Data Protection Act 2018 and UK GDPR Part 1

Aims: To provide an understanding of the Data Protection Act 2018 and how to apply the UK General Data Protection Regulation (GDPR) to comply with the Data Protection Act 2018 in dental practice. Part 1 gives an overview of GDPR in dental practice. GDPR and an introduction to the Data Use and Access Act 2025 – Part 2 is available on the website and provides a more in depth look at the regulations and requirements.

Learning Outcomes: On completion of this verifiable CPD article the participant will be able to demonstrate, through the completion of a questionnaire, the ability to:

- Define the Data Protection Act 2018.
- Have knowledge of the Data Use and Access Act 2025.
- Identify the 12 steps that should be taken to comply with GDPR.
- Demonstrate more detailed knowledge of the steps required to comply with GDPR.
- Identify key points in gaining consent to meet GDPR compliance.
- Identify the main principles of privacy relating to the GDPR.
- Demonstrate knowledge of how to deal with a data breach.
- Demonstrate knowledge of how a dental practice should show accountability.
- Pass an online assessment, scoring over 70%.

Introduction

The Data Protection Act 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998 and came into effect on 25 May 2018. It was amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU.

It sits alongside and supplements the UK GDPR, the 'UK General Data Protection Regulation'. GDPR is a UK law which came into effect on 01 January 2021. It sets out the key principles, rights, and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.

It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679) which applied in the UK before that date, with some changes to make it work more effectively in a UK context.[1]

Together, the Data Protection Act 2018 and UK GDPR aim to regulate how personal data is collected, used, stored, and shared, ensuring the rights and freedoms of individuals are respected.

The Data Use and Access Act 2025

The first Data (Use and Access) Act 2025 (DUAA) came into force on 19th August 2025.[2] It amends parts of the UK GDPR and the Data Protection Act 2018.

- The DUAA is a new Act of Parliament that updates some laws about digital information matters.
- It changes data protection laws in order to promote innovation and economic growth and make things easier for organisations, whilst it still protects people and their rights.
- Most of the changes offer an opportunity to do things differently, rather than needing you to make specific changes to comply with the law.
- The changes will be phased in between June 2025 and June 2026.[2]

Following the introduction of the DUAA, the ICO will continue to update its guidance on their website, and this should be checked regularly before implementing any changes to policies.

What is Data Protection?

Data protection is the fair and proper use of information about people. It is part of the fundamental right to privacy – but on a more practical level, it is about building trust between people and organisations. It is about treating people fairly and openly, recognising their right to have control over their own identity and their interactions with others, and striking a balance with the wider interests of society.

It is also about removing unnecessary barriers to trade and co-operation. It exists in part because of international treaties for common standards that enable the free flow of data across borders. The UK has been actively involved in developing these standards.

Data protection is essential to innovation. Good practice in data protection is vital to ensure public trust in, engagement with and support for innovative uses of data in both the public and private sectors.[4]

About the Data Protection Act 2018

Everyone responsible for using personal data has to follow strict rules called 'data protection principles.' They must make sure the information is:

- Used fairly, lawfully, and transparently.
- Used for specified, explicit purposes.
- Used in a way that is adequate, relevant, and limited to only what is necessary.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary.
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.[3]

There is stronger legal protection for more sensitive information, such as:

- Race.
- Ethnic background.
- Political opinions.
- Religious beliefs.
- Trade union membership.
- Genetics.
- Biometrics (where used for identification).
- Health.
- Sex life or orientation.

There are separate safeguards for personal data relating to criminal convictions and offences.[3]

Your rights

Your Data
Your Rights

Under the Data Protection Act 2018, you have the right to find out what information the government and other organisations store about you. These include the right to:

- Be informed about how your data is being used.
- Access personal data.
- Have incorrect data updated.
- Have data erased.
- Stop or restrict the processing of your data.
- Data portability (allowing you to get and reuse your data for different services).
- Object to how your data is processed in certain circumstances.[3]

You also have rights when an organisation is using your personal data for:

- Automated decision-making processes (without human involvement).
- Profiling, for example to predict your behaviour or interests.[3]

To find out what data an organisation has about you

You can write to an organisation to ask for a copy of the information they hold about you. If it is a public organisation, write to their Data Protection Officer (DPO). Their details should be on the organisation's privacy notice. If the organisation has no DPO, or you do not know who to write to, address your letter to the company secretary.

How long it should take

The organisation must give you a copy of the data they hold about you as soon as possible, and within 1 month at most. In certain circumstances, for example, particularly complex or multiple requests, the organisation can take a further 2 months to provide data. In this case, they must tell you:

- Within 1 month of your request.
- Why there is a delay.

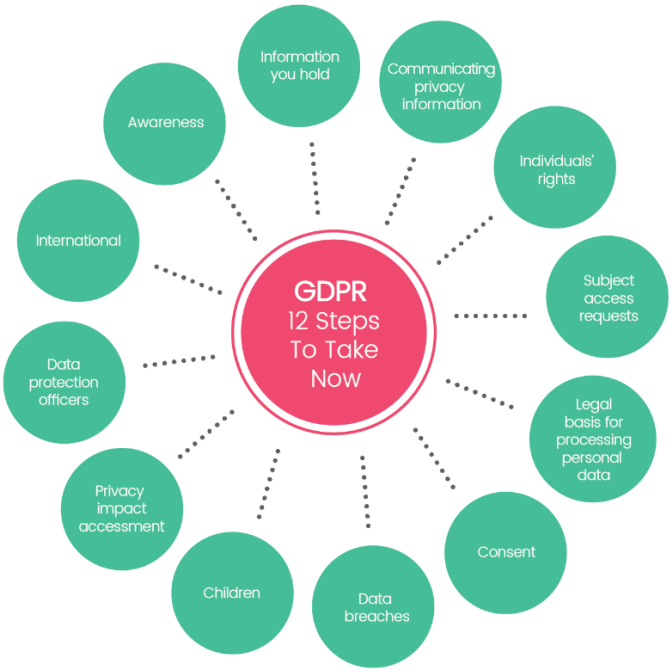
When information can be withheld

There are some situations when organisations can withhold information, for example if the information is about:

- The prevention, detection or investigation of a crime.
- National security or the armed forces.
- The assessment or collection of tax.
- Judicial or ministerial appointments.

An organisation does not have to say why they are withholding information.[3]

12 Steps to GDPR Compliance



1. Awareness

You should make sure that decision makers and key people in your organisation are aware that the law has changed to GDPR. They need to appreciate the impact this is likely to have and identify areas that could cause compliance problems under the GDPR. It would be useful to start by looking at your organisation's risk register if you have one.

Implementing the GDPR could have significant resource implications, especially for larger and more complex organisations.

2. Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit across the organisation or within your business areas.

The GDPR requires you to maintain records of your processing activities. It updates the rights for a networked world. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own records. You will not be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this. Doing this will also help you to comply with the GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

3. Communicating privacy information

Review your current privacy notices and make sure any necessary changes comply with GDPR.

Previously, when you collect personal data, you had to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you must tell people. For example, you need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to complain to the Information Commissioner's Office (ICO) if they think there is a problem with the way you are handling their data. The GDPR requires information to be provided in concise, easy to understand and clear language.

The ICO has developed a code of practice for privacy notices with templates available which organisations can use to ensure they record lawful basis and retention periods and maintain GDPR compliance.

4. Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you delete personal data or provide data electronically and in a commonly used format.

The rights for individuals were previously discussed under your rights (see above).

On the whole, the rights individuals enjoy under the GDPR are the same as those under the DPA (1998) but with some significant enhancements. You should check your procedures and work out how you would react if someone asks to have their personal data deleted, for example, would your systems help you to locate and delete the data? Who will make the decisions about deletion?

The right to data portability is new. It only applies:

- To personal data an individual has provided to a controller.
- Where the processing is based on the individual's consent or for the performance of a contract.
- When processing is carried out by automated means.

You should consider whether you need to revise your procedures and make any changes. You need to provide the personal data in a structured, commonly used and machine-readable form and provide the information free of charge.

5. Subject access requests

Under GDPR the following apply:

- In most cases you will not be able to charge for complying with a request
- You have a month to comply.

- You can refuse or charge for requests that are manifestly unfounded or excessive.
- If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy.
- You must do this without undue delay and at the latest, within one month.

If your organisation handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly. You could consider whether it is feasible or desirable to develop systems that allow individuals to access their information easily online.

6. Lawful basis for processing personal data

The lawful basis for processing personal data under the GDPR is a foundational concept that determines the legal grounds for collecting, using, or storing personal data. It ensures compliance with the principle of lawfulness, fairness, and transparency.

You should identify the lawful basis for your processing activity under the GDPR, document it and update your privacy notice to explain it.

The lawful bases in the GDPR are broadly the same as the conditions for processing in the DPA. It should be possible to review the types of processing activities you carry out and to identify your lawful basis for doing so. You should document your lawful bases in order to help you comply with the GDPR's 'accountability' requirements.

7. Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

You should read the detailed guidance the ICO has published on consent under the GDPR and use the ICO consent checklist to review your practices. Consent must be freely given, specifically informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. It must also be separated from other terms and conditions, and you will need to have simple ways for people to withdraw consent.

Public authorities and employers will need to take particular care. Consent must be verifiable, and individuals generally have more rights where you rely on consent to process their data.

If you rely on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

8. Children

You should consider whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

GDPR provides special protection for children's personal data, particularly in the context of commercial internet services such as social networking. If your organisation offers online services (information society services) to children and relies on consent to collect information about them, then you may need a parent or guardian's consent in order to process their personal data lawfully.

The GDPR sets the age when a child can give their own consent to this processing at 13 in the UK. If a child is younger, then you will need to get consent from a person holding 'parental responsibility'.

This could have significant implications if your organisation offers online services to children and collects their personal data. Remember that consent must be verifiable and that when collecting children's data your privacy notice must be written in language that children will understand. The ICO website should be checked for any changes regarding children's data as it may change this year with the introduction of the Data (Use and Access) Act 2025.

9. Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Some organisations are already required to notify the ICO (and possibly some other bodies) when they suffer a personal data breach. GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases.

You should put procedures in place to effectively detect, report and investigate a personal data breach. You may wish to assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred. Larger organisations will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

10. Data Protection by Design and Data Protection Impact Assessments

It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term 'data protection by

design and by default'. It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- Where a new technology is being deployed;
- Where a profiling operation is likely to significantly affect individuals; or,
- Where there is processing on a large scale of the special categories of data.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, you are required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

You should assess the situations where it will be necessary to conduct a DPIA. Who will do it? Who else needs to be involved? Will the process be run centrally or locally?

You should be familiar with the guidance the ICO has produced on DPIAs as well as guidance from the Article 29 Working Party and work out how to implement them in your organisation. This guidance shows how DPIAs can link to other organisational processes such as risk management and project management.

11. Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

You should consider whether you are required to formally designate a Data Protection Officer (DPO). You must designate a DPO if you are:

- A public authority (except for courts acting in their judicial capacity).
- All practices providing NHS treatment are considered as public authorities and must appoint a DPO or have arrangements to share one. Small practices can share a DPO or use an external DPO service provided the DPO can act independently and is resourced.
- An organisation that carries out the regular and systematic monitoring of individuals on a large scale.
- An organisation that carries out the large-scale processing of special categories of data, such as health records, or information about criminal convictions.

The Article 29 Working Party has produced guidance for organisations on the designation, position, and tasks of DPOs.

It is most important that someone in your organisation, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge, support, and authority to carry out their role effectively.

12. International

You should review procedures for transferring or sharing personal data across borders (either with relevant authorities or others) to ensure that they are compliant.[1]

Protecting data in dental practice

All organisations that collect or use personal data must comply with GDPR. Some of the things you must do to meet it are:

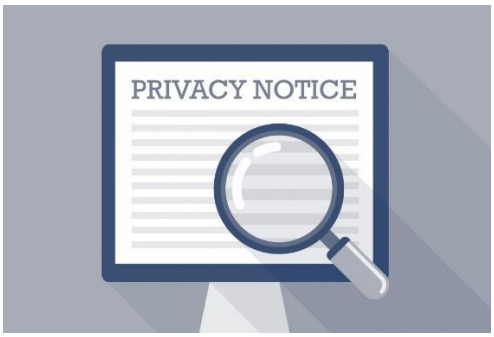
- Process the least possible amount of personal data.
- Only keep it for as long as you need to.
- Carry out assessments to make sure you process personal data in a lawful way.
- Take the right steps to protect data and identify risks to privacy.
- Consider if the person whose data you want to collect needs to give their consent.
- Understand and respect the rights of the person whose data you are collecting.
- Decide if you need to appoint a data protection officer.
- Be transparent and open about the processing of personal data.
- Report any security breaches.[5]

Audit

You should conduct an information audit to clarify what personal data your practice holds:

- Who do you hold information about?
- What information do you hold about them?
- What is the purpose of the processing?
- Who do you share it with?
- How long do you hold it for?
- How do you keep it safe?

Privacy Notices



It is compulsory to have a privacy notice in your dental practice. There are templates available on the ICO website to assist with privacy notices. The point of a privacy notice is to tell people in plain English (or possibly another language):

- Who you are (i.e., the name and contact details of the data controller).
- The name and contact details of the Data Protection Officer.
- What personal information do you hold?
- What you do with their information.
- Who it will be shared with.
- What are you doing to ensure the security of personal data?
- Information about the individual's right of access to their data.
- The retention period for the data.[5]

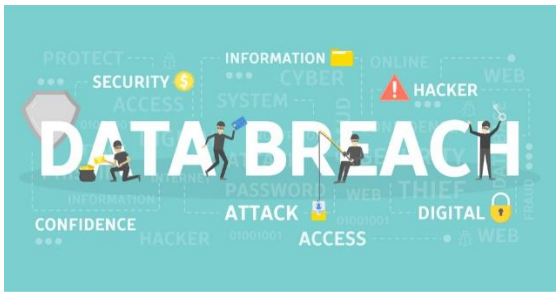
Personal Data

To be able to process your employees' data legally, you have to be able to show that there is a legitimate basis for doing so. The regulation is concerned with the "processing of data". For example, this could be running the monthly payroll or using an employee's data to refer them to occupational health. This applies whether the practice is private or NHS.

The following should be considered:

- What categories of personal data do I process as an employer of staff?
- What do I do with that personal data?
- Why do I do this – what is the legal basis for processing it?
- Is it necessary for me to be processing all the personal data that I have and/or storing it (the more personal data you have, the greater the risk of a breach)?
- Who am I sharing that personal data with? This information would form the basis for your "privacy notice" [6]

Data Breaches



A data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. This means that a breach is more than just losing data.

The main causes of breaches are loss or theft of paperwork; data sent to the wrong person by email; and data posted or faxed to the incorrect person.

Breaches also include deliberate attacks on computer systems; unauthorised access of data by staff; and insecure disposal of paperwork.

You are not only responsible for things that happen in your own practice but also for the personal data that you might pass on to third parties for processing on your behalf. These could be companies that deal with your shredding, payroll, storage, recruitment, or that carry out mail merges on your behalf. You must have a suitable written GDPR-compliant contract with such third parties.

Informing the Information Commissioner's Office

You need to notify the Information Commissioner's Office (ICO) of a breach where it is likely to present a risk to the rights and freedoms of individuals. If you have a breach and you decide that there is no risk to the rights and freedoms of the individuals concerned, then you don't need to report it. This decision would be made following an assessment of the situation. The GDPR does not tell you when to self-report. You need to decide. You should document your decision. The ICO is an advocate of voluntary self-reporting.

The Data Security and Protection Toolkit

All care providers who work under the NHS Standard Contract must register with the toolkit. You can use the NHS Digital Data Security and Protection Toolkit to measure if you meet the National Data Guardian's standards and GDPR. It will help you find out what do if there are any standards you do not meet.

Personal Development Plan and Reflective Learning

This CPD is linked to the following GDC Enhanced CPD Development Outcome:

A. Effective communication with patients, the dental team, and others across dentistry, including when obtaining consent, dealing with complaints, and raising concerns when patients are at risk.

C. Maintenance and development of knowledge and skill within your field of practice.

D. Maintenance of skills, behaviours and attitudes which maintain patient confidence in you and the dental profession and put patients' interests first.

Reflective learning is now a requirement of the GDC Enhanced Professional Development Scheme. As such, you will be given the option to answer some reflective learning questions, before your certificate is generated.

Please remember that you can choose if you wish to fill this in on completion of the exam, but you can also update this at any time from your CPD log. If you take a few moments to write your reflection on completion, you will have fulfilled the Enhanced CPD requirements.

Further Reading

General information about GDPR - https://ico.org.uk.

A useful checklist to make sure you are compliant with GDPR –

Data protection self assessment | ICO

References:

1.Information Commisioners Office (2025) Available from: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/ (accessed 21/11/2025).

2..Information Commisioners Office (2025) Available from: https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/ (accessed 21/11/2025).

3. Gov.Uk (2025) Available from: https://www.gov.uk/data-protection/(accessed 21/11/2025).

4. Information Commisioners Office. (2025) Available fromhttps://ico.org.uk/for-organisations/advice-for-small-organisations/ (accessed 21/11/2025).

5. CQC (2022) Available from: https://www.cqc.org.uk/guidance-providers/all-services/check-way-you-handle-personal-information-meets-right-standards-0 (accessed 21/11/2025).

6. MDDUS (2022) Available from: https://www.mddus.com/-/media/files/training-and-cpd/learning-tools-and-exercises/guidance-sheet---privacy-notices-gdpr-june-22.pdf (accessed 21/11/2025).