DPIA template for Money Maven

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.
Majority of the populace find it difficult to manage their finances, stick to a budget and have a hard time paying their bills. Hence, the project intends to create a web-based finance tracker app. Our aim is simple; it is to simplify financial management. A finance tracker app can automate many financial tasks such as categorising expenses into different groups and generating reports and graphs enabling the user to view their entire financial status in just a glance. This can save a lot of time and make financial management a lot less overwhelming. This app will also allow users to set and achieve their financial goals and constantly be able to monitor their progress towards them. This can include goals such as paying off debt, saving for a down payment on a house, building an emergency fund or simply to save money. They can view all their previous expenses and see which is their primary expense category. This app will enable users to be able to make more informed decisions and facilitate wise spending. We identified the need for a Data Protection Impact Assessment (DPIA) for our personal finance tracker web app because it involves processing sensitive personal data related to financial information, which poses a high risk to individuals' rights and freedoms. The DPIA will help you identify, assess, and mitigate potential privacy and data protection risks associated with the app's data processing activities, and ensure compliance with data protection regulations such as the GDPR. As it is a browser-based app, only the internet is required to access it, enhancing usability and improving accessibility as it can be accessed from any device which has an internet connection and is not limited to a specific device. This makes it easier for users to stay on top of their finances and make informed financial decisions.

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?

Money Maven collect most of the data from our users. We collect and process data when they:

- Register for the app.
- Voluntarily complete a customer survey or provide feedback on any of our message boards or via email.
- Use or view our website via their browser's cookies.
- Enter financial transactions into the app.
- Integrate their Money Maven account with their bank account.

Money Maven uses customers data in the following ways

- Management of their account.
- Email with special offers on other products and services.
- Help our users with financial planning.
- Fix any technical issues.

Money Maven securely stores users' data at the university of Birmingham and the following security precautions are taken to make sure that the data is safe:

- Data is encrypted before it is stored.
- The data is regularly backed-up to ensure that there is no data loss.
- Access to the apps data is monitored to ensure there is no unauthorized access.
- Proper access control is set to ensure there is no unauthorized access.
- Workers that have access to the app's data will have to use strong passwords and two factor authentication.

Money Maven will keep user data for the period that the user has an account Once this time period has expired, we will delete your data by correctly identifying the data that needs to be deleted and wiping it from our system.

The source of the data is the users/customers. We will not be sharing the data with anyone. Processing identified as high risk are users' credentials and financial information.

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?

These are the nature of the data Money Maven deals with:

- Name
- email address
- Phone number
- Transaction data of purchases and transfers made by the user.
- Usage data
- Bank account information

It does not include any special category or criminal offence data. The amount of data Money Maven collects is the ones listed above.

Money Maven will keep user data for the period that the user has an account Once this time period has expired, we will delete your data by correctly identifying the data that needs to be deleted and wiping it from our system and if a former user signs up again, we will collect the data again as they would have been off our system.
The individuals affected are our users/customers who registered for our web app and the geographical area mainly covered is the United Kingdom.

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 relationship between us and the individuals is a brand-customer relationship. They will have control over most of the functionalities in the app such as their financial information and budgets. Customer relations are very dear to us at Money Maven, and we put the customers first in our processing.

Yes, they would expect us to use their data in these way as we have provided them with our privacy policy on our web app. They do not include children as the minimum age to register to our app is 18 and they would be additional checks such as ID to verify. They are no concerns over this type of processing as we have taken steps to ensure the security and safety of our app. The state of technology used is not novel but very efficient. The issues of public concern we should factor in are security breaches and leaks of sensitive information such as the user's financial information and we have taken sufficient steps to mitigate that. No we are not signed up to any approved code of conduct or certification scheme but we are working under the University of Birmingham so adequate steps are taken in regards to an approved code of conduct.

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 purposes of processing for Money Maven include These are the intended effect on individuals:

- Tracking and categorizing personal expenses and incomes
- Generating reports and analytics to help users understand their spending habits.
- Providing financial recommendations and advice based on user data.
- Facilitating the management of financial accounts and transactions
- Customizing the user experience and marketing based on user data and preferences.

The purpose of processing for us is to simplify financial management.

The purposes of processing more broadly refer to the reasons why user's data is being collected and used in a project such as a personal finance tracker web app (Money Maven).

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?

It is very important to seek individuals' views on the processing of their personal data, as this can help to identify any privacy or data protection risks that may not be immediately apparent. We seek individuals views before starting our application and we compiled them into personas to guide our development. We also seek individual's views when the personal data being processed is particularly sensitive and the processing is likely to have a significant impact on individuals' lives or well-being. How we seek individual's views is to provide clear and concise information about the processing of personal data, including the purposes of processing, the types of personal data being processed, and who will have access to the data while also providing individuals with an opportunity to ask questions and provide feedback and ensuring that individuals' feedback is taken into account in the DPIA process and documented in the final report.

It is not appropriate to seek individual's views if seeking views would compromise the purpose of processing (such as in a criminal investigation).

Within our organisation, we need to involve the School of Computer Science and IT Department at the University of Birmingham. Yes, we need to ask processors to assist as we are students. We plan to consult information security experts and other experts present at the University of Birmingham.

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?

The lawful basis for processing data is consent as users of Money Maven have given us consent to store and process their data. The processing of user data achieves the purpose of an app where users can track their finances and budget appropriately which falls in line with the expectations of the users. There is no other way to achieve the same outcome. Function creep, which is the expansion of a system or technology beyond its original purposes, is prevented by regularly updating user consent forms and the privacy policy of the app. Data quality and data minimization would be ensured by only collecting data that is necessary and making sure that the data collected is adequate to achieve the app's purpose. User rights will be supported by having the data protection rights in the GDPR policy which would be available for viewing on the app that contains instructions on how users can exercise their rights and who to contact. The measures money maven has taken to ensure processors comply include keeping track of the name and contact details of processors, keeping track of the name and contact details of controllers for whom the data is processed, and keeping track of the categories of processing activities that are processed on behalf of the controller. To safeguard international transfers the following measures are taken: a transfer to an “adequate” country is the simplest way to transfer personal data outside the EEA; these transfers are permitted and legal under the GDPR. a transfer to a non “adequate “ country will require user consent.

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**
1.) Data Breach - This could happen if unknown attackers gain access to our systems. This would result in our users' personal and financial information being stolen. It would have negative impacts on our users and be a threat to Money Maven's financial, organizational, or reputational standing.	Possible	Severe	High
2.) Inaccurate data -Another source of risk is inaccurate data that could lead to Money Maven providing inaccurate financial advice. This could negatively impact the user and would be a compliance risk because it would negatively impact the company's reputation.	Remote	Significant	Medium
3.) Data Protection - As this is a finance tracker it must comply with the GDPR and failure to do so will be a compliance risk. Which could lead to financial penalties and damage to the company's reputation.	Remote	Significant	Medium
4.) Inadequate customer service - This includes not enough support for users and slow response times by the company. This would hurt the company's reputation so, therefore, is a corporate risk.	Remote	Minimal	Low
5.) Issues with technology - This includes significant downtime or the app not functioning like it's supposed to. This would have a negative impact on the user as they cannot use the app and would also cause damage to the company's reputation.	Probable	Significant	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**
1.) Data Breach	• Data is encrypted before it is stored. • The data is regularly backed-up to ensure that there is no data loss. • Access to the apps data is monitored to ensure there is no unauthorized access. • Proper access control is set to ensure there is no unauthorized access. • Workers that have access to the app's data will have to use strong passwords and two factor authentication.	Reduced	Low	Yes
2.) Inaccurate Data	• The interface will be easy to use, and this would help users to enter data accurately. • The data will be regularly checked for completeness and integrity.	Reduced	Low	Yes
3.) Data Protection	• Putting someone in charge of making sure that the app complies with the GDPR.	Reduced	Low	Yes

4.) Issues with technology	• Making sure the app is always tested. thoroughly and regularly. • Having regular system updates. • Giving users the opportunity to give feedback and report if they have had any issues with the app.	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	**Name/date**	**Notes**
Measures approved by:	Leila Shaibu 28/03/2023	Integrate actions back into project plan, with date and responsibility for completion

Residual risks approved by:	Leila Shaibu 28/03/2023	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Leila Shaibu 28/03/2023	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: All measures in place and to be sustained.		
DPO advice accepted or overruled by:	Leila Shaibu 28/03/2023	If overruled, you must explain your reasons
Comments: N/A		
Consultation responses reviewed by:	Leila Shaibu 28/03/2023	If your decision departs from individuals' views, you must explain your reasons
Comments: N/A		
This DPIA will kept under review by:	Leila Shaibu 28/03/2023	The DPO should also review ongoing compliance with DPIA