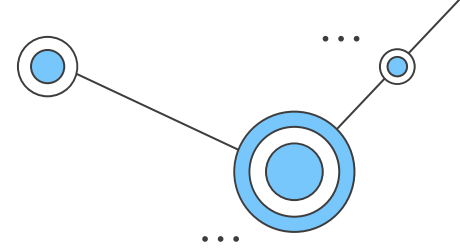


Understanding GDPR


C-102588

How does it apply in
practice?

Understanding GDPR



A brief history of Data Protection



These rules and rights were revised and superseded by the Data Protection Act 1998 which came into force on 1st March 2000

The Data Protection Act 1984 introduced basic rules of registration for users of data and rights of access to that data for the individuals to which it related

GDPR entered into force in 2016 after passing European Parliament, and as of May 25, 2018, all organizations were required to be compliant

8 Principles Of Data Protection

01

Fair & Lawful

Lawfully, fairly and in a transparent manner

02

Purposes

Specified, explicit and legitimate purposes (only those)

03

Adequacy

Adequate, relevant and limited to what is necessary

04

Accuracy

Accurate and, where necessary, kept up to date



8 Principles Of Data Protection

05

Retention

Kept for no longer than is necessary

06

Rights Of Users

Gives individuals the right to choose how their personal data would be used

07

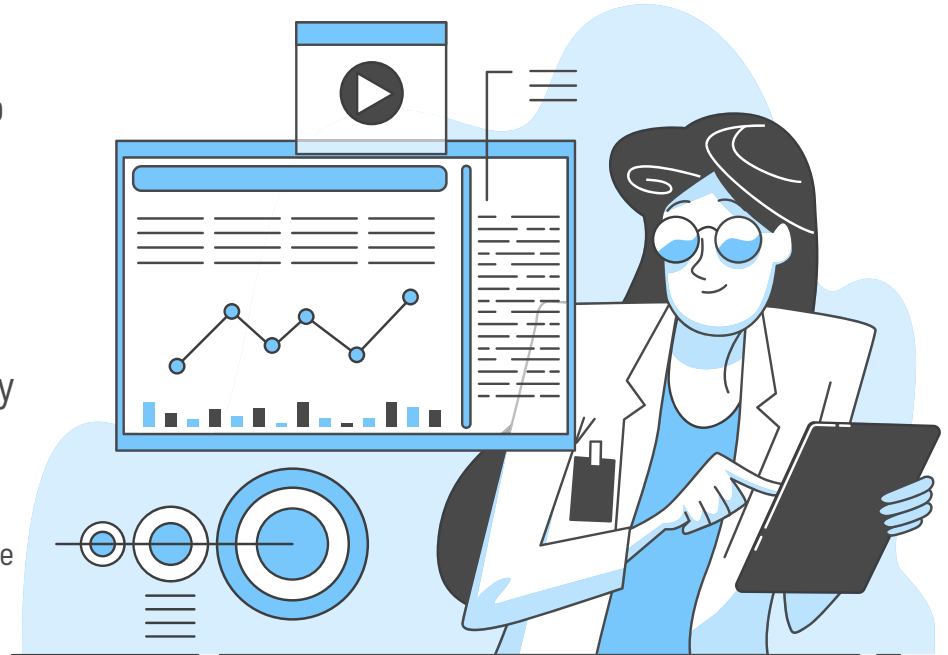
Security

Processed in a manner that ensures appropriate security

08

Data Transfer

Data should not be transferred outside the EU unless the country it is being transferred to can ensure adequate protection of the data





2018 GDPR

General Data Protection Regulation



What changed?

...
...
...
Geographic reach and scope: The previous European Data Protection Directive utilised much more of a light-touch approach than GDPR, setting out aims and requirements for data protection standards that were then implemented through national legislation, such as the UK's Data Protection Act. By contrast, GDPR is a binding piece of regulation, which was legally enforceable as soon as it came into effect on May 25th 2018, and applies to all EU nations and every company holding data on EU citizens.



...
...
...
Definition of personal data: GDPR expanded the definition of "personal data" to include a much wider range of consumer information. Whereas the Data Protection Act only pertains to information used to identify an individual or their personal details, GDPR broadens that scope to include online identification markers, location data, genetic information and more.

...
...
...

...

Consent policies: This is one of the defining differences between GDPR and the Data Protection Act. Under the old rules, data collection did not necessarily require an opt-in, but under GDPR clear privacy notices must be provided to consumers, allowing them to make an informed decision on whether they consent to allow their data to be stored and used. This consent can then be withdrawn at any time.



Data breach policies: With the previous rules businesses were under no obligation to report when data breaches occur, although they were encouraged to do so. This changed with the advent of GDPR, with any future breaches having to be reported to the relevant authorities within 72 hours of the incident.

...

...

Accountability: GDPR places a much greater focus on explicit accountability for data protection, placing a direct responsibility on companies to prove they comply with the principles of the regulation, rather than the hands-off approach of the Data Protection Act. This means firms need to commit to mandatory activities such as staff training, internal data audits and keeping detailed documentation if they wish to avoid falling foul of the GDPR rules.



Data protection governance: The Data Protection Act did not stipulate how the governance of data security functions should be allocated, requiring only a basic commitment to the concept from management. GDPR changes this, as any company employing more than 250 people will be mandated to appoint a dedicated data protection officer, as will any firm processing more than 5,000 subject profiles annually.

...

Penalties and compensation: Previously, non-compliance with the Data Protection Act could see companies fined up to £500,000, or one per cent of annual turnover. Under GDPR, these limits will rise significantly to €20 million, or four per cent of annual turnover, whichever is higher. It's also worth remembering that GDPR will allow individuals to claim compensation for material and non-material damage resulting from data security lapses, whereas the previous rules only covered material damage.

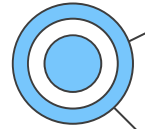




...



What are the rights of our patients?



...

01

**Right to be
informed**

02

**Right of
access**

03

**Right to
rectification**

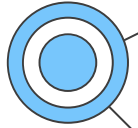
04

**Right to
erase**

...



What are the rights of our patients?



...

05

**Right to
restrict
processing**

06

**Right to
data
portability**

07

**Right to
object**

08

**Rights with regards
to automated
decision making &
profiling**



What are the rights of our patients?

Right	What does this mean in practice?
The right to be informed	<ul style="list-style-type: none">• 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.
The right of access	<ul style="list-style-type: none">• 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
The right to rectification	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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.



What are the rights of our patients?

Right	What does this mean in practice?
The right to restrict processing	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• This is unlikely to apply to optical practices because it applies when processing is carried out by automated means.
The right to object	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• This is unlikely to apply in optical settings.

Personal Data & Special 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 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.

Personal Data & Special Data

- Name
- Address
- Email Address
- Date of Birth
- National Insurance Number

- Racial Origin
- Sexual Orientation
- Health Information
- Genetic & Biometric Data

Data Controller & Data Processor

- 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
CONTROLLER

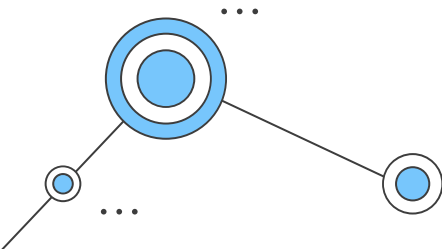
DATA
PROCESSOR

- 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.



KEY ROLES & RESPONSIBILITIES

Who's responsible for what?





DATA CONTROLLER

- 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 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

- 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
- Data processors are also liable for breaches

Patient Data Shared Between Controller & Processor

- 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.





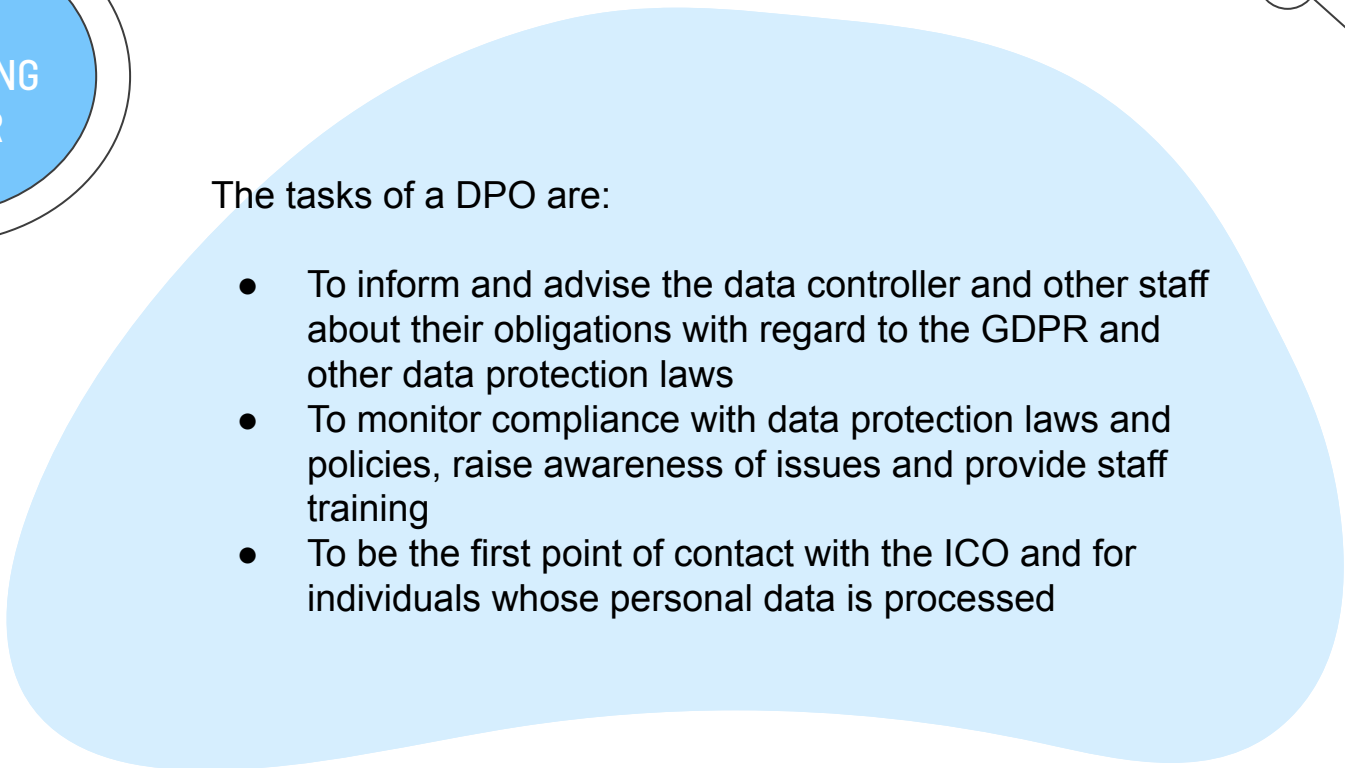
DATA PROCESSING OFFICER

- 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.
- DPO must have experience and expert knowledge of data protection law, 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



DATA PROCESSING OFFICER

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
- 

Identifying The Lawful Basis For Processing Data

- Once all of the personal data and the purposes for which it is intended to be used has been identified, at least one lawful basis for each category of personal data and the purposes of the intended use must be identified before it can be processed.

- Each lawful basis should be documented and included in the privacy notice. This is important 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

Identifying The Lawful Basis For Processing Data

- 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

- 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, it is important to note that this consent is separate from the patient consent you need to provide health services to a patient.

Examples Of Record Keeping In Practice

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.

Examples Of Record Keeping In Practice

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
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.



How to be GDPR Safe In Practice

What YOU need to be aware of to
ensure you stay compliant

- Be aware of who is around you and what may be visible to them
- Be aware of what data is written and stored in the area you work in
- This includes data not stored electronically - post it notes, Rx copies etc
- Shred any personal data on paper, don't just throw it in the bin
- Don't share passwords & ensure screens are locked when you are not using them

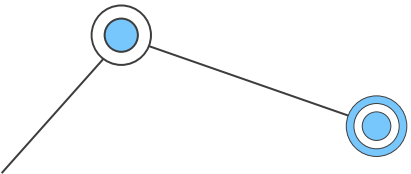
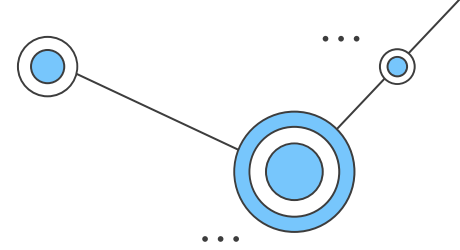


Computer Safety

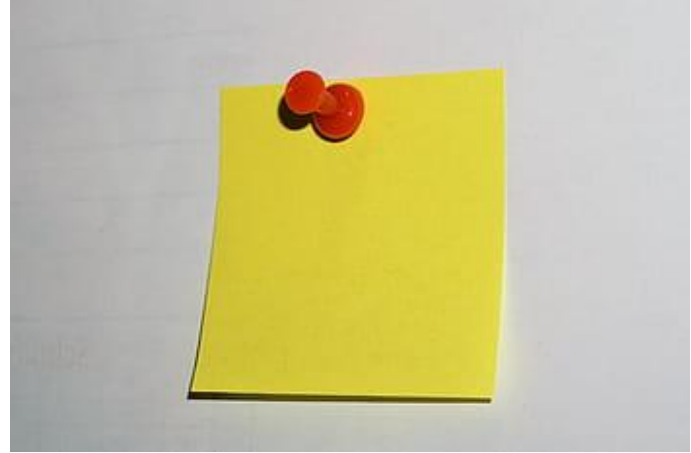
- Be aware of who is around you and what may be audible to them
- Be aware of what data is discussed within earshot of other people - both staff and patients
- Do not repeat sensitive data - especially payment information within earshot of other people
- Make sure you know who you are talking to and confirm they have permission to be given data



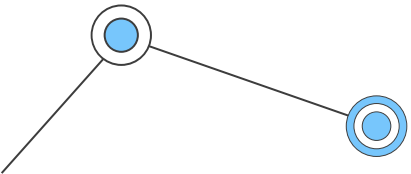
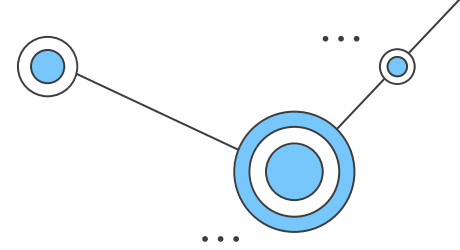
Phone Safety



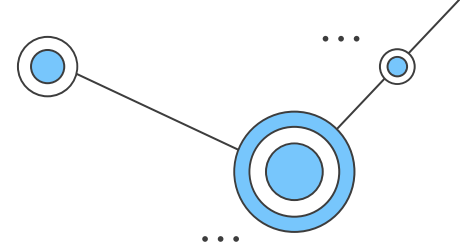
- Be tidy - don't leave personal or sensitive data lying around
- Keep data secure - don't take written data outside of the practice



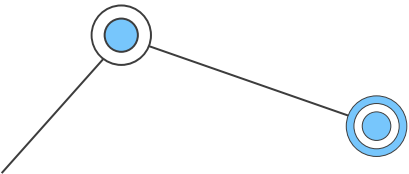
Practice Safety



Key Points



- **Ensure clear guidance and training is given to all staff involved in data handling and processing**
 - **Stay alert and protect privacy at all times**
 - **Treat sensitive data like it's your own**
 - **Consent is key**
 - **Remember the rights of the patient**



Thanks!

Do you have any
questions?

CREDITS: This presentation template was created by [Slidesgo](#), including icons by [Flaticon](#), infographics & images by [Freepik](#) and illustrations by [Stories](#)

