

**Template Data Protection Policy**

|  |  |
| --- | --- |
| Author |  |
| Last updated |  |
| Review Due |  |

## Definitions

|  |  |
| --- | --- |
| **GDPR** | means the General Data Protection Regulation 2018. |
| **Responsible Person** | means **[insert name of person responsible for data protection within the Organisation].** |
| **Data Processing Inventory** | means a register of all systems or contexts in which personal data is processed by the Organisation |

### 1. Data protection principles

**ORGANISATION NAME** is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

### 2. General provisions

1. This policy applies to all personal data processed by **ORGANISATION NAME.**
2. The Responsible Person shall take responsibility for **ORGANISATION NAME** ongoing compliance with this policy.
3. This policy shall be reviewed annually or where otherwise indicated, whichever is sooner.
4. **ORGANISATION NAME** shall maintain registration with the Information Commissioner’s Office as an organisation that controls and processes personal data.
5. **ORGANISATION NAME** has appointed **DPO NAME** as the Data Protection Officer.

### 3. Lawful, fair and transparent processing

1. To ensure its processing of data is lawful, fair and transparent, **ORGANISATION NAME** shall maintain a Data Processing Inventory and Breach Notice Register.
2. The Data Processing Inventory shall be reviewed at annually or where otherwise indicated, whichever is sooner.
3. Individuals have the right to access their personal data and any such requests made to **ORGANISATION NAME** shall be dealt with in a timely manner.
4. **ORGANISATION NAME** shall publish Fair Process Notices on the practice website and make these notices available in paper form should they be requested.
5. Poster(s) shall be shown in the Practice waiting room to publicise our commitment to privacy by design and default.

### 4. Lawful purposes

1. All data processed by **ORGANISATION NAME** must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.
2. **ORGANISATION NAME** shall note the appropriate lawful basis in the Data Processing Inventory.
3. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
4. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in **ORGANISATION NAME** systems.

### 5. Data minimisation

1. **ORGANISATION NAME** shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

### 6. Accuracy

1. **ORGANISATION NAME** shall take reasonable steps to ensure personal data is accurate.
2. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

### 7. Archiving / removal

1. To ensure that personal data is kept for no longer than necessary, **ORGANISATION NAME** shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
2. The archiving policy shall consider what data should/must be retained, for how long, and why.

### 8. Security

1. **ORGANISATION NAME** shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
2. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
3. When personal data is deleted this should be done safely such that the data is irrecoverable.
4. Appropriate back-up and disaster recovery solutions shall be in place.

### 9. Breach

1. In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, **ORGANISATION NAME** shall promptly assess the risk to people’s rights and freedoms and if appropriate report this breach to the ICO.
2. The Practice response to loss of personal data shall be managed in accordance with the **ORGANISATION NAME** Data Breach Policy.