Privacy Impact Assessment Worksheet

Part 1 – Information Gathering

## Describe the project:

Describe the project briefly.

Describe the purpose of changing what happens with personal information – what is the business aim in making the change?

Example:  
We are collecting user information via our online website and social media activities for the purposes of marketing and lead generation (email newsletters, etc).

## Describe the personal information involved and what will happen to it:

The focus of a Privacy Impact Assessment (PIA) is the personal information involved in the project and any positive or negative effects that the project may have on the privacy of the individuals affected by it.

Consider how PII is stored, who’s going to use it and why, how it’s kept up to date, how long it will be kept for, and what will happen if the individual whose information it is asks to see it.

If the PII is shared with another organisation, would that sharing take the individual by surprise - perhaps because they weren’t told when you collected the information? How will you make sure the information is secure when it’s being sent to the other organisation, and that it won’t be misused?

Example:  
E-mail addresses are collected via a form on our website. This data is sent to Mailchimp, where the mailing list is stored.  
Marketing staff have access to Mailchimp to create and send e-mail marketing material.  
The Mailchimp password is a strong password, changed every six months and stored in BitWarden.  
Mailchimp will manage the un-subscription process when a user wishes to unsubscribe.  
Customers can also manage their e-mail preferences via Mailchimp.

1. Receipt information
2. Phone Number
3. Address

You can use an information flow diagram to displays the flow of information. (These can be created quickly at <https://app.diagrams.net/>)

Graphical user interface, text, application, chat or text message

Description automatically generated

Part 2 – Privacy Analysis

Complete the following analysis for at least 3 pieces of personally identifiable information collected by the business.

Complete all fields, or explain why the field is not relevant for the PII analysed.

|  |  |
| --- | --- |
| **Aspects of information assessed** | Email addresses collected via website subscription form.  1.  2.  3. |
| **Description of the risk** | Risk of third-party obtaining mailing list, potential abuse (spam) of list. |
| **Why is this PII necessary?**  **What are the consequences for the individual?** | Email addresses required for marketing. Customers can manage their preferences or unsubscribe via Mailchimp. |
| **Existing controls that are in place to manage risks identified** | Mailchimp implements strong security. Mailchimp password only held by marketing staff. |
| **Assessment of current risk** | Low. Mailchimp’s security protects our mailing list adequately. Possible risk of unauthorised access by our internal staff. |
| **Recommended additional actions to reduce this risk** | Set up password manager to store strong password to Mailchimp. Implement access controls so password is only shared with minimal staff. Change password every 6 months. |
| **What is the new risk assessment after additional actions are implemented?** | Low/unlikely  Minimal harm |