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 involves collecting personal information through a mobile app and website to facilitate user feedback on the energy drink and enable bulk buy purchases by companies. Personal data such as age, gender, location and contact details are captured to improve user experiences and ensure proper account functionality. For the website, company-specific data, including addresses and payment details, is processed to handle bulk orders.

This DPIA is required as the project involves processing personal data and feedback from individuals, which could introduce potential risks to privacy.

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?

Data is collected directly from app users for account creation, feedback, and wellness tracking.

Some information (e.g., age, gender location) may be shared within the app community (optional). Contact details (e.g., email addresses) will remain private and used solely for account functionality.

Website data for companies including order details, addresses, and payment information. Payment data will not be stored.

Data will be stored on encrypted servers and deleted upon user or buyer request.

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 collected includes user demographics (age, gender, location) and feedback (optional).

Company data includes addresses and order details.

No special category data is collected.

Data is stored for the duration of user activity or until deleted upon request.

Geographic coverage is limited to the UK.

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)?

Users are aware of data collection as it is required for account creation and app functionality. Feedback sharing is optional, and users can control what they share.

No vulnerable groups are involved.

The data processing aligns with industry-standard practices and complies with GDPR principles.

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?

Enable account creation and feedback sharing on the app.

Provide insights into user preferences (e.g., gender, location) for product improvement.

Facilitate order fulfilment for companies on the website.

Build community engagement through shared feedback, fostering user engagement with features like streak tracking.

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?

Customer trials will be conducted to obtain feedback on data usage and ensure transparency. This will also ensure customers accept the use of data before pushing to production.

Internal stakeholders, including developers and processors, are already involved in aligning data handling practices.

Security experts will review the system to ensure compliance with data protection requirements.

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 includes consent for data collection and legitimate interest for order fulfilment.

Data collected is directly tied to the project's objectives of improving user experience and enabling community engagement.

Only essential data (e.g., age, gender, feedback) is collected.

Users can request access, modification, or deletion of their data. Clear privacy policies are provided to support informed consent.

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	Unauthorised access to the app or website data	Remote	Severe	Low
002	Data breach exposing user or buyer information	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 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 all sensitive data in transit and at rest	Reduced	Low	Yes
002	Implement regular security audits and robust access controls	Reduced	Low	Yes

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