**[The sections below in red type cover the specific tasks which must be designated to any statutory appointed Data Protection Officer under Article 39 of the GDPR.]**

**TEMPLATE JOB DESCRIPTION & PERSON SPECIFICATION**

**Job Title**: Data Protection Co-Ordinator/Lead

**Overall Summary**

This post is key in supporting [name of organisation] to ensure compliance with both national and European data protection laws and in advising [name of organisation] of the changes required to comply with the General Data Protection Regulation (“GDPR”) which comes into force on 25 May 2018.

The post holder will be involved in all issues relating to data protection, in particular Data Protection Impact Assessments (“DPIAs”) and privacy by design.

The post holder will be part of working groups detailing with data processing activities within an organisation and will be regularly involved in meetings of senior and middle management.

The post holder will report to the [Board of Directors/Trustees].

**Key tasks and responsibilities**

1. To inform and advise [name of organisation] and its employees about their obligations to comply with the GDPR and other data protection laws.
2. To monitor compliance with the GDPR and other data protection laws, including managing internal data protection policies and activities including assigning responsibilities. This includes:
	* Collecting information to identifying processing activities;
	* Analysing and checking the compliance of processing activities;
	* Informing, advising and issuing recommendations to [the Board of Trustees/Directors]
3. To develop and deliver a comprehensive data protection awareness and training programme for staff and conduct internal audits.
4. To foster a data protection culture within the organisation and help to implement essential elements of the GDPR, such as the principles of data processing, data subjects’ rights, data protection by design and by default, records of processing activities, security of processing, awareness training, and notification and communication of data breaches.
5. To provide advice on DPIAs and monitor whether processing is performed in accordance with DPIAs undertaken. This will include:
* advising on whether or not to carry out a DPIA;
* what methodology to follow;
* whether to carry out the DPIA in house or outsource it;
* what safeguards to apply to mitigate any risks;
* whether or not the DPIA has been correctly carried out and whether its conclusions are in compliance with the GDPR.
1. To have overall responsibility for dealing with personal data breaches, including any reporting requirements.
2. To have overall responsibility for dealing with requests for:
	1. access to personal data;
	2. rectification of inaccurate personal data;
	3. erasure of personal data;
	4. restriction of processing of personal data;
	5. data portability;

together with overall responsibility for complying with the notification requirements where data is rectified and/or erased and/or where processing of personal data is restricted.

1. To act as the point of contact for the Information Commissioner’s Office (“ICO”) and any other relevant supervisory or regulatory authorities on issues relating to processing and any other data protection matters.
2. To cooperate with the ICO for example to facilitate access by the ICO to documents and information and to assist the ICO in the exercise of its investigative, corrective and advisory duties.
3. To identify and manage risks related to data protection, and escalate data protection risks and issues to [the Board of Directors/Trustees], as appropriate.
4. To provide comprehensive reports to the [the Board of Directors/Trustees?] on the organisation’s compliance with data protection legislation.
5. To maintain the organisation’s data protection records.

**Expertise and professional qualities**

1. [Expert/In depth] knowledge of data protection law and practices.
2. Knowledge of IT systems and data security.
3. Integrity and high professional ethics.
4. Excellent written and verbal communication skills.
5. Ability to work under pressure and deal with a demanding workload which may include conflicting demands on time.
6. Ability to communicate effectively with the highest levels of management and decision-making individuals within the organisation.
7. Ability to interpret complex legislative requirements.
8. Good judgement, with the ability to make considered decisions.
9. Ability to work on own initiative and as a member of a team.
10. Familiarity with privacy and security risk assessment, best practices and gap analysis, privacy certifications/seals, and information security certifications.