Privacy Impact Assessment Worksheet

Part 1 – Information Gathering

## Describe the project:

* The business is collecting information regarding 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:

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, IT need to access usernames and passwords to help any customers having account issues, 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. If there is a data breach, then the access control system can check who accessed the information at the time of breach. 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.

Customers can access and edit their details (password, email, address) at their own desire and remove account information if they wish to delete the account. Employees can update bank details through HR via forms, they can also expect any information regarding their bank details and medical records be removed upon their departure from the company.

Part 2 – Privacy Analysis

|  |  |
| --- | --- |
| **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 spam of list. * Risk of external parties obtaining user information, sell user info on dark web * Potential for Human Resources to abuse power and obtain unnecessary employee 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 their private information disclosed by an external hacker or employee not following company protocols regarding 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. * Access control system for employees who need to access customer sensitive data (passwords and addresses etc.) * Access control and secure storage with encryption of employee bank details and medical records to prevent hackers and unauthorised staff from accessing this info. |
| **Assessment of current risk** | * Low. Mailchimp’s security protects our mailing list adequately. Possible risk of unauthorised access by our internal staff. * Low. Staff accessing the customer info is logged so they cannot abuse power, possible risk of someone hacking the secure server would be low but hard to completely prevent. * Low. If HR don’t abuse power and release employee details, then they shouldn’t get leaked. |
| **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. * Strengthen and frequently change password for the secure server * Implement the latest and best security protection for the employee records, more chance of data breach if the software is old and cheap. |
| **What is the new risk assessment after additional actions are implemented?** | * Low/unlikely - Minimal harm * Very Unlikely – Minimal harm * Low – Potentially harmful though, due to bank and medical details being involved |