WRIGLEYS
— SOLICITORS —

GDPR MAY 2018

General Data Protection Regulation

Questionnaire to identify personal data held/processed by

[Name of charity or social enterprise]

Working to become Dementia Friendly

DAA Dementia Action Alliance

Lexcel Legal Practice Quality Mark Law Society Accredited

MINDFUL EMPLOYER

Living Wage Foundation

Introduction

The purpose of this questionnaire is to help the trustees/directors/management committee of the organisation identify the types of personal data held/processed by the organisation and its advisers and service providers and the processing carried out by and on behalf of them.

Your responses will help:

- to draft a comprehensive data protection policy and privacy notices,
- to identify where individual consent may be required to the processing of personal data,
- to provide you with better instructions regarding the processing of personal data relating to the organisation, and
- to put in place appropriate contractual provisions which regulate, amongst other things, the transfer, processing, retention and security of personal data by the organisation.

Questionnaire completed by : (*insert your name*)	
Questionnaire completed on behalf of: (*insert name of organisation*)	
Date:	

Questionnaire

1.	**What personal data does the organisation hold/process?** Identify "types" of personal data held/processed by the organisation and by reference to the different "categories" of data subjects. Categories of data subjects might include, for example, members, beneficiaries or staff.

Personal data means *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

"Processing" *means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

Generic data held in relation to all categories:	
Members:	
Beneficiaries:	
Staff:	
Donors:	
Volunteers:	
Trustees:	
Directors:	

2.	What sensitive data does the organisation hold/process?

Sensitive data covers *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*.

3.	In relation to each item of data identified under 1 and 2 above, please indicate: • how long the organisation intends to hold/process the data and • why (i.e. what criteria does the organisation use to determine the relevant period)?

4.	**Does the organisation share personal data or sensitive data with third parties?** If yes, please provide details.

5.	**Does the organisation send personal or sensitive data in an encrypted format:** **a. within the organisation?** b. **outside the organisation?**

6.	**In relation to each item of data identified under 1 and 2 above, does the organisation hold/process any data which is not necessary for its day to day administration?** If yes, please provide details.

7.	**In relation to each item of data identified under 1 and 2, what steps does the organisation take to ensure the data is accurate and up to date?**

8.	**In relation to each item of data identified under 1 and 2, what security measures does the organisation take to protect data against unauthorised / unlawful processing and against accidental loss, destruction and damage?**

9.	**What consents (if any) have data subjects given to the holding/processing of personal data? Compile copies of consents. Is the obtaining of data subject consent built into any processes (e.g. membership or other application forms)?**

10.	**Does the organisation hold/process the personal data of children under the age of 16?** Please give details regarding the type of data held/processed and the length of time for which such data is typically held/processed.

11.	**Has any personal data held/processed by the organisation been transferred overseas or does the organisation intend to transfer personal data overseas in the future?** If yes, please provide details.

12.	**What steps is the organisation taking to ensure that it complies with the GDPR? In particular, what measures is it taking to comply with Article 32?**

Article 32 provides*, inter alia, that the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate:*

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

13.	**Who holds and / or processes personal data relating to the organisation other than the organisation?** Consider: • professional advisers (lawyers, accountants etc) • IT/internet service providers • payroll providers

14.	a. **What privacy notices have been issued by the organisation** b. **What data protection and / or cyber security and/or data retention and destruction policies that apply to the organisation exist?** **In each case, compile copies.**

15.	**How secure is personal data held by the organisation?** Consider how personal data is shared. If personal data is shared by email, is the data routinely encrypted / password protected? Who has access to the emails / computers?

16.	a. **If the organisation has a parent, umbrella or partner organisation, what steps are they taking in relation to GDPR?** b. **Are there any areas where both organisations can work together? (For example, agreeing a cyber security policy? A disaster recovery policy? The aim here would be to share any expertise in these areas)**