General Data Protection Regulation Policy

1. **Purpose**
   The purpose of this policy is to ensure compliance with the General Data Protection Regulation (GDPR) and relevant UK data protection laws.

2. **Definitions**
   Spring Care For You is registered with the Information Commissioner's Office as a 'controller'. In the context of the GDPR:

   - **Controller**: The person, public authority, agency, or body that determines the purposes and means of processing personal data.
   - **Processing**: Any operation performed on personal data, whether automated or not, such as collection, recording, storage, use, or erasure.
   - **Personal Data**: Any information relating to an identified or identifiable person.
   - **Processor**: A person or organisation that processes data on behalf of the controller.
   - **Consent**: A freely given, specific, informed, and unambiguous indication of the data subject's wishes.

3. **The Rights of Data Subjects**
   Spring Care For You fully respects the rights of data subjects as stipulated in the GDPR. These include the right to:

   - Transparent communication regarding data processing.
   - Access to personal data.
   - Rectification of incorrect data.
   - Erasure (the right to be forgotten).
   - Restriction of processing.
   - Data portability.
   - Object to processing.

- Automated decision-making restrictions.

4. **Special Categories of Personal Data**
   GDPR specifies special categories of personal data, including:
   - Racial or ethnic origin
   - Political opinions
   - Religious or philosophical beliefs
   - Trade union membership
   - Genetic data
   - Biometric data
   - Health data
   - Data concerning sex life or sexual orientation
     Processing of such data is prohibited unless there is a legitimate ground for processing, such as a legal obligation or a court order.

5. **Consent**
   Consent is only one lawful basis for processing personal data. Spring Care For You uses clear, plain language in consent forms and ensures data subjects can withdraw consent at any time. For children, consent is verified by someone with parental responsibility.

6. **Key Roles in Processing Personal Data**
   - **Controller**: The organisation is accountable for GDPR compliance and must be able to explain its data processing activities to data subjects and the Information Commissioner's Office (ICO).
   - **Processor**: Processors must meet all GDPR obligations as outlined in data processing agreements.

- **Data Protection Officer (DPO)**: The DPO advises on GDPR compliance and ensures that the company takes appropriate measures to protect personal data.

7. **Accountability**
   Spring Care For You ensures GDPR compliance by:
   - Implementing technical and organisational measures.
   - Maintaining relevant documentation.
   - Proactively reviewing data protection procedures.
8. **Data Protection Impact Assessment (DPIA)**
   DPIAs are conducted when processing activities pose a high risk to data subjects' rights, particularly for special categories of data. Spring Care For You follows the ICO's screening checklist to assess whether a DPIA is required.
9. **Security of Personal Data and Privacy by Design**
   Spring Care For You ensures that privacy is integrated into all systems, using measures such as:
   - Real-time data encryption
   - Encrypted memory sticks
   - Strong password protection
   - Locked filing cabinets for physical data
     Additional methods include anonymisation, redaction, and pseudonymisation, depending on the nature of the data.
10. **Data Subject Access Request (DSAR)**
    Individuals may submit a DSAR in writing, requesting access to their personal data. Spring Care For You responds to DSARs within 30 days, verifying the identity of the requester, and providing the information unless the request is manifestly unfounded or excessive.
11. **Cross-border Processing**
    Spring Care For You processes personal data exclusively within the UK and does not transfer data outside of the UK.

12. **Record of Processing Activities (ROPA)**
    Spring Care For You maintains a record of processing activities that includes details such as:

- Purpose of processing
- Categories of data subjects
- Retention period
- Security measures

    This document ensures transparency and allows for monitoring of data processing activities.

13. **Personal Data Retention**
    Personal data is not kept for longer than necessary. The Data Protection Officer maintains a retention schedule that outlines the retention period for each type of document.

14. **Personal Data Breach**
    In the event of a personal data breach, Spring Care For You reports the incident to the ICO within 72 hours if there is a risk to the rights and freedoms of data subjects. Data subjects are also notified if the breach poses a high risk to their rights.

15. **GDPR Compliance by Processors**
    Spring Care For You has written agreements with processors to ensure they meet GDPR compliance requirements.

16. **Transparency through Privacy Statement**
    Privacy statements are provided to all data subjects and are reviewed regularly. These statements are written in clear, plain language and explain how personal data is processed.

17. **Training**
    All staff receive GDPR training, and ongoing training is provided to raise awareness and reinforce best practices for data protection.

18. **Related Documents**

- **GDPR Personal Data Retention Schedule**
- **GDPR ROPA**
- **GDPR DPIA Checklists**

19. **Revision History**

- Date of next review: September 2025
- Date of release: September 2024

Legal Updates for 2024

The **UK GDPR** remains in place following Brexit, with amendments reflecting domestic law under the **Data Protection Act 2018**. Key updates include:

- Enhanced requirements for **data protection impact assessments (DPIAs)**, particularly for high-risk data processing(GDPR Policy (1)).
- Strengthened reporting requirements for **data breaches**, requiring notification to the ICO within 72 hours unless the risk is minimal(GDPR Policy (1)).

This version is fully compliant with 2024 GDPR regulations.