CHECKLIST – PREPARING FOR THE GDPR

1) Awareness

- Ensure that decision-makers and key staff know about the GDPR and understand its likely impact.

2) Personal data you hold

- Conduct an information audit across your business to identify and understand personal data flows.
  - What 'personal data' do you hold?
  - Where did it come from?
  - What is the lawful basis for processing it?
  - Why do you need it?
  - Who is it shared with?
  - Where is it stored?
  - From where is it accessed?
  - How long is it being kept for?

3) Lawful basis for processing personal data

- Review all the various types of processing activities that you carry out.
- Identify and document the lawful basis for each of your processing activities.
- Review whether these are appropriate and whether another lawful basis is required.

  ⇨ The individual has given consent; or
  ⇨ Necessary for performance of a contract with the individual or to take steps to enter into a contract; or
  ⇨ Necessary for compliance with a legal obligation to which your business is subject; or
  ⇨ Necessary for the purposes of the legitimate interests of your business or a third party, except where such interests are overridden by the interests or rights of the individual.

  And for "sensitive data" (e.g. personal data concerning health), also need:
  ⇨ The individual has given explicit consent; or
  ⇨ Necessary for carrying out obligations and exercising rights under employment or social security law.

4) Consent

- Review how you seek, record and manage consent.
- Do you need to refresh any existing consents to meet the GDPR standard?
- Or find another lawful basis?

5) Accountability

- You must be able to demonstrate your compliance with all six data processing principles.
  - Lawfulness, fairness and transparency
  - Purpose limitation
  - Data minimisation
  - Accuracy
  - Storage limitation
  - Security, integrity and confidentiality

- Implement appropriate technical and organisational measures to ensure that processing is performed in accordance with the GDPR and a level of security appropriate to the risk
- Implement internal policies and processes
- Maintain documentation and keep records of compliance (check if Article 30 applies)
- Conduct regular training to integrate and embed data processing policies and procedures
- Use ongoing testing and internal auditing to demonstrate your compliance

- Data Protection by Design and by Default
- Data Protection Impact Assessments
- Approved codes of conduct and/or certification schemes, should these become available

6) Privacy Policy [Privacy Statement] [Privacy Notice]

- Prepare and maintain a compliant Privacy Policy
- Ensure this is provided to individuals in a clear and accessible format, and on a timely basis.

7) Security breach management

- Ensure that you have the right procedures in place to detect, report and investigate a personal data breach
- Implement a data breach response plan and document all incidents
- Staff training and awareness

8) Data subject rights

- Establish procedures and documentation to ensure that you can facilitate all the rights that individuals have under the GDPR within the required time periods.
    - Policies and procedures for responding to access requests and other requests
    - Template letters and forms
    - Inventory or log for recording requests and for tracking responses

9) Data Protection Officer (DPO)

- Is appointing a DPO mandatory for your business? If yes, action this and document the appointment.
- If no, assuming you are not appointing a voluntary DPO, document the decision, and designate a lead person for data protection issues (don't use the title 'Data Protection Officer' or 'DPO').
- Provide your DPO or lead person with adequate training, resources and ongoing support.

10) Transfer of personal data outside of the EEA

- Implement and document compliant data transfer mechanisms

11) Data Processors

- Implement a policy for engaging your data processors.
- Contracts and mandatory terms.
- Are you acting as a data processor?

12) Organisational Policies

- Data Protection Policy
    - Collection and use of personal data
    - Collection and use of sensitive personal data
    - Secondary uses of personal data.
    - Obtaining valid consent.
    - Maintaining data quality.
    - Anonymising or pseudonymizing data.
    - Personal data retention and secure destruction.
    - Security breach management.
    - Using personal data for direct marketing.
    - Information security including the specific security measures implemented.

- Data subject access and rights procedures
- CCTV Policy and Notice
- Employee Privacy Policy and Notice (email, internet, communications usage and monitoring)