**Annex A** – **EXAMPLE OF RECORD KEEPING IN TYPICAL PRACTICE**

**Name of Controller: Address of Controller: Telephone/Email: DPO:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category of personal data and data subject** | **Legal basis for processing personal data** | **Who these personal data are shared with** | **Time limits for erasure** | **Technical/organisational security measures to ensure level of security appropriate to risks** |
| **GOS patient records – including retinal photographs, referral letters etc.** | The condition for processing special category data - the provision of health care. The lawful bases - the performance of a task carried out in the public interest and legitimate interests | Registered health care professionals and those under their supervision | The NHS specifies 7 years or, in the case of children under 18, until their 25th birthday.  Accepted good practice in the profession is that records should be kept for 10 years after last contact with the patient. | Only registered health care staff have access to the complete patient record. All registered staff comply with GOC standards, which ensure they respect patient confidentiality. Paper records are kept securely. Electronic data is password protected, employees can only access the information essential for their role, all employees have passwords so there is an audit of any changes made, there is also a back-up system that means data can be restored. All anti-virus software and other software are kept up to date. |
| **Private patient records and NHS patients seen under the NHS Standard Contract – including retinal photographs, referral letters**  **etc.** | The condition for processing special category data - the provision of health care. The lawful basis - legitimate interests | Registered health care professionals and those under their supervision | The NHS specifies 7 years or, in the case of children under 18, until their 25th birthday.  Accepted good practice in the profession is that records should be kept for 10 years after last contact with the patient. | Only registered health care staff have access to the complete patient record. All registered staff comply with GOC standards, which ensure they respect patient confidentiality. Paper records are kept securely. Electronic data is password protected, employees can only access the information essential for their role, all employees have passwords so there is an audit of any changes made, there is also a back-up system that means data can be restored. All anti-virus software and other software are kept up to date. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Customer records –** e.g. direct debit/payment details | Legitimate interest | The data subject’s  bank | Kept for tax purposes and future claims/information | Paper records are kept securely. Electronic data is password protected, employees can only access the information essential for their role and receive appropriate training for their role. All employees have passwords so there is an audit of any changes made, there is also a back-up system that means data can be restored. All anti-virus software and other software are kept up to date. |
| **Staff records – includes bank details, NI number, and other personal information** | Any special category data, the condition is processing is necessary for carrying out obligations as an employer.  Lawful basis: performance of a contract with the data subject or to take steps to enter into a contract, legal obligation (tax) and legitimate interests (absence monitoring). | HR (including payroll) and senior management only | Kept for tax purposes and future claims/information | Paper records are kept securely. Electronic data is password protected, employees can only access the information essential for their role and receive appropriate training for their role. All employees have passwords so there is an audit of any changes made, there is also a back-up system that means data can be restored. All anti-virus software and other software are kept up to date. |

# Annex B – LAWFUL BASES FOR PROCESSING PERSONAL DATA

Practices and businesses will need to have **at least one** lawful basis for each processing activity.

Practices will need to have **at least one** lawful basis for processing personal data from Table 1. In addition, when processing special category personal data, such as health information, they will also need one condition for processing from Table 2.

Table 1

|  |  |
| --- | --- |
| **Lawful basis for processing personal data** | **Notes** |
| 1. **Consent** of the data subject | Should **NOT** be used as the lawful basis for health records or employee records. Most likely to be the lawful basis when data is processed for marketing purposes. Please note that there are other regulations to consider when using personal data for marketing. For more details on marketing please also see the [ICO guidance on](https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf) [direct marketing.](https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf)  Also note that the EU is giving consideration to reforming the existing e-Privacy  Directive, with the aim of harmonising it with the GDPR. |
| 2.Processing is necessary for the **performance of a contract** with the data subject or to take steps to enter into a contract | Employment contracts and data held on employees that is consistent with the contract of employment. |
| 3.Processing is necessary for **compliance with a legal obligation** | Might be used by a practice, for example to comply with tax law. It is not necessary  to cite each specific piece of legislation. |
| 4.Processing is necessary to protect the vital **interests** of a data subject or another person | Unlikely to be used by optical practices and businesses. |
| 5.Processing is necessary for the performance of a task carried out in the  **public interest** or in the exercise of official authority vested in the controller | Most likely to be the lawful basis for processing health record for GOS patients. As  special category data lawful processing also requires a condition from Table 2. |
| 6.Necessary for the purposes of **legitimate interests** pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject (Note that this condition is not available to processing carried out by public authorities in the performance of their tasks). | Likely to be the lawful basis for health records for private patients and NHS patients treated through the NHS Standard Contract. May be used as the lawful basis for marketing to patients and others. Lawful processing for any special category data also requires a condition from Table 2. |

**Table 1:** Legal basis for processing personal data, modified ICO table: source [https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-](https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/key-areas-to-consider/) [gdpr/key-areas-to-consider/](https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/key-areas-to-consider/)

Table 2

|  |  |
| --- | --- |
| **Condition for processing special categories of personal data** | **Notes** |
| A. Explicit **consent** of the data subject, unless reliance on consent is  prohibited by the DPA2018 | Unlikely to rely on this condition. Health professionals are more likely to rely on  condition H below. |
| B. Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement | Practices might rely on this condition. |
| C. Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of  giving consent | Unlikely that practices will rely on this condition. |
| D. Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no  disclosure to a third party without consent | Unlikely that practices will rely on this condition. |
| E. Processing relates to personal data manifestly made public by the data subject | Unlikely that practices will rely on this condition. |
| F. Processing is necessary for the establishment, exercise or defence of legal  claims or where courts are acting in their judicial capacity | It is possible that health care records and other special categories of data might have  to be shared in this context – e.g. sharing of patient records with regulators. |
| G. Processing is necessary for reasons of substantial public interest on the  basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards | Unlikely that practices will rely on this condition. |
| H. Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or  Member State law or a contract with a health professional | Practices will rely on this provision when processing health records. |
| I. Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical  devices | Unlikely that practices will rely on this condition. |
| J. Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1) | Unlikely that practices will rely on this condition. |

# Annex C - INDIVIDUAL RIGHTS

The table below sets out the eight rights individuals will have under the new law.

|  |  |
| --- | --- |
| **Right** | **What does this mean in my practice or business?** |
| **The right to be informed** | * Be transparent about how you use personal data by letting patients and customers have access to ‘fair processing information’ – e.g. by using a privacy notice. * Supply this information in a way that is: concise, transparent, intelligible and easily accessible; written in clear and plain language, particularly if addressed to a child; and free of charge. * For more information on privacy statements see section 2.6. |
| **The right of access** | * If you process personal data then individuals – e.g. customers, patients, staff – can ask what you are processing and why, and ask for copies of that data, see section 2.6. |
| **The right to rectification** | * Individuals can ask you to rectify personal data if it is inaccurate or incomplete. * Respond to such requests within one month, although if it is a complicated request you might be able to extend this by two months. |
| **The right to erasure** | * This is also known as ‘the right to be forgotten’ – e.g. a person might be able to ask you to delete or remove personal data you hold on them. * This applies where there is no compelling reason for its continued processing. It is therefore **not** applicable where there is a duty to keep accurate records – e.g. keeping health and employee records is often a legal requirement or best practice and a requirement in case of a legal   claim etc. |
| **The right to restrict processing** | * A customer has the right to ‘block’ or suppress you processing their data in certain circumstances. This is unlikely to apply in a typical optical practice. * If there is a basis for a customer to exercise this right then you can store the personal data, but not further process it. |
| **The right to data portability** | * This is unlikely to apply to optical practices because it applies when processing is carried out by automated means. |
| **The right to object** | * Individuals can object to you processing their personal data in certain circumstances * If you used “legitimate interest” as the lawful basis for processing personal data and an individual objects you must stop processing data **unless** you can a) demonstrate how your legitimate interests override the interests, rights and freedoms of the individual or b) you are processing the data for the establishment, exercise or defence of legal claims * If an individual objects to you processing personal data for direct marketing, you must stop processing data for that purpose. |
| **The right not to be subject to automated decision- making including**  **profiling** | * This is unlikely to apply in optical settings. |