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).

* The business is collecting information in regards to email and residential addresses for the purpose of marketing, sending promotional information to potential customers.
* The business records employee bank details so they can pay their workers.
* The business is collecting user information(accounts and passwords) so customers can set up accounts on the website
* The business collects medical history on their employees prior to hiring them so they can make sure they are fit for work.

## 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.

Residential addresses, usernames and passwords are collected via user input on the website, bank details and medical history of employees is collected by employee forms and medical professionals. The data needs to be stored on secure servers only accessible by the relevant staff members, e.g Marketing need to access customer information and Human Resources need to access to employee details.

The business has access controls in place for staff so only the correct staff can access the required information. The secure server has a strong password with 2 factor authentication and the password is changed every 3 months. The password is stored in a password manager.

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.  Residential address, username and password collected via account creation on website  Bank details and Medical Records collected via hiring process of employees. |
| **Description of the risk** | Risk of third-party obtaining mailing list, potential abuse (spam) of list.  Risk of external parties obtaining user or employee information, potential for employees to abuse power and obtain unnecessary customer information for inappropriate use. |
| **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.  Residential addresses, usernames and passwords required for promotional and delivery of products to customers. The consequences for the individual are they could have there private information disclosed by an external hacker or employee not following company protocols in regards to customer privacy.  Medical records and bank details need to be collected for hiring and paying employees. If an external source obtained these details then the employees personal information and bank accounts are at risk of being made public. |
| **Existing controls that are in place to manage risks identified** | Mailchimp implements strong security. Mailchimp password only held by marketing staff.  Secure servers, 2 factor authentication |
| **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 |