tasks and to-do lists. The application will not collect or store any special category or criminal offence data. The amount of data collected will depend on the user's activity and usage of the application. The data will be collected and used on an ongoing basis as the user interacts with the application. The data will be retained for as long as the user has an active account with the application. The application will be accessible to users globally. The number of individuals affected will depend on the number of users of the application.

**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 users who will have control over their own data. The nature of the relationship is that of a service provider and user. Users would expect their data to be used to provide them with the features of the application, such as scheduling and to-do list management. The application does not target any specific vulnerable groups, but it is important to ensure that the application is accessible to all users. There are no known prior concerns over this type of processing or security flaws. The current state of technology in this area includes many similar applications available in the market. There are no current issues of public concern that need to be factored in, and the application is not currently signed up to any approved code of conduct or certification scheme.

**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?

For the Time Management web application, the purposes of the processing are to provide users with tools to manage their time more effectively and efficiently. The intended effect on individuals is to increase their productivity and reduce their stress levels by helping them to stay organized and on track with their tasks and schedule. The benefits of the processing for the application developers are the potential for increased user engagement, retention, and revenue through offering valuable tools and features. The benefits more broadly are the potential for increased productivity and wellbeing of the individuals using the application, which could have positive impacts on their personal and professional lives.

# 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 organization? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

One way to seek individuals' views is to include a user survey or feedback form within the application itself, or to conduct user testing sessions. It may also be appropriate to consult with information security experts or other professionals who can provide guidance on best practices for handling personal data.

Within the organization, it may be necessary to involve the development team, as well as any data protection or privacy officers. It may also be necessary to consult with processors, such as third-party service providers who are involved in the processing of personal data.

## 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 minimization? 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?

**Lawful basis for processing**: Identify the lawful basis for processing personal data. For example, the lawful basis may be the consent of the individual, or the processing may be necessary for the performance of a contract.

**Purpose**: Ensure that the processing of personal data is necessary to achieve the intended purpose. There should be no function creep, meaning the processing of data should be limited to what is strictly necessary to achieve the purpose.

**Data quality and minimization**: Ensure that the personal data collected is accurate, up-to-date, and relevant to the purpose for which it is processed. Personal data should not be kept for longer than necessary.

**Transparency and individuals' rights**: Provide individuals with clear and concise information about the processing of their personal data, including the lawful basis for processing, the purpose of processing, the categories of personal data processed, and the retention period. Individuals have the right to access, rectify, erase, and restrict processing of their personal data.

**Processor compliance**: Ensure that any third-party processors comply with data protection requirements by putting in place a data processing agreement that includes appropriate safeguards.

**International transfers**: If personal data is transferred to a country outside the European Economic Area (EEA), ensure that appropriate safeguards are in place, such as standard contractual clauses or binding corporate rules.

## 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** |
|---|---|---|---|
| **Security risks**: The application will collect and store personal data, such as email addresses and to-do lists, which could be attractive to hackers or malicious actors. | Possible | significant | medium |
| **Accuracy risks**: The application will use algorithms to manage and categorize personal data, which could lead to errors or false assumptions. The potential impact on individuals could be missed deadlines or incorrect scheduling. | possible | Minimal | Low |
| **Transparency risks**: The application may not clearly explain to individuals how their personal data is being used or shared. The potential impact on individuals could be confusion about the purpose of the application or loss of trust in the organization. | Remote | 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** | **Options to reduce or eliminate risk** | **Effect on risk** | **Residual risk** | **Measure approved** |
| **Security risks** | 1. Regular software updates and patching: Ensuring that software and systems are kept up-to-date with the latest security patches can help to reduce the risk of security vulnerabilities being exploited.<br>2. Encryption of sensitive data: Using encryption to protect sensitive data can help to mitigate the risk of data breaches.<br>3. Encryption of sensitive data: Using encryption to protect sensitive data can help to mitigate the risk of data breaches. | The potential impact on individuals could be loss of personal data or breach of their privacy. | medium | Yes |

# Step 7: Sign off and record outcomes

| **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 kept under review by: | | The DPO should also review ongoing compliance with DPIA |