Produced by **Supported by**

Data Protection Law - Information and Guidance

September 2026

Produced for the optical profession in the UK by FODO supported by ABDO and AOP.

ABOUT THIS GUIDANCE

This guidance aims to help the sector – including optical practices, manufacturers/suppliers/distributors, and employees – understand data protection rules and what they mean.

We will continue to work with the Information Commissioner's Office (ICO), the NHS and other primary care contractor professions, to ensure an approach that does not place disproportionate burdens on the sector whilst fully protecting the personal data of patients, customers and staff.

The guidance is in two parts:

- Part one: What you need to know – provides a basic overview of data protection rules.
- Part two: What you need to do – explains what steps you need to take.

We will update this guidance as necessary in response to new guidance from the ICO and the NHS.

CONTENTS

ABOUT THIS GUIDANCE 1
1.1 The law at a glance 3
1.2 Key terms 3
1.3 Principles of data protection 4
PART 2: WHAT YOU NEED TO DO 4
2.1 Key roles and responsibilities 5
2.2 Getting people involved 6
2.3 Demonstrating compliance and accountability 7
2.4 Identifying the lawful basis for processing personal data 9
Patient data 9
Customer and marketing data 10
Employee records and data 11
Health care records 11
Patient correspondence 11
Referrals 11
Customer data for other purposes – e.g. advertising and marketing 12
2.6 Understanding and complying with individual rights 12
Right to be informed: privacy notices 13
Right to access: responding to requests 13
Right to erasure: right to be forgotten 14
National data opt-out (NDOO) – England 14
2.7 Data breaches – prevention and reporting requirements 15
Preventing a data breach 15
Action in the event of a data breach 15
Informing individuals affected 16
2.8 Further information 17
Annex A – EXAMPLE OF RECORD KEEPING IN TYPICAL PRACTICE 18
Annex B – LAWFUL BASES FOR PROCESSING PERSONAL DATA 20
Annex C - INDIVIDUAL RIGHTS 22

PART 1: WHAT YOU NEED TO KNOW

1.1 The law at a glance

In the United Kingdom (UK), data protection is governed by the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and the Privacy and Electronic Communications Regulations 2003 (PECR). These pieces of legislation were amended in 2025 by the Data (Use and Access) Act 2025 (DUAA). Data protection law applies to **personal data** held in electronic and paper form – i.e. not just computer records. It therefore applies to all optical businesses/practices.

Data protection law **does not apply to non-personal data** – e.g. it does not cover information you hold that is not about a natural person or anonymised data from which an individual cannot be identified. Pseudonymised data – which could be used to identify an individual if combined with other data – might still fall within the scope of 'personal data' depending on how difficult it is to attribute the pseudonym to a particular individual. Information about a person who is deceased is **not** 'personal data', but access to their information may be restricted by other legislation, such as The Access to Health Records Act (1990).

Although the law does not apply to all data you hold, data protection by design requirements mean that you are likely to benefit by taking steps to protect all your data (see Part 2: What you need to do).

1.2 Key terms

The table below sets out the key terms used in the UK GDPR and DPA 2018 that you need to know**.**

Key terms	What it means
Personal data	Any information relating to an identified or identifiable natural living person ('data subject'). An identifiable person is someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
Special categories of personal data	Special categories of personal data have additional safeguards. This includes personal data concerning health, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, or data concerning a natural person's sex life or sexual orientation.
Data controller	The person(s) or organisation that determines the purposes and means of processing personal data – usually the practice owner or company registered with the Information Commissioner.

Data processor	The person(s) or organisation(s) responsible for processing personal data on behalf of the controller (other than a person who is an employee of the controller) – for example an external provider that manages the controller's payroll.
Data protection law	The UK GDPR and the DPA 2018 – which should be read together – and the PECR. These pieces of legislation were amended in 2025 by the DUAA.
Lawful basis for processing	There must be at least one lawful basis in order to process personal data. The lawful bases are clearly explained in section 2.4 and Annex B.

1.3 Principles of data protection

It is important to remember that the UK GDPR is a principles-based rather than rules-based system and, in the event of a problem, the ICO is likely to look more favourably on organisations that can show they have considered the principles and tried to apply them.

The data controller is responsible for compliance and must be able to demonstrate that personal data is:

a) processed lawfully, fairly and transparently;
b) collected and used for specific and legitimate purposes, and not used in an incompatible way with those purposes;
c) adequate, relevant and limited to what is necessary for the intended purposes;
d) accurate and where necessary kept up to date – e.g. errors can be rectified without undue delay;
e) kept in a way that permits identification of an individual for no longer than is necessary; and
f) kept secure using appropriate technical or organisational measures – e.g. protecting against accidental loss, destruction or damage.

The law aims to strengthen citizens' rights by putting more focus on **demonstrating** data security and clearer accountability.

Both the UK GDPR and the DPA impose high data protection requirements on those who process special categories of personal data. This includes, among other things, data related to health. Some requirements were softened slightly following the introduction of the DUAA.

It should be noted that all GOS providers are classified as public authorities. This means that **all GOS providers must appoint a Data Protection Officer (DPO)**. See section 2.2.

PART 2: WHAT YOU NEED TO DO

In this section we set out the steps you can take to help you comply with data protection law.

Complying with data protection law is an ongoing process, this means you will need to have systems in place to ensure you are always meeting your obligations to protect personal data. This is particularly important when processing health care data as it is a special category of personal data.

Managers of optical practices and businesses and anyone who works in the practice/business should read and follow this guidance to be sure they are meeting their obligations. In addition, as a minimum, anyone working in an optical practice which offers NHS services should be familiar and compliant with the relevant sections of the GOS contract and Quality in Optometry (QiO, England) / Quality for Optometry (QfO, Wales) / Scottish GOS Compliance Toolkit (SGCT, Scotland) as applicable.

2.1 Key roles and responsibilities

The definitions of a **data controller** and **data processor** are as follows:

Data controllers – usually the practice or business owner, or someone appointed by the practice or business owner, who has overall control and responsibility for how personal data is collected, processed and stored in a practice/business. The data controller is responsible for:

- determining how and why personal data is processed;
- compliance and may be liable for any breaches;
- reporting serious breaches to the ICO (see section 2.7); and
- ensuring that data processors – people and organisations who handle data on the data controller's behalf – comply with the law.

Data processors – are all other persons who process personal data on behalf of the controller (other than a person who is an employee of the controller). In an optical practice this could include a practice management software provider or payroll company, for example. Data processors are liable for breaches. It is therefore important for data controllers and processors to have contracts in place which explain how obligations under data protection law will be managed. The ICO guidance to the UK GDPR includes a checklist for contracts. We recommend that controllers who are using external processors refer to the ICO checklist for contracts, which can be found here.

Optical practices are required to appoint a DPO if they provide GOS, or if they don't provide GOS but do process large amounts of special category personal data such as healthcare data.

You should consider the following points carefully before deciding who to appoint as DPO:

- The DPO must have experience and expert knowledge of data protection law
- The DPO should report directly to the highest level of management and have independence to perform their tasks
- The DPO's other tasks or duties should not create a conflict of interest with their role as DPO.

The tasks of a DPO are to:

- inform and advise the data controller and other staff about their obligations regarding the UK GDPR and other data protection laws;

- monitor compliance with data protection laws and policies, raise awareness of issues and provide staff training; and
- be the first point of contact with the ICO and for individuals whose personal data is processed.

The ICO has been clear that the knowledge and expertise that the DPO is required to have should be proportionate to the type of processing carried out and the level of risk.

It may not be appropriate to give the DPO title to a member of staff simply because they have previously led on data protection for the organisation. You may also want to note that the ICO has indicated that it is acceptable for a DPO to be shared by several practices.

The ICO has recognised that small organisations may find it difficult to identify (or may not have) an employee who has both the skills to take on the role, and no potential conflict of interest with their other duties as an employee. The ICO has indicated that it will be pragmatic when dealing with such cases and that if an optical practice appoints a DPO with a potential conflict of interest then the practice should document the reasons for the appointment, what the possible conflicts of interest are and what measures (if any) will be taken to reduce or eliminate such conflicts.

You can find further information on the role of the DPO on the ICO website.

2.2 Getting people involved

Make sure decision makers and key people in your organisation are involved in helping you comply with data protection requirements. This might include:

- Business owners, partners, directors etc
- IT leads
- Practitioners – e.g. registrants
- Information and Clinical Governance leads
- Practice managers
- Human Resources and payroll leads
- Optical assistants, receptionists.

If you are an **employer**, ensure all employees are aware of data protection laws and that they are kept informed about:

- what the practice or company is doing or plans to do to comply with the rules;
- their own responsibilities in respect of practice and company operating procedures; and
- training and continuing professional development opportunities in data protection.

Most optical **employees** are likely to be employed by a data controller, and the data controller will be responsible for ensuring processes are in place to comply with the rules. Individuals should therefore comply with company data protection policies, especially the things that are easy to overlook such as the use of screen savers and secure passwords, etc.

Individuals who process data who are not employees are likely to be classified as data processors. Data about a person which is passed from a data controller to a third-party data processor is only “personal data” for this purpose if the data processor can link the data to an identifiable individual.

For example, an optical practice (the data controller) may send patient information to a supplier of spectacles or contact lenses (the data processor). If the optical practice gives the supplier an ID number for the patient, rather than information that could enable the supplier to identify the patient, then the prescription is not “personal data” and there will be no need for a UK GDPR-compliant contract between the practice and the supplier.

It should, however, be noted that providing a supplier with a patient ID number instead of a name does not automatically mean the data ceases to be personal data. Where the individual could be identified using additional information held by the practice or another party, the data is likely to be pseudonymised personal data rather than anonymous data.

If the practice gives the supplier the patient’s name and address so the supplier can send the order direct to the patient, this is “personal data” so a UK GDPR-compliant contract will be needed.

2.3 Demonstrating compliance and accountability

Optical practices and practitioners handle large amounts of health data as part of their routine activities. The law places increased emphasis on being able to demonstrate compliance and accountability in the handling and storage of personal data.

The ICO has helpfully clarified that:

“You are expected to put into place comprehensive **but proportionate** governance measures.” (our emphasis)

All optical businesses that process personal data for business purposes should register and maintain registration as a data controller with the ICO unless they are exempt from the data protection fee requirements.

You should also maintain a record of processing activities and how you protect this personal data.

Keep a record of all your processing activities. The record should include:

1. name and contact details of the person responsible for protecting personal data/DPO;

2. a list of all the categories of personal data you hold – e.g. patient records, staff records, customer details etc. – and the purposes for which you use that data. The list should include all personal data held in both paper and electronic formats. Remember, you only have to do this for personal data;

3. the lawful basis on which you process personal data – it is important to understand (and be able to explain) the lawful bases you use to process personal data. Record the lawful bases for holding each category of personal data (see section 2.4 and Annex B for more information);

4. where possible, include the time limits for erasure of the different categories of personal data you hold;

5. where possible, include a general description of your technical and security measures – e.g. how you ensure ongoing confidentiality, integrity, availability and resilience of systems and services; how you would restore personal data in a timely manner in the event of a physical or technical incident; whether and how you test, assess and evaluate the effectiveness of technical and organisational security measures.

See Annex A for an example of what such a record might look like.

Some, **but not all,** data controllers will have to perform a **Data Protection Impact Assessment** (DPIA). You must carry out a DPIA if you are processing data that is likely to result in a high risk to individuals or if you intend to undertake any major project which requires the processing of personal data. A DPIA is therefore unlikely to be needed for an optical practice carrying out its normal activities. However, you may want to carry one out, for example, if you were changing your practice management software systems. Again, it is important to note that a DPIA, like all other aspects of data protection, should be proportionate to the type of data being processed and the likely risks.

Under the rules you are required to meet the principles of **data protection by design and data protection by default**. The ICO has stated that it expects organisations to put in place comprehensive but proportionate governance measures. This means that small companies are not expected to invest large sums in state-of-the-art defence systems.

Although the law only applies to personal data and not any other information you hold, protecting all the information you hold is likely to help you comply – e.g. if you use computers to store personal data then ensuring software is up to date and supported, anti-virus software is correctly installed and current, and accounts protected with robust passwords etc. will help safeguard any personal data held on the same network.

2.4 Identifying the lawful basis for processing personal data

Once you have identified all of the personal data you hold (or intend to hold) and the purposes for which you intend to use it, you **must** identify at least one lawful basis for **each** category of personal data and the purposes for which you intend to use it before you begin processing. You should document each lawful basis and include this in your privacy notice. It is important to get this right from the outset because it can affect the rights of the people whose data you are processing and, if you decide to change the legal basis you use at a later date, you will need to be able to justify the change (see 2.6 Understanding and complying with individual rights).

The lawful bases you opt for will depend on the type of personal data you are processing and the reasons for processing. However, there are two key points to note:

- **Health data** is a special category of data, so you need to identify both a lawful basis for general processing of the data, and a condition for processing special category data. As an optical business your condition for special category processing will usually be 'the provision of health or social care'.
- **Consent** should **NOT** be used as the lawful basis for processing health care records or staff records. This is because there are more appropriate and simpler lawful bases for processing these types of data (see below and Annexes A and B). You do not need to ask patients if you can process their data for healthcare reasons. If you are seeking consent for data processing, for instance in order to send electronic marketing material to patients, it is important to note that this consent is separate from the patient consent you need to provide health services to a patient.

Important: Consent to treatment is not the same as consent under UK GDPR. A patient may consent to an eye examination or treatment, while the practice relies on another lawful basis under data protection law to process the patient's personal data. The lawful basis for processing should be assessed separately from any clinical consent obtained.

Below, we outline the key points for patient, customer and employee data. **Annex A** includes examples of the lawful bases you may use, and **Annex B** provides a full list of lawful bases with examples to help you identify and record the appropriate basis for each type of personal data you hold.

It is also important to note that the rights of the data subject will depend on the lawful basis you use for processing personal data, see **Annex C** for more details and the ICO guidance on rights.

Patient data

For the purposes of processing special category (i.e. health) data for privately funded patients, or for primary eye care services provided under contract with the NHS, the condition for processing special category data will be the provision of health care. The lawful basis for data processing is likely to be:

- **for legitimate interests** – e.g. keeping patient record cards, dispensing of spectacles, contacting existing patients about appointments for future sight tests

For patients whose sight test is GOS funded, the condition for processing special category data will again be the provision of health care. The lawful basis for data processing is likely to be:

- **the performance of a task carried out in the public interest** (for processing of the patient health record and GOS claim) and **legitimate interests** (e.g. for processing for the dispense of spectacles, or to send reminders for future appointments).

The legal bases for processing data for a GOS sight test are different because a practice performing GOS work is treated as a public authority for that purpose, and so cannot use "legitimate interests" as a legal basis for processing the patient health record.

Customer and marketing data

The practice may rely on legitimate interests as its UK GDPR lawful basis for processing customer data for marketing purposes, but it must also comply with PECR. In many cases this will mean obtaining an appropriate opt-in for electronic marketing communications or ensuring that the requirements of the soft opt-in exemption are satisfied. Patients must always have a simple means of opting out of further marketing communications.

Whenever using legitimate interests as your legal basis for non-health purposes, such as marketing, you must make it clear to a customer or patient that they can ask you to stop processing their data for this purpose at any time. If they do, you must stop unless you can demonstrate that your legitimate interests in processing the data outweigh theirs. In practice, it would be difficult to justify continuing such processing.

It is possible however that some practices/businesses will rely on **consent** as the lawful basis for specific marketing purposes.

In cases where you use customer consent as the lawful basis for holding/processing personal data, it is important that your consent procedures are compliant with the rules.

In order to comply with the rules consent must be:

1. given by a clear affirmative act – e.g. include ticking a box when visiting an internet website, therefore silence, pre-ticked boxes or inactivity do not constitute consent;
2. freely given, specific, informed and unambiguous – the data subject agreeing by a written statement, including by electronic means, or an oral statement; and
3. easy to withdraw.

If you use consent as your legal basis for marketing the customer has the right to withdraw consent at any time and, if they do so, you must stop processing their data for this purpose.

Employee records and data

Employee records and data are normally held and processed on one of the following legal bases:

- **for the performance of a contract with the data subject** – e.g. employee records, payment of salary;
- to comply with a **legal obligation** - e.g. on tax and pensions; or
- due to **legitimate interests** of the practice/business – e.g. recording and managing holiday dates.

You are also likely to hold some data on your staff that falls into a special category, for example if you maintain sickness records, for which you will need to identify a condition from **Annex B** (table 2), most likely **assessing the working capacity of the employee**.

So you do not need to ask staff to sign consent forms for you to hold their data for HR purposes. But, as with all personal data you process, you should only hold and process it where it is necessary for a specific purpose, and you must respect the data subject's rights (see **Annex C**).

2.5 Managing patient and customer data

Health care records

The law complements rather than replaces existing best practice guidance and standards and contractual requirements on record keeping.

Optical practices should continue to follow:

- GOS contract requirements, including retention periods
- GOC standards
- Sector specific guidance on record keeping, including QiO, England / QfO, Wales / SGCT, Scotland, as applicable.

Patient correspondence

Nothing in data protection law prevents practices from writing to patients about their direct care – e.g. sending appointment reminders, or writing to patients about their sight test, contact lens aftercare/follow-up, other appointments and other services which might meet their needs. Indeed, it would be clinically inappropriate if it did. However, as discussed above, it will be important to understand and record the lawful basis on which personal data is processed.

Referrals

Nothing in data protection law prevents practices or practitioners from passing information about a patient's direct care to other healthcare professionals, provided this is done in a way that protects the patient's data so that it can only be accessed by those who need to see it. However, you should still ask for the patient's permission when writing to their GP or referring

them into secondary care. Similarly, practices and practitioners can use patients' personal data in recognised NHS and social services referral systems.

Customer data for other purposes – e.g. advertising and marketing

It is important to note that data protection rules do not cover all circumstances in which personal data is collected or used. There are also other professional standards and regulations that businesses will need to comply with.

For the purposes of this guidance businesses should ensure customer data is processed in a way that complies with:

- data protection requirements; and
- PECR.

Businesses might find the following ICO resources helpful:

- Direct marketing and privacy and electronic communications
- Direct Marketing – checklist

The law does not prevent practices or businesses alerting potential patients or customers to their services by routine advertising, as this may not involve processing individuals' personal data.

2.6 Understanding and complying with individual rights

Organisations are required to have a process for handling data protection complaints.

Individuals must be given a clear way to raise concerns about how their personal data has been collected, used, shared, retained or protected.

Organisations must:

- acknowledge complaints within 30 days;
- investigate and respond appropriately;
- keep complainants informed where necessary; and
- communicate the outcome without undue delay.

Practices should ensure staff understand how to recognise a data protection complaint and know how to escalate it internally.

The rules strengthen individuals' rights over the processing of their personal data. The main rights under the law, with examples of how they may apply in optical practices, are listed in Annex C. We highlight some of the key rights below in more detail. Right to be informed: privacy notices

These are the notices you use to explain how you process data, and the procedures you use to deal with data queries and problems. Review these notices and, if required, update them so they comply with data protection requirements. Working through the suggestions in this guidance will help provide you with the information you need to write your privacy notices. They should be:

- concise and transparent;
- easy to understand and accessible; and
- free of charge.

What the privacy notice contains will depend on how you obtained the personal data, but briefly it should include:

- data controller details;
- what personal data you process, for what purposes, and where possible how long you retain it;
- the lawful basis (or bases) for processing personal data;
- whether you share it with any other party, and if so why;
- an explanation of how to withdraw consent or opt-out of marketing where relevant. If you are using consent as a lawful basis for processing then make clear the individual can withdraw consent at any time, and similarly if you have used legitimate interests for marketing the individual can also opt-out of marketing; and
- how to complain to your business and to the ICO about data processing issues.

Think about whether your privacy notices will be easier to understand if you have different privacy notices for different groups (such as patients, suppliers and your staff) or for different purposes. For further details on what to include in a privacy notice, see the ICO's guidance on privacy notices and cookies.

Right to access: responding to requests

A Subject Access Request (SAR) allows individuals (including ex-patients and ex-employees) to access personal data that is held about them in any format (subject to some safeguards).

There are three points to be aware of:

- You must respond to a SAR without undue delay and within **one month**
- You cannot charge the person making the SAR, unless a request is manifestly unfounded or excessive, e.g. for multiple further copies of the same information. Even then, you cannot charge more than the administrative cost of providing the information
- Data controllers are only required to make 'reasonable and proportionate' searches, when responding to a SAR.

For example, if you have provided a copy of a prescription following a sight test and a customer subsequently asks for another copy you will be able to charge a fee that is no more than the administrative cost of providing the information. There are circumstances where it may not be appropriate to charge patients for providing a duplicate prescription. For example, if a patient with cognitive impairment loses their original prescription, and needs a copy for an upcoming hospital appointment, data controllers should consider providing this free of charge, by way of 'reasonable adjustment'.

Right to erasure: right to be forgotten

A person can ask you to delete or remove personal data you hold on them. However, this right does not apply if there is a valid legal reason for its continued processing – for example if the data takes the form of health records that you have a legal duty to retain. You should not delete patient records before the usual time limit. You should, however, remove the patient from all mailing lists if requested (see Annex A for further information on record keeping).

National data opt-out (NDOO) – England

The NDOO service enables NHS patients in England to view, or change, their NDOO choice at any time and to decide whether their confidential information can be used for purposes other than for patient care, such as for research and planning.

This can be done:

- through the NHS App by clicking on "Your Health" and selecting "Choose if data from your health records is shared for research and planning";
- online via the NHS data matters page; or
- by phone, email or post via the manage your choice page.

NHS England also supports organisations to understand how they can comply with the NDOO.

The NDOO will only affect an optical practice in England if you are planning on using confidential patient information or data for anything other than patient care such as your own research or planning purposes, in which case you should contact NHS England to establish whether the opt-out applies to any of the confidential patient information you plan to use. The opt-out does not apply, however, if you have sought explicit consent for the activity. There are currently no equivalent schemes in Scotland, Wales or Northern Ireland.

Following the introduction of DUAA, data subjects can give 'broad consent' to an area of scientific research, and in certain situations, organisations can re-use people's personal information for scientific research, without giving them a privacy notice.

2.7 Data breaches – prevention and reporting requirements

Preventing a data breach

The ICO has helpfully clarified that "You are expected to put into place comprehensive **but proportionate** governance measures" (our emphasis). This means small companies will not be expected to invest large sums in state-of-the-art defence systems.

Ensuring software and anti-virus software is up to date, computers are protected with strong passwords etc. should be sufficient in most cases.

The law does allow potential sanctions for serious data breaches – up to £17.5 million, or 4% of total worldwide annual turnover, whichever is higher. However, as noted previously, the ICO has also been clear that it will focus on supporting compliance rather than on imposing fines, this includes providing a Helpline service for small businesses.

As with most systems, it is important that all employees understand company policies on data protection and that they are appropriately trained. Demonstrating that reasonable steps have been taken to protect data in these ways will reduce the risk of reputational damage and financial sanctions that may result from any potential data breach.

Practices should ensure that reasonable procedures are in place to protect data and ensure appropriate action is taken if a breach occurs. As a minimum, practices should check that they are compliant with the relevant sections of the GOS contract and QiO, England / QfO, Wales / SGCT, Scotland, as applicable.

Action in the event of a data breach

A personal data breach is any breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. You do not have to report all breaches, but you should learn from every event – e.g. near misses – in order to reduce future risks.

You have to report a data breach to the ICO where it is likely to result in a risk to the rights and freedoms of individuals, which if left unaddressed could cause a 'significant detrimental effect'. This includes breaches resulting in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

In practice, this includes any inappropriate or unauthorised release or disclosure of patient or staff data.

Data controllers will need to look at the facts and circumstances of each breach to decide what to do including, but not limited to, determining if each data breach needs its own assessment and investigation.

Example 1

An optical practice mistakenly sends a referral letter to the wrong GP practice, who notifies the optical practice about the error. This is unlikely to be notifiable to the ICO or the patient, because the data breach has been contained, and is unlikely to result in a risk to the patient's rights and freedoms. However, the optical practice should look at its procedures and protocols to find out why this happened, take steps to avoid this happening in the future, then document these steps and the justification for not reporting the breach.

Example 2

An optical practice mistakenly sends a referral letter to the wrong patient, who notifies the optical practice about the error and agrees to return or destroy the letter immediately. This is unlikely to be notifiable to the ICO or the patient, because the data breach has been contained, and is unlikely to result in a risk to the patient's rights and freedoms. However, the optical practice should look at its procedures and protocols to find out why this happened, take steps to avoid this happening in the future, then document these steps and the justification for not reporting the breach.

Example 3

An optical practice mistakenly sends a referral letter to the wrong patient, who posts the letter on social media. This is likely to be notifiable to the ICO and the patient, because the data breach has not been contained, and is likely to result in a risk to the patient's rights and freedoms. The optical practice should notify the ICO and the patient (and possibly the NHS), and look at its procedures and protocols to find out why this happened, take steps to avoid this happening in the future, then document the steps taken. **In the event of a serious breach the ICO must be notified within 72 hours without undue delay.**

A breach report should include the following information:

- The nature of the breach;
- The numbers of individuals affected;
- The actions being undertaken to rectify the breach; and
- The data controller's or reporter's name and contact details.

Details of when and how to notify the ICO of a breach can be found here.

Informing individuals affected

Individuals affected must also be notified if the breach is likely to result in a 'high risk' to their rights and freedoms. More details can be found on the ICO website.

2.8 Further information

If you require further advice/guidance please contact your professional representative organisation

You may also find the following helpful:

- ICO Helpline
- ICO Blogs for organisations
- NHS England – Information Governance
- NHS Wales – Information Governance / Llywodraethu Gwybodaeth
- NHS Scotland – Information Governance
- Health & Social Care Northern Ireland – Information Governance

Annex A – EXAMPLE OF DATA PROTECTION RECORD KEEPING IN A 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,	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

referral letters, etc.				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 direct marketing.
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 records 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.

7. Processing is necessary as a recognised legitimate interest, where the data controller needs to use personal information for: • Crime prevention • Public security • National security or defence • Safeguarding • Emergencies • Sharing personal information to help other organisations perform their public tasks or official functions	Might be used by a practice to share personal data with a local authority (e.g. to safeguarding a child) or with the police (e.g. following a road traffic accident). Data controllers don't need to assess whether a person's rights, freedoms or interests outweigh the recognised legitimate interest, but they still need to consider whether processing information in this way is 'necessary'.

A guide to lawful basis | ICO

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 DPA 2018	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 Domestic Law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental right and the interests of the data subject	Unlikely that practices will rely on this condition.
H. Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Domestic Law or pursuant to 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 have under the 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 'privacy 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 a further 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.

Data Protection Complaints Procedure:

Step 1 – Receipt
Record the complaint.
Confirm whether it relates to the processing of personal data.

Step 2 – Acknowledgement
Acknowledge receipt within 30 days.

Step 3 – Investigation
Review relevant records and processes.
Make appropriate enquiries.
Maintain a record of the investigation and findings.

Step 4 – Outcome
Explain the findings and any remedial action taken.
Inform the individual of their right to escalate concerns to the ICO if they remain dissatisfied.

Step 5 – Learning
Record trends and use complaints to improve data protection practices.