Changes to Data Protection Law
Information and Guidance

Published: July 2018

ABOUT THIS GUIDANCE

The General Data Protection Regulation (GDPR) and the new Data Protection Act 2018 (DPA2018) both came into effect on 25 May 2018. The changes they introduced affect everyone in the optical sector.

This guidance aims to help the sector – including optical practices, manufacturers/suppliers/distributors, and employees – understand the new data protection rules and what you need to do. It updates and replaces the guidance the Optical Confederation issued in December.

The guidance is in two parts:

- Part One – What you need to know - provides a basic overview of the new data protection rules and what has changed.
- Part Two – What you need to do - explains what steps you need to take.

Some of the important detail of the new rules is still not confirmed - the Information Commissioner's Office (ICO) and the NHS are still developing and publishing guidance.

The Optical Confederation will continue to work with the ICO, the NHS and other primary care contractor professions to ensure an approach that does not place disproportionate burdens on front line practices, manufacturers, distributors and suppliers whilst fully protecting the personal data of patients, customers and staff.

We will update this guidance as necessary in response to new guidance from the ICO and the NHS. Updates and revised guidance will be posted on the Optical Confederation and related websites as well as being shared via your representative body, whose contact details are as follows:

ABDO – dmcgill@abdolondon.org.uk
ACLM – secgen@aclm.org.uk
AOP – regulation@aop.org.uk
FMO – info@fmo.co.uk or 020 7298 5123
FODO – optics@fodo.com or 020 7298 5151

TABLE OF CONTENTS **Page**

PART 1: WHAT YOU NEED TO KNOW

1.1 The law at a glance

The General Data Protection Regulation (GDPR) came into force on 25 May 2018 across all EU member states.

The GDPR allows Member States to make some variation in how GDPR is applied within their jurisdiction. The UK has done this using the Data Protection Act 2018 (DPA2018). The GDPR and DPA2018 therefore have to be read side by side.

The changes to data protection law will not be affected by the UK's decision to leave the EU.

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[1]. Pseudonymised data – which could be used to identify an individual if combined with other data – might still fall within the scope of this law depending on how difficult it is to attribute the pseudonym to a particular individual[2].

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 GDPR and DPA2018 that you will need to know**.**

Key terms	What it means
Personal data	Any information relating to an identified or identifiable natural 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 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, **data concerning health** or data concerning a natural person's sex life or sexual orientation.

[1] Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016
[2] ICO, 21 Nov. 2017, Guide to the General Data Protection Regulations (GDPR)

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	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Data Protection Act 2018. Both need to be read together.
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

The principles in the new law are similar to previous UK law. It is important to remember that the 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 will be responsible for ensuring, and will need 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
f) kept secure using appropriate technical or organizational measures –e.g. protecting against accidental loss, destruction or damage.

1.4 What has changed?

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

Both the GDPR and DPA2018 impose higher data protection requirements on those who process special categories of personal data. This includes, among other things, data related to health.

Previous data protection law and existing professional standards already require you to protect personal data. The good news is that many data protection concepts and principles have not changed, therefore your previous polices will help you comply with the new data protection law.

Importantly, you do not need to change the way you contact existing patients about their direct care.

The most significant change for optical practices is that all GOS providers are classified as public authorities. This means that **all GOS providers must appoint a Data Protection Officer**. 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 the new rules.

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 should be familiar and compliant with the GOS contract sections A10.1, 10.2, 10.4 and 10.5 of Quality in Optometry.

If you already have good data protection measures in place, the new law largely involves reviewing, updating and documenting existing procedures and policies to ensure they are compliant with new requirements, rather than starting from scratch. This should include ensuring all relevant employees are trained in the new requirements and procedures. You will also need to take some additional steps, such as appointing a DPO and determining the lawful bases you use to process personal data.

2.1 Key roles and responsibilities

The definitions of a **data controller** and **data processor** are essentially the same as under the previous law.

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;
- responsible (and liable) for personal data and any breaches;
- responsible for reporting serious breaches to the ICO - with new reporting requirements (see section 2.7); and
- responsible for 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. It is also likely to include locums.

The most significant change is that for the first time data processors will also become liable for breaches. It is therefore important for data controllers and processors to have contracts in place which

explain how obligations under the new data protection law will be managed. This means you may need to review and update your contracts.

In the case of **locums** it is not yet clear what, if any, impact this will have on those individual health care professionals, but it is possible that as a processor they will be liable for data breaches.

The ICO guidance to the GDPR includes a checklist for contracts. We recommend controllers who use external processors use the ICO checklist for contracts, which can be found here.

Optical practices are required to appoint a **Data Protection Officer** (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
- they should report directly to the highest level of management and have independence to perform their tasks
- their 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 with regard to the GDPR and other data protection laws
- To monitor compliance with data protection laws and policies, raise awareness of issues and provide staff training
- To 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 and, specifically for NHS healthcare providers, on the Information Governance Alliance website.

This section will be reviewed updated if there are significant changes.

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.
- Practitioners – e.g. all registrants
- Practice managers
- Optical assistants, receptionists
- IT leads
- Information and Clinical Governance leads
- Human Resource and payroll leads

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

- what the practice/company is doing or planning to do to comply with new rules
- their own responsibilities in respect of practice and company operating procedures; and
- training and continuing professional development (CET) opportunities in data protection and GDPR.

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 new rules. Therefore, as now, individuals should comply with company data protection policies especially the things that are easy to forget such as the use of screen savers and secure passwords, etc.

People processing 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 GDPR-compliant contract between the practice and the supplier. However, 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 GDPR-compliant contract will be needed.

In the case of **locums** it is not yet clear what, if any, impact this will have on those individual health care professionals, but it is possible that as a processor they will be liable for data breaches. At this stage locums should ensure they are familiar with the existing data protection policies where they work. We will publish further guidance in due course, if necessary.

2.3 Demonstrating compliance and accountability

The fundamental basis for keeping health records has not changed which means that, on a daily basis, optical practices and optical practitioners will continue as now when processing most data. However, the new law increases the emphasis on organisations being able to **demonstrate** compliance and accountability in the handling and storage of **personal data.**

This means optical practices and optical practitioners must be able to demonstrate compliance and accountability.

The ICO has helpfully clarified that:

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

All optical businesses[3] should register and maintain registration as a data controller with the ICO.

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 basis you use to process personal data. Record the lawful basis 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 now 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.

[3] Practices that do no electronic processing at all (including no use of computers or other electronic equipment to keep records or produce letters to patients) need not register as a data controller, but do still need to appoint a DPO if providing GOS

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 new rules you are encouraged 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 will not be expected to invest large sums in state-of-the-art defence systems.

Although the new 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 with the new law – 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 data~~ 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 marketing material to patients, i~~I~~t is important to note that this consent is separate from the patient consent you need to provide health services to a patient.

We have provided key points in relation to patient, customer and employee data below. We have also included examples in **Annex A** to demonstrate what lawful bases you may use. And we have provided a full list of lawful bases, with examples, in **Annex B** t**o** help you work through for all the personal data you hold the appropriate lawful basis for processing it. Your representative body may be able to provide further advice and resources.

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 the NHS Standard Contract, 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, dispense 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

When sending direct marketing to existing customers your lawful basis is likely to be "**for legitimate interests"**.

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. You will not usually be able to show this.

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 new rules.

In order to comply with the new 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
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.

Your OC representative body will be able to advise in particular cases.

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.
- in order to comply with a **legal obligation** - e.g. on tax and pensions
- 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 table 2 in Annex B, most likely **assessing the working capacity of the employee**.

So you don't 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 if you need to do so 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 new 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

Patient correspondence

Nothing in the new 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 the new 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 the new 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

- new data protection requirements
- the Privacy and Electronic Communications Regulations (PECR)[4].

Businesses might find the following ICO resources helpful

- Direct Marketing, PECR – long form
- Direct Marketing – checklist

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

2.6 Understanding and complying with individual rights

The new rules strengthen individuals' rights over the processing of their personal data. A full list of these rights, with examples of what they might mean for optical practices, is included at **Annex C**. We set out below in greater detail a few of the key rights that optical practices should be aware of.

[4] PECR also originates from an EU Directive and is in the process of being updated. We will update guidance once the new regulations are published, subject to how EU regulations are implemented in the UK after March 2019

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 the new rules. Your representative body may be able to provide further advice.

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 access, 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, why, and where possible how long you keep 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 pages 93-101 ICO, 04 Jun 2018, Guide to the General Data Protection Regulations

Right to access: responding to requests

As under previous data protection rules, 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, however, two changes from previous law:

- you must respond to an SAR within **one month** (not 40 days as under the previous Data Protection Act)
- you will no longer be able to 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.

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.

You should review your SAR procedures and plan how to manage SARs under the new rules.

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 compelling 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. However you should remove the patient from all mailing lists if requested. (See Annex A for further information on record keeping.)

National data opt out

On 25 May 2018 NHS England introduced a new, national data opt out. This enables patients to opt out of their confidential patient information being used for purposes other than their direct health care – such as for research or health planning purposes.

The National Data Opt Out is managed by the NHS – patients make their choice online at nhs.uk/your-nhs-data-matters, or they can call 0300 303 6578.

The national data opt out will only affect an optical practice if you are planning on using confidential patient information for your own research or planning purposes, in which case you should contact the NHS 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.

2.7 Data breaches – prevention and reporting requirements

Preventing a data breach

The ICO has helpfully clarified that that "You are expected to put into place comprehensive **but proportionate** governance measures"[5] (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 new law does increase potential sanctions for serious data breaches - up to €20 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.

[5] ICO, 2017, Overview of the General Data Protection Regulation (GDPR) page 30, https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-12.pdf, accessed 15 September 2017

As with most systems, the main risk is that due to human error; it is therefore 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.

Double-check now that reasonable procedures are in place to protect data and ensure appropriate action is taken if a breach occurs. For optical practices, as a minimum check that you are compliant with GOS contract sections A10.1, 10.2, 10.4 and 10.5 of Quality in Optometry.

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 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 short, as now, the definition will apply to 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.

Your Optical Confederation representative body will be able to advise in individual cases.

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:

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

Details of how to notify the ICO of a breach can be found here: https://ico.org.uk/for-organisations/report-a-breach/

Informing individuals affected

Individuals affected must also be notified if the breach is likely to result in a 'high risk' to their individual freedoms. More details can be found on the ICO website or your Optical Confederation representative body will be able to offer advice on a case by case basis.

2.8 Further information

Updates to this guidance, as well as any additional guidance, will be posted on the Optical Confederation website as well as being shared via your representative body.

If you require further advice/guidance please contact your representative body.

You may also find the following helpful:

- ICO helpline
- ICO Health Sector webinar on the GDPR
- ICO Myth Busting Blog
- NHS – Information Governance Alliance guidance

Optical Confederation
July 2018

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 direct marketing. 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-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.