# UK GDPR Information Audit

The [insert practice name] processes personal data that relate to employees and patients and is therefore required by law to comply with the UK General Data Protection Regulations (UK GDPR), which protects the privacy of individual personal data and ensures that they are processed fairly and lawfully.

This information audit will list the types of personal data processed, the reasons we hold this information, how and why this information was initially gathered, the lawful basis for data processing, the retention period, data storage and security and the third parties with whom we might share the data.

The [insert practice name] will conduct regular reviews of personal data to ensure that it remains accurate and up to date.

Date of Review: [insert date]

Name of Reviewer: [insert name]

Date of Next Review: [insert date]

[Amend/update the categories in this table to include all types of personal data held by the practice. If you transfer data to countries outside the UK, you must document this and describe the safeguards applied to ensure the data remains secure. If you discover that you have shared incorrect information with another organisation, inform them that the information was incorrect, and the changes required to rectify this.]

| **Type of personal data processed** | **Purpose of processing** | **Lawful basis** | **Is special category data processed?** | **Special category processing basis (if applicable)** | **How is data collected** | **How is data stored** | **How is data kept secure** | **How long is the data stored?** | **Is this data shared?** | **Who is the data shared with?(if applicable)** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [e.g. Patient contact details] | [e.g. Recall notices, appointment reminders] | [Insert lawful basis] | [Yes/no] | [Insert special category processing basis or N/A] | [e.g. When patient registers and checked at every appointment] | [e.g. Stored on a secure password-protected practice computer] | [e.g. Password protected, encrypted, accessed by authorised staff only, regular back-ups] | [e.g. adult patients at least 10 years; child patients 10 years. On death, adult records are kept for 3 years. Where the person dies before their 17th birthday, the record should be held until they would have turned 25.    | [Yes/no] | [e.g. with other healthcare professionals, NHS payment authorities, benefits agencies] |
| [e.g. Patient dental, social and medical histories] | [e.g. Patient care] | [Insert lawful basis] | [Yes/no] | [Insert special category processing basis or N/A] | [e.g. When patient registers and checked at every appointment] | [e.g. Stored on a secure password-protected practice computer] | [e.g. Password protected, encrypted, accessed by authorised staff only, regular back-ups] | [e.g. adult patients at least 10 years; child patients 10 years. On death, adult records are kept for 3 years. Where the person dies before their 17th birthday, the record should be held until they would have turned 25.    | [Yes/no] | [e.g. with other healthcare professionals] |
| [e.g. Patients’ GP contact details] | [e.g. Patient care] | [Insert lawful basis] | [Yes/no] | [Insert special category processing basis or N/A] | [e.g. When patient registers] | [e.g. Stored on a secure password-protected practice computer] | [e.g. Password protected, encrypted, accessed by authorised staff only, regular back-ups] | [e.g. adult patients at least 10 years; child patients 10 years. On death, adult records are kept for 3 years. Where the person dies before their 17th birthday, the record should be held until they would have turned 25.    | [Yes/no] | [e.g. with other healthcare professionals] |
| [e.g. Patient treatment record, inc. radiographs and clinical photographs] | [e.g. Patient care] | [Insert lawful basis] | [Yes/no] | [Insert special category processing basis or N/A] | [e.g. Updated at every appointment] | [e.g. Stored on a secure password-protected practice computer] | [e.g. Password protected, encrypted, accessed by authorised staff only, regular back-ups] | [e.g. adult patients at least 10 years; child patients 10 years. On death, adult records are kept for 3 years. Where the person dies before their 17th birthday, the record should be held until they would have turned 25.    | [Yes/no] | [e.g. with other healthcare professionals] |
| [e.g. records of treatment provided and costs] | [e.g. Patient care] | [Insert lawful basis] | [Yes/no] | [Insert special category processing basis or N/A] | [e.g. Updated at every appointment] | [e.g. Stored on a secure password-protected practice computer] | [e.g. Password protected, encrypted, accessed by authorised staff only, regular back-ups] | [e.g. adult patients at least 10 years; child patients 10 years. On death, adult records are kept for 3 years. Where the person dies before their 17th birthday, the record should be held until they would have turned 25.    | [Yes/no] | [e.g. with other healthcare professionals, NHS payment authorities, benefits agencies] |
| [e.g. proposed care, inc. advice, referrals] | [e.g. Patient care] | [Insert lawful basis] | [Yes/no] | [Insert special category processing basis or N/A] | [e.g. Updated at every appointment] | [e.g. Stored on a secure password-protected practice computer] | [e.g. Password protected, encrypted, accessed by authorised staff only, regular back-ups] | [e.g. adult patients at least 10 years; child patients 10 years. On death, adult records are kept for 3 years. Where the person dies before their 17th birthday, the record should be held until they would have turned 25.    | [Yes/no] | [e.g. with other healthcare professionals] |
| [e.g. details of consent] | [e.g. Patient care] | [Insert lawful basis] | [Yes/no] | [Insert special category processing basis or N/A] | [e.g. collected when necessary] | [e.g. Stored on a secure password-protected practice computer] | [e.g. Password protected, encrypted, accessed by authorised staff only, regular back-ups] | [e.g. adult patients at least 10 years; child patients 10 years. On death, adult records are kept for 3 years. Where the person dies before their 17th birthday, the record should be held until they would have turned 25.    | [Yes/no] | [e.g. with other healthcare professionals] |
| [e.g. details of correspondence with other healthcare professionals] | [e.g. Patient care] | [Insert lawful basis] | [Yes/no] | [Insert special category processing basis or N/A] | [e.g. collected when necessary] | [e.g. Stored on a secure password-protected practice computer] | [e.g. Password protected, encrypted, accessed by authorised staff only, regular back-ups] | [e.g. adult patients at least 10 years; child patients 10 years. On death, adult records are kept for 3 years. Where the person dies before their 17th birthday, the record should be held until they would have turned 25.    | [Yes/no] | [e.g. with other healthcare professionals] |
| [e.g. Appointment information] | [e.g. Practice administration] | [Insert lawful basis] | [Yes/no] | [Insert special category processing basis or N/A] | [e.g. Updated at every appointment] | [e.g. Stored on a secure password-protected practice computer] | [e.g. Password protected, encrypted, accessed by authorised staff only, regular back-ups] | [e.g. retention period for practice appointment systems] | [Yes/no] | [e.g. with NHS payment authorities, benefits agencies] |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| [e.g. Employee contact details] | [e.g. Payroll, personnel file] | [Insert lawful basis] | [Yes/no] | [Insert special category processing basis or N/A] | [e.g. At recruitment; at start of employment] | [e.g. Stored on a secure password-protected practice computer] | [e.g. Password protected, encrypted, accessed by authorised staff only, regular back-ups] | [Insert relevant retention period] | [Yes/no] | [e.g. with the HM Customs and Revenue, pension providers, professional bodies] |
| [e.g. Employee qualifications] | [e.g. Personnel file] | [Insert lawful basis] | [Yes/no] | [Insert special category processing basis or N/A] | [e.g. At recruitment; at start of employment] | [e.g. Stored on a secure password-protected practice computer] | [e.g. Password protected, encrypted, accessed by authorised staff only, regular back-ups] | [Insert relevant retention period] | [Yes/no] | [e.g. with professional bodies] |
| [e.g. Employee bank details] | [e.g. Payroll] | [Insert lawful basis] | [Yes/no] | [Insert special category processing basis or N/A] | [e.g. At start of employment] | [e.g. Stored on a secure password-protected practice computer] | [e.g. Password protected, encrypted, accessed by authorised staff only, regular back-ups] | [Insert relevant retention period] | [Yes/no] | [e.g. with the processors of our payroll] |
| [e.g. Employee pension details] | [e.g. Payroll] | [Insert lawful basis] | [Yes/no] | [Insert special category processing basis or N/A] | [e.g. At start of employment] | [e.g. Stored on a secure password-protected practice computer] | [e.g. Password protected, encrypted, accessed by authorised staff only, regular back-ups] | [Insert relevant retention period] | [Yes/no] | [e.g. with the processors of our payroll, pension providers] |
| [e.g. Employee tax details] | [e.g. Payroll] | [Insert lawful basis] | [Yes/no] | [Insert special category processing basis or N/A] | [e.g. At start of employment] | [e.g. Stored on a secure password-protected practice computer] | [e.g. Password protected, encrypted, accessed by authorised staff only, regular back-ups] | [Insert relevant retention period] | [Yes/no] | [e.g. with the processors of our payroll, pension providers] |
| [e.g. Employee pay details] | [e.g. Payroll, personnel file] | [Insert lawful basis] | [Yes/no] | [Insert special category processing basis or N/A] | [e.g. At start of employment] | [e.g. Stored on a secure password-protected practice computer] | [e.g. Password protected, encrypted, accessed by authorised staff only, regular back-ups] | [Insert relevant retention period] | [Yes/no] | [e.g. with the HM Customas and Revenue pension providers, professional bodies] |
| [e.g. Employee annual leave details] | [e.g. Personnel file] | [Insert lawful basis] | [Yes/no] | [Insert special category processing basis or N/A] | [e.g. annual leave forms submitted by employee] | [e.g. Stored on a secure password-protected practice computer] | [e.g. Password protected, encrypted, accessed by authorised staff only, regular back-ups] | [Insert relevant retention period] | [Yes/no] | [Insert relevant reason if data is shared] |
| [e.g. Employee sickness absence details] | [e.g. Personnel file] | [Insert lawful basis] | [Yes/no] | [Insert special category processing basis or N/A] | [e.g. sickness absence forms submitted by employee] | [e.g. Stored on a secure password-protected practice computer] | [e.g. Password protected, encrypted, accessed by authorised staff only, regular back-ups] | [Insert relevant retention period] | [Yes/no] | [Insert relevant reason if data is shared] |
| [e.g. Employee performance/appraisal details] | [e.g. Personnel file] | [Insert lawful basis] | [Yes/no] | [Insert special category processing basis or N/A] | [e.g. appraisal forms completed annually] | [e.g. Stored on a secure password-protected practice computer] | [e.g. Password protected, encrypted, accessed by authorised staff only, regular back-ups] | [Insert relevant retention period] | [Yes/no] | [Insert relevant reason if data is shared] |
| [e.g. Employee training details] | [e.g. Personnel file] | [Insert lawful basis] | [Yes/no] | [Insert special category processing basis or N/A] | [e.g. training details updated as required] | [e.g. Stored on a secure password-protected practice computer] | [e.g. Password protected, encrypted, accessed by authorised staff only, regular back-ups] | [Insert relevant retention period] | [Yes/no] | [e.g. with the professional bodies] |
| [e.g. Employee health clearance and immunisation status] | [e.g. Health and Safety] | [Insert lawful basis] | [Yes/no] | [Insert special category processing basis or N/A] | [e.g. At start of employment; changes in status] | [e.g. Stored on a secure password-protected practice computer] | [e.g. Password protected, encrypted, accessed by authorised staff only, regular back-ups] | [Insert relevant retention period] | [Yes/no] | [e.g. with the professional bodies] |
|  |  |  |  |  |  |  |  |  |  |  |