Purefy DPIA Form

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 proposed project is a web application with the aim of improving the quality of people's lives through the avoidance of cheap sources of dopamine. This is done through the user completing challenges based on their selections, as well as tracking their mood and daily tasks through a mood journal and habit tracker respectively. Part of this process includes collecting data about the user's mood and daily lifestyle, to help track their progress on their journey towards a better lifestyle. Due to this data collection, to comply with GDPR law, we are required to fill out a DPIA. We must use a DPIA to mitigate and understand the risks associated with processing this data (personal and behavioural etc).

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 data will be collected initially when the user first creates an account, as well as throughout the use of the application. The initial data will be used to tailor the app experience for the user, and the rest of the data is used to track the user's progress for their own benefit. This data will be stored in a database which means we can wipe their data from it if the user requests we delete it.
The data is sourced from user input upon registering (name, email etc.), as well as more user input when navigating and using the application (mood, behavioural data etc.)
Some of the initial data will be shared with people that the user shares a group with such as their name and challenge progress, while other data such as mood, is only shared internally with the database and other systems.
Currently there isn't any processing which identifies as likely high risk.

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 data we are processing includes personal data (including name and email address) as well as behavioural data. We aren't collecting any special category or criminal offence data, as the data doesn't involve the user's race, gender or criminal history etc.
Data is only collected while the user is using the web application, as well as when they register, so the amount of data that is collected depends on how much the user utilises the app.
Data will only be kept while the user has an account and will be deleted either upon account deletion or after July 2024.
The number of individuals affected depends on the number of users that Purefy has, but this could be anywhere from a very small userbase to quite large depending on interest.
The geographical area affected once again depends on the where the users of Purefy are located, as that could be any place with access to the Internet.

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)?
Purefy is providing a service to the users in the form of a free web application. The users can request deletion of their data anytime by simply deleting their account. The users of Purefy would expect their data to be used in this way as the main purpose of the web application is made clear to them, and most of the data collected is through user input. Our userbase could potentially include children, but not any other vulnerable groups. Currently Purefy is not signed up to any approved code of conduct or certification scheme, but we are considering it for the future.

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 main purpose of Purefy is to improve the lifestyle of users through detoxing of cheap dopamine, while building good habits and avoiding bad ones. Averting cheap sources of dopamine (e.g. scrolling, smoking, drinking, etc.) enables users to lead a more a more productive lifestyle. By processing the data that the users input, it allows us to give the users a more personalised experience. This also benefits us as it ensures users are more likely to continue using the website.

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?
The main individuals and stakeholders which are relevant for Purefy are the users who log into and use the website. When the users sign up and create an account, they consent to Purefy using the data which they gave to tailor their experience, so consulting them under normal circumstances is not necessary. However, if occur some extraordinary event was to occur, such as a data leak, users would be informed and consulted, as well as all members of our team. If the aforementioned situation arose, we would consider consulting with information security expert.

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 processing our users' personal data is enabled by the user's consent. This consent is granted by the user upon account creation and allows Purefy to use the user's personal data to enhance and personalise their experience. Without being able to process this data, Purefy would not be able to provide the same service. To prevent function creep, if new features are implemented that affect the way we collect data, we will reflect and consider changes to the DPI. Data quality and minimisation can be ensured by requiring that personal be kept up to date. User's rights will be supported by ensuring they are aware of the data that is collected and what it is used for. As well as this, users can control their data by being able to delete their account, if they require their data to be deleted. Purefy will ensure relevant processors abide by relevant policies and regulation. International transfers will be safeguarded by ensuring that they comply with GDPR policy.

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** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high
Unauthorised access – Access to individual users' accounts from third parties.	Possible	Significant	Medium
Physical data location – Security of the physical location of the database server.	Remote	Significant	Low
Virtual data location – Security of the server to cyber-attacks.	Possible	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**
Unauthorised access	Ensure all user's and admin/dev team's password are required to: • Be a minimum length of 7 characters. • Contain at least one upper and lowercase letter, number and special symbol.	Reduced	Low	Yes
Virtual data location	Data being sent to and from the database server is encrypted to a good level and ensure the 3rd party server host's security protocols are up to standard.	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	**Name/date**	**Notes**
Measures approved by:	Adnaan Loonat 04/03/24	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Asa Bizanjo 04/03/24	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Allen Jen Joseph 04/03/24	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: As the Data Protection Officer (DPO), I conducted a comprehensive review of the DPIA for a proposed web application aimed at improving users' lives by avoiding cheap sources of dopamine. To ensure compliance with GDPR regulations I advised on the need to set up a DPIA to understand and mitigate the risks associated with the processing of personal data. In reviewing Stage 6 decisions including preventing unauthorized access and virtual data security, I recommended implementing a strong password policy, review that the transmitted data is kept confidential to reduce risks. After careful consideration, I determined that processing can proceed as the implemented measures effectively mitigate risks, resulting in low residual risk levels and maintaining compliance with GDPR regulations.		
DPO advice accepted ~~or overruled~~ by:	Adnaan Loonat 04/03/24	If overruled, you must explain your reasons
Comments: N/A		
Consultation responses reviewed by:	Prince Alexander John 04/03/24	If your decision departs from individuals' views, you must explain your reasons

Comments: N/A		
This DPIA will be kept under review by:	Adnaan Loonat 04/03/24	The DPO should also review ongoing compliance with DPIA