Preparing for Changes to Data Protection Law
Initial Guidance
Published: 15 December 2017

SUMMARY

Data protection law in the UK will change on 25 May 2018. This will affect everyone in the optical sector.

This guidance aims to help the sector – including optical practices, manufacturers/suppliers/distributors, and employees – understand what is changing and what you need to do.

Some of the important detail of the new rules is not clear yet. A Bill is still going through the UK Parliament and the Information Commissioner's Office (ICO) has not finalised its own guidance. We will publish updated detailed guidance when the rules are confirmed.

In the meantime, the new rules, like the current ones, cover "personal data" – any information relating to a specific person who could be identified from that information. This might include customer details, health records and employee records. The good news is that the new rules build on the existing law, and **most of what you already do to protect personal data will stay the same**.

The main change is that anybody who controls or processes data will need to demonstrate that they comply with the law.

Our full guidance is in two parts:

- Part One provides a basic overview of new data protection rules and what is changing.
- Part Two explains what steps you should take now to manage risks and be ready for the change.

The key points are summarised below.

What you need to do now

If you own or manage an optical business (including manufacturing, distribution or supply of optical products or services), read our full guidance and make sure people responsible for managing, administering or analysing personal data – including the directors of your business, your optical practitioners, your IT and HR staff – are familiar with it.

This guidance will help address each of the points below and more

- **make a list of all the personal data your business/practice holds either on paper or electronically**
- **work out and make a note of the legal "basis" for processing the different types of data you hold** – e.g. optical practices will use "*for health or social care purposes*" as the legal basis for processing patient records but a different legal basis for processing staff records (see part 2 of the full guidance for more detail)
- **review your privacy notices and update them if necessary**
- **review the methods you use to keep data secure and update them if necessary**
- **if applicable, review your consent processes and update them if necessary**
- **ensure that you only collect the data you need and that this is retained securely for only as long as necessary for any checks, remakes etc.**

If you are an employee or locum practitioner**,** find out the data protection policies of the businesses you work for.

What you do not need to do (yet)

Optical practices -you do not need to change the way you contact existing patients about their direct care – for instance, you can continue to send them reminders about their next appointment.

If your practice delivers locally commissioned services under the NHS Standard Contract in England (i.e. not GOS), you will need to complete the new **Data Security and Protection Toolkit** from April 2018. The Optical Confederation and the Local Optical Committees Support Unit (LOCSU) will issue separate guidance on this, so **you do not need to do anything about it yet**.

Finally, you may be approached by consultants offering advice on complying with the new rules, and claiming you're exposed to big risks and costs if you don't use them. Because many of the key rules that will affect optical practices are still unclear, **we recommend you do not spend a lot of money on external advice yet** unless you have checked with your Optical Confederation representative body first.

All businesses - You may have heard that all businesses will need to appoint a "Data Protection Officer" (DPO) to comply with the new rules; this is not true. Some businesses may need a DPO, but this will depend on the Bill that's going through Parliament. We're monitoring this and will provide more guidance as soon as we can. In the meantime, **we recommend that you don't hire a DPO, nor give the DPO title to one of your staff**. That is because DPOs have specific legal responsibilities and it could create an additional regulatory burden, resulting in unnecessary work for your business, if you appoint a DPO when you do not need to.

Keeping up to date

The OC is working closely with the other contractor professions - GPs, dentists, pharmacists and community hearing providers - to ensure clarity across the professions and to resist disproportionate burdens on front line practices, manufacturers, distributors and suppliers whilst fully protecting the personal data of patients, customers and staff in line with the new requirements.

The Optical Confederation and its partners may provide training for practices, businesses and practitioners once the final rules are confirmed.

Updates and revised guidance will be posted on the Optical Confederation and related websites as well as being shared via your representative body.

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

TABLE OF CONTENTS

PART 1: WHAT YOU NEED TO KNOW

1.1 Principles of data protection

The principles in the new law are similar to existing UK law[1] - i.e. as now, any processing of personal information must be:

a) Lawful, fair and transparent
b) Collected and used for a specific purpose
c) Adequate, relevant and limited for the intended purpose
d) Kept accurate and can be erased/rectified without undue delay
e) Kept in a way that permits identification of an individual for no longer than is necessary.

This law only applies to personal data:

> **Personal data** is any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one 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.

This law **does not apply to other types of data** – e.g. anonymised data from which an individual can't be identified, or other information you hold that is not about a natural person.

This law applies to personal data held in both electronic and paper form.

1.2 What is changing?

The UK Data Protection Act (1988) will be replaced by the EU General Data Protection Regulation (GDPR) and associated new UK legislation on **25 May 2018**. This change aims to strengthen citizens' rights by putting more focus on **demonstrating** data security and clearer accountability. The Government has confirmed that the UK's decision to leave the EU will not affect this change.

> The new law largely involves reviewing, updating and documenting existing procedures 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.

[1] Providers with international operations might find that the difference between the new law and existing law is more significant in other EU Member States. This is because the new law, the GDPR, is based on significant input from the UK data protection authority and raises the bar in regions where the original Data Protection Direct was implemented differently to the UK

Community optical practices must already have procedures in place to comply with existing data protection regulations, information governance, patient consent and staff data. These are set out in the GOS contract sections A10.1, 10.2, 10.4 and 10.5 of Quality in Optometry with which all practices should be compliant and all practitioners familiar.

Quality in Optometry will be updated to reflect the new requirements in due course.

Local Representative Committees (LRCs) – that is LOCs, ROCs, AOCs (and Primary Eyecare Companies in England) will also have procedures in place to comply with existing data protection regulations and information governance in respect of members, levy payers and employed or contacted staff.

LOCSU will be considering with Optometry Scotland, Optometry Wales and Optometry Northern Ireland whether specific new guidance specifically for LRCs is required.

Manufacturers, distributors and suppliers - prescription houses, contact lens suppliers and manufacturers, distributors and suppliers of equipment - that captures or processes patient identifiable data already have systems in place to minimise use of, protect and in due course destroy such data.

1.3 Why has the Optical Confederation not issued definitive guidance?

The GDPR is finalised and will apply across all EU member states but

- although the aims and principles of the new rules are clear, much of the detail in the changes that the GDPR will require still has to be worked through
- the EU has set up a working party of regulators (including the UK's ICO) to clarify key points and issue guidance when appropriate – this is ongoing
- the GDPR allows Member States some flexibility to define specific legal terms – health care is one such area and certain requirements may therefore change
- the UK Data Protection Bill, which will supplement and sit alongside the GDPR, is still passing through Parliament and may yet be amended
- the ICO has not yet finalised its own guidance for the UK.

1.4 Why not wait for the definitive version of the OC guidance?

While it may take some time before the final details of the law are confirmed, the broad principles of the GDPR are already known and a reasonable level of guidance exists so that you can start to make progress by checking, updating and documenting existing processes and refreshing staff training.

Preparing for implementation now will help to avoid problems and avoidable costs in the run-up to 25 May 2018.

1.5 Common myths about GDPR

So many myths are circulating about the GDPR and other changes to data protection law, that the ICO has felt it necessary to publish a series of 'myth busting' blogs.

Some of the most common myths in our sector are busted below.

We have heard that under GDPR sending patient correspondence will be more difficult,

There is absolutely nothing in the new law that stops optical practices from contacting patients about their direct care. For example, the ICO has confirmed that it is a myth that ''*GDPR will stop [you] ringing patients to remind them about appointments*".

As part of delivering quality care and best practice you can still send reminders to your patients or any other correspondence about their direct care. As under the GOC and GMC standards, the patient must be your first and overriding priority.

We have heard that under the new law we will have to change all our data protection policies from scratch

Whilst the GDPR does strengthen citizens' rights in relation to their personal data by putting more focus on accountability and security, the ICO has made clear its view that the 'GDPR is an evolution in data protection, not a burdensome revolution'. The new law should therefore be seen as an opportunity to update your data management and governance processes, not to start again from scratch.

We have heard we will be bankrupted by fines for any breach of the new rules

The GDPR does increase sanctions for serious breaches, including in the worst cases a fine of up to €20 million, or 4% of total worldwide annual turnover, whichever is higher. However, the ICO has said it is a myth that "*[professionals] will face massive fines that will put them out of business"* and reassured UK businesses "*it's scaremongering to suggest that [it will] be making early examples of organisations for minor infringements or that maximum fines will become the norm. The ICO's commitment to guiding, advising and educating organisations about how to comply with the law will not change under the GDPR. [The ICO has] always preferred the carrot to the stick […]* ***Issuing fines has always been and will continue to be, a last resort.*****"**

We need to appoint a Data Protection Officer (or buy-in such a service) as soon as possible

You may have been told/read that all businesses need to appoint a "Data Protection Officer" (DPO) to comply with the new rules; this is not true. Some optical practices may need a DPO, but this will depend on the Bill which is currently going through Parliament and has not been finalised. The OC is monitoring this and will provide more guidance as soon as we can.

In the meantime, **we recommend that you do not hire a DPO, or give the DPO title to one of your staff**. That is because DPOs have specific legal responsibilities and it could create an additional regulatory burden, resulting cause unnecessary work for your business, if you appoint a DPO when you do not need to.

We need to buy in expensive external advice to ensure we are compliant and to avoid being heavily fined on 25 May 2018

This is not true, although you may well have been approached by sales agents offering to sell various services to help you manage changes to data protection law, often scaremongering about the risks and costs you may face. We strongly encourage you to contact your representative body before investing significant resources in any non-accredited provider**.**

PART 2: GETTING STARTED

In this section we cover what you need to do next. The goal is to help you make progress towards complying with the new rules that come into effect on **25 May 2018**.

2.1 Key requirements

Get the right people involved and make a record of the data you hold. This is because you will need to demonstrate compliance and accountability.

2.1.1. Getting the right people on board

Ensure that this guidance is read by decision makers and key people in your organisation including

- business owners/partners/company directors/managing directors
- Human Resource and payroll leads
- IT leads
- Practice managers
- Practitioners – including superintendent optometrists/opticians, heads of professional services and all GOC and GMC registrants
- Information and Clinical Governance leads
- Other staff responsible for operational tasks that involve processing personal data.

If you are an employer, it is important to ensure all employees are aware that data protection laws are changing and that they are kept up to date 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
- training and CET opportunities in data protection and GDPR.

2.1.2 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 **demonstrating** compliance and accountability in the handling and storage of **personal data**[2] **.** While some industries may be exempt from some of these requirements, health care providers are unlikely to be exempt.

This means optical practices and optical practitioners should 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"[3] (our emphasis).

At this stage optical practices should

Make a record of all processing activities. The record should include:

1. name and contact details

2. a list of all the categories of personal data you hold - e.g. patient records, staff records, customer details etc. 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 legal basis on which you process personal data – changes in the law mean that it will be important to understand (and be able to explain) the legal basis you use to process personal data. Record the legal basis for holding each category of personal data – see Annex B for a full list of the legal bases available[4]

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

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.

[2] "Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one 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.

[3] 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

[4] Please note the UK Data Protection Bill might introduce additional bases.

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.

2.1.3 Basis for Lawful Data Processing

It is important that you identify the lawful basis for any personal data you process, document this and update your privacy notice to explain it[5].

The GDPR specifies lawful bases but the UK Data Protection Bill might add or modify certain categories. We will update this guidance as soon as there is greater clarity on this issue.

The complexity of data protection rules, and pending UK legislation, can make establishing the lawful basis difficult. We have therefore provided a full list of lawful bases with examples in **Annex B.** In the optical sector however, we expect the basis for processing personal data will usually be:

- **for the provision of health care**[6] – e.g. keeping patient record cards
- **for legitimate interests**[7] – direct marketing to existing customers[8] **for the performance of a contract with the data subject**[9] – e.g. employee records.

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

Using consent as a legal basis

Optical practices and businesses should **NOT** use consent as the lawful basis for processing health care records or staff records[10]. This is because the conditions for consent are unlikely to be met. And, in these cases there are more appropriate specific lawful bases to process data (see Annex A and B). In most other cases we expect practices/businesses should be able to rely on "legitimate interest" as the lawful basis for processing data.

---

[5] ICO, 21 Nov. 2017, Guide to the General Data Protection Regulations (GDPR)
[6] Article 9(2)(g) the GDPR
[7] Article 6(1)(f) the GDPR
[8] Slaughter and May, 2016, Processing of personal data: consent and legitimate interests under the GDPR, https://www.slaughterandmay.com/media/2535723/processing-of-personal-data-consent-and-legitimate-interests-under-the-gdpr.pdf accessed 24 November 2017
[9] Article 6(1)(b) the GDPR
[10] This is based on draft guidance from the ICO, 2017, Draft Consent Guidance. If the ICO updates its guidance the OC will issue an update to this section. Please also note that GDPR states, "Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation […] Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment", it is the OC view therefore – like the ICO – that optical businesses should not use consent as the lawful basis for processing health and employee records.

It is possible however that some practices/businesses will rely on consent as the lawful basis for specific purposes - e.g. marketing to new customers.

In cases where you use customer consent as the lawful basis for holding/processing personal data, it is important to note that there are significant changes to the existing rules on consent.

If you rely on consent as a lawful basis, it is important you check your procedures are compliant with the new rules, and if not that you update these.

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.

Once the ICO publishes its final guidance on the requirements around using consent as a lawful basis, the OC will issue further guidance. In the meantime, your OC representative body will be able to advise in particular cases.

2.2 Roles and responsibilities

2.2.1 Data Controllers and Processors

The definitions of a **data controller** and **data processor** are likely to remain the same as under the existing 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
- 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).

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.

The ICO published a checklist for contracts on 21 November 2017. At this stage we recommend controllers who use external processors use the ICO checklist for contracts, see pages 34 to 38 ICO, 21 Nov 2017, Guide to the General Data Protection Regulations Version 1.

Employed Staff

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.

For now, 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. 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.

Non-Employed Staff – e.g. locums

People processing data who are not employees are likely to be classified as processors and therefore become liable for data breaches from 25 May 2018. It is not yet clear what, if any, impact this will have on individual health care professionals who are not employed (e.g. locums). At this stage locums should ensure they are familiar with the existing data protection policies where they work. The OC is currently reviewing the potential impact on self-employed professionals in the context of UK specific law and will issue further advice in due course.

2.2.2 Data Protection Officers and Data Protection Impact Assessments

Some, **but not all,** data controllers will have to

- appoint a Data Protection Officer (DPO) and/or
- perform a Data Protection Impact Assessment (DPIA)

It is not yet clear which, if any, optical businesses will have to appoint a DPO or carry out a DPIA. At this stage, based on the definitions in EU law and the fact the UK legal definitions are still under discussion, our view is that optical businesses, practices and practitioners should not have to appoint a DPO or carry out a DPIA unless they carry out large scale processing of special categories of data (see Annex A)

You should consider the following points carefully before appointing a DPO or giving the title of DPO to a member of staff:

- the definition and scope of a DPO is very different under the new law. The DPO must have specialist knowledge of data protection law and work under conditions and terms specified in the new law

- therefore, optical practices are advised **not** to give the DPO title to a member of staff simply because they lead on data protection for the organisation
- if an existing staff member has the title of DPO, but your organisation is not required to have a DPO under the new law, then consider changing their title – e.g. to a Data Protection Lead or Data Protection Manager.

This section will be updated if there are significant changes.

2.3 Managing patient and customer data Health care records

The new law is likely to classify health records as a special category of data "for health care or social care purposes" [11] (See Annex B). These do not require patient consent for collecting, processing and storing.

The new law complements, rather than replaces, existing best practice guidance and standards on record keeping. You should continue to follow the GOC Standards and Sections X-Y of *Quality in Optometry.*

The main change under the new law for health care records (including fields plots, retinal photographs, OCT records, referral letters etc.) is understanding and recording the lawful basis for processing this data.

Practices and practitioners should therefore understand and record that it is on the basis of "for health care or social care purposes" (and not on the basis of patient consent) that these personal data are required, processed and protected (until no longer needed and securely destroyed) (see Annex A for an example).

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

[11] 2017, ICO, Consultation, GDPR consent guidance, page 15

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)[12].

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.

2.4 Employee Records and Data

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

- for performance of the employment contract
- in order to comply with legal obligations e.g. on tax and pensions
- to protect the vital interests of the employee or of another natural person (including the employee's dependents or family)
- due to legitimate interests of the practice/business.

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 personal data if you need to do so for a specific purpose and you must respect the data subject's rights (see Annex C).

2.5 Responding to requests

As now, 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 will however be two changes from existing law from 25 May 2018

[12] 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

- you must respond to an SAR within **one month** (not 40 days as under the current Data Protection Act)
- you will no longer be able to charge the person making the SAR to cover the costs of this, unless a request is manifestly unfounded or excessive, e.g. for multiple further copies of the same information.[13] Even then, you cannot charge more than the administrative cost of providing the information.[14]

For example, when you have provided a copy of a prescription following a sight test and a customer subsequently asks for another copy then, as the law currently stands, you will be able to charge a fee that is no more than the administrative cost of providing the information.

At this stage you should review your SAR procedures and plan how to manage SAR under the new rules from 25 May 2018

2.6 Privacy notice

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 these so they comply with new rules. Your privacy notices 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 person data, but briefly it should include:

- data controller details
- what personal data you process, and how long you keep it and why
- the purpose of processing this data, and the lawful basis for this
- whether you share it with any other party, and if so why
- an explanation of how to withdraw consent - if you have used consent as lawful basis for processing; and
- how to lodge a complaint with the ICO.

For further details on what to include in a privacy statement, see pages 17-18, ICO, 21 Nov 2017, Guide to the General Data Protection Regulations Version 1.

[13] 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
[14] 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

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"[15] (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 in part one, the ICO has also been clear that it will focus on supporting compliance than imposing fines, this includes providing a helpline service for small businesses.

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 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.

[15] 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

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.

From 25 May 2018 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 What next?

Keep up to date with changes to this guidance and related sector news – especially between now and June 2018.

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.

You may also find the following helpful:

- ICO helpline
- ICO Health Sector webinar on the GDPR
- ICO Myth Busting Blog

Optical Confederation
15 December 2017

Annex A - EXAMPLE OF RECORD KEEPING IN TYPICAL PRACTICE

Name of Controller:
Address of Controller:
Telephone/Email:
Responsible person:

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
Patient records – including retinal photographs, referral letters etc.	Legitimate interest and for the purposes of health care	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. College of Optometrists guidance is that it is best practice for records to be kept for 10 years.	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	Performance of a contract with the data subject or to take steps to enter into a contract and processing is necessary for carrying out obligations as an employer	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 processing personal data. This means having a legal basis for each processing activity.

Legal 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.
4.Processing is necessary to protect the vital interests of a data subject or another person	Less likely that practices will rely on this condition.
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	Less likely that practices will rely on this condition.
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 most personal data held by practices (please note that health records cannot be processed solely on this lawful basis as they are also a special category of data – see below)
There are additional requirements for anybody processing the following special categories of data: 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 shall be prohibited, unless this is done as part of any of the following provisions:	
7. Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law	Less likely that practices will rely on this condition.
8. 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.

9. 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	Less likely that practices will rely on this condition.
10. 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	Less likely that practices will rely on this condition.
11. Processing relates to personal data manifestly made public by the data subject	Less likely that practices will rely on this condition.
12. 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. the final Data Protection Act in the UK might clarify sharing of patient records with regulators.
13. 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	Less likely that practices will rely on this condition.
14. 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.
15. 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	Less likely that practices will rely on this condition.
16. 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)	Less likely that practices will rely on this condition.

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/

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 details on what you might include in a privacy statement 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 Subject Access Requests.
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 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. ▪ If you would like to learn more about this particular right, please see pages 30-32 ICO, 21 Nov 2017, Guide to the General Data Protection Regulations Version 1

Table 3: An individual's rights under new data protection law, adapted for hearing practice from pages 16-30 of the ICO, 21 Nov. 2017, Guide to the General Data Protection Regulations (GDPR)