Data Protection Act 2018 and UK GDPR Part 2

Aims: To provide a further understanding of the Data Protection Act 2018, UK GDPR, and the Data Use and Access Act 2025, exploring in more detail the roles and responsibilities of the Data Controller and Data Processor; Data Protection Impact Assessments; data breaches and ransomware; cyber security; and storing and using employment information.

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:

- Understand the purpose of the Data Protection Act 2018.
- Have knowledge of the Data Use and Access Act 2025.
- Know the role of the Data Protection Officer.
- Know the role and responsibilities of the Data Protection Controller.
- Know the role and responsibilities of the Data Protection Processor.
- Understand the purpose of a Data Protection Impact Assessment.
- Have knowledge of how a data breach could occur.
- Have knowledge of storing, using and sharing employees' data.
- 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 GDPR UK, 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.

Data Protection Officer

The Data Protection officer is a designated individual within an organisation responsible for overseeing compliance with data protection laws and acting as a point of contact for data subjects and supervisory authorities.

Their key responsibilities are:

- Monitor the organisation's compliance with data protection laws.
- Advising the organisation on its obligations under the UK GDPR and DPA 2018.
- Acting as a contact point for the Information Commissioner's Office (ICO) and data subjects.
- Conducting Data Protection Impact Assessments (DPIAs) when necessary.
- Remaining independent within the organisation (cannot be penalised for performing their duties).

Data Controller

The Data Controller holds the key decision-making power over the use of personal data, making them responsible for ensuring compliance with GDPR and protecting individuals' data rights. Essentially, the data controller decides why and how personal data is processed. The Information Commissioner Office defines the controller as:

"The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."[3]

A controller can be a company or other legal entity (such as an incorporated partnership, incorporated association or public authority), or an individual (such as a sole trader, partner in an unincorporated partnership, or self-employed professional, e.g. a barrister). The controller can be a jointly held position.

Responsibilities of a Data Controller

Collecting Data: The data controller decides the reason for collecting personal data (e.g., for marketing, payroll, or service delivery purposes). The controller is responsible for ensuring processing including any processing carried out by a processor on your behalf complies with the UK GDPR.[4,5]

Determining the Processing Methods: The controller defines how the personal data will be processed, including the technology, security measures, and duration of storage. [4,5]

Compliance with UK GDPR: The controller is primarily responsible for ensuring that data processing complies with GDPR principles and regulations. This includes ensuring that data is collected lawfully, transparently, and for legitimate purposes. [45]

Handling Data Subject Rights: The controller must respond to and facilitate data subjects' rights, such as requests for access to their data, rectification, erasure (right to be forgotten), and data portability. [4,5]

Selecting and Overseeing Processors: The controller can only use a processor that provides sufficient guarantees that they will implement appropriate technical and organisational measures to ensure their processing meets UK GDPR requirements. If the controller uses a third-party service (referred to as a Data Processor) to handle or process personal data on its behalf (e.g., cloud storage, payroll services), the controller remains responsible for ensuring that the processor complies with GDPR and other applicable regulations. Contracts or data processing agreements must be in place to ensure this.[4,5]

Data Breach Notifications: The controller is responsible for reporting any data breaches to the relevant data protection authority and, in some cases, to the affected individuals within 72 hours, as required by GDPR. [4,5]

Co-operation with supervisory authorities: The controller must cooperate with supervisory authorities (such as the Information Commissioner's Office (ICO) and help them perform their duties. [4,5]

Data protection fee: The controller must pay the ICO a data protection fee unless they are exempt. [4,5]

Data Processor

A Data Processor is an entity (organisation or individual) that processes personal data on behalf of the Data Controller under the instructions given by the controller. Processors act on behalf of the relevant controller and under their authority and in doing so, they serve the controller's interests rather than their own. The Information Commissioner Office defines the data processor as:

"A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

Responsibilities of a Data Processor

Processors have less autonomy and independence over the data they process, but they do have several direct legal obligations under the UK GDPR and are subject to regulation by supervisory authorities. A processor has the following obligations:

Controller's instructions: The processor can only process the personal data on instructions from a controller (unless otherwise required by law).[5,6]

Processor contracts: The processor must enter into a binding contract with the controller. This must contain a number of compulsory provisions, and they must comply with their obligations as a processor.[5,6]

Sub-processors: The processor must not engage another processor (i.e. a sub-processor) without the controller's prior specific or general written authorisation. If authorisation is given, the processor must put in place a contract with the sub-processor with terms that offer an equivalent level of protection for the personal data as those in the contract between the processor and the controller.[5,6]

Security: The processor must implement appropriate technical and organisational measures to ensure the security of personal data, including protecting against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.[5,6]

Notification of personal data breaches: If the processor become aware of a personal data breach, they must notify the relevant controller without undue delay. Most controllers will expect to be notified immediately, and may contractually require this, as they only have a limited time in which to notify the supervisory authority (such as the ICO). The processor must also assist the controller in complying with its obligations regarding personal data breaches.[5,6]

Notification of potential data protection infringements: The processor must notify the controller immediately if any of their instructions would lead to a breach of the UK GDPR or local data protection laws.[5,6]

Accountability obligations: The processor must comply with certain UK GDPR accountability obligations, such as maintaining records and appointing a data protection officer.[5,6]

International transfers: The UK GDPR's prohibition on transferring personal data applies equally to processors as it does to controllers. This means you must ensure that any transfer of data outside the UK is authorised by the controller and complies with the UK GDPR's transfer provisions.[5,6]

Co-operation with supervisory authorities: The processor is also obliged to cooperate with supervisory authorities (such as the ICO) to help them perform their duties.[56]

Summary Table

Role	Decision-Making Authority	Direct Responsibility for Compliance	Accountability	Required by Law?
Data Controller	Decides **why** and **how** data is processed.	Primary responsibility.	Accountable to supervisory authorities (e.g., ICO).	Always needed when processing personal data.
Data Processor	Acts under controller's instructions.	Shared responsibility (with controller).	Accountable to the controller and ICO.	Depends on whether the controller outsources processing.
Data Protection Officer	No decision-making power over processing.	Ensures compliance and provides advice.	Reports to the highest level of management.	Required in specific cases (e.g., public authorities, large-scale monitoring, special categories of data).

Data Protection Impact Assessment (DPIA)

A DPIA is a process designed to help to systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of a company's accountability and obligations under UK GDPR, and when done properly helps to assess and demonstrate how to comply with all of the data protection obligations.[1]

Dental practices handle a significant amount of sensitive personal data, including health records, medical histories, payment details, photographs and X-rays, making data protection a priority. DPIAs help dental practices assess the risks associated with data processing and adopt measures to protect patients' privacy.[7]

Why do we Need a DPIA?

A DPIA can cover a single processing operation, or a group of similar processing operations. A DPIA can be used for more than one process and, it can be amended to use for different processes. In dental practice a DPIA should be in place to ensure data protection for the following:

- **Patient Health Records:** Dental practices store detailed records about a patient's health history, treatment plans, and ongoing care.

- **Digital Data Processing:** Many practices use electronic systems for appointment systems, patient records, and communication, introducing potential risks of unauthorised access.

- **Third-party Processors:** Practices may share patient data with dental laboratories, insurance companies, or referral partners, which must be carefully managed.

- **Automated Appointment Systems:** Use of automated text reminders, emails, or marketing communications can raise privacy concerns.

- **CCTV and Monitoring:** Some practices may use security cameras that record patient areas, potentially requiring a DPIA.

There may be other processes that also require a DPIA in dental practice and this list is not exhaustive. It is important to remember that DPIAs are also relevant if you are planning to make changes to an existing system. In this case you must ensure that you do the DPIA at a point when there is a realistic opportunity to influence those plans for example if you decide to change computer software systems a DPIA should be considered and in place before using the new software.[8]

A DPIA in a dental practice is an important tool for maintaining patient trust and meeting legal obligations regarding data protection. By carefully evaluating the ways personal data is processed and identifying potential risks, dental practices can implement strong safeguards to ensure that patient data is handled securely and responsibly.

Key Steps in Conducting a DPIA for a Dental Practice

1. **Describe the data that needs processing:**

Document the types of personal data you process (e.g., patient records, payment information, appointment details) and why it's being processed.

2. **Is it necessary to collect the data?**

Ensure that the data collection and processing activities are necessary for the delivery of dental services and in line with legal obligations.

3. **Identify and assess risks:**

Consider the potential risks to patient data, including unauthorised access, data breaches, or accidental loss of data. For example: What happens if a patient’s health record is exposed to unauthorised personnel? How secure are digital patient management systems against cyber threats? Are there risks associated with sharing data with third parties like dental laboratories?

4. **Implement safeguards and mitigation measures:**

Based on the identified risks, implement appropriate controls to mitigate them. This could include encrypting patient health records; limiting access to sensitive data to only authorised personnel; training staff on data protection best practices.

5. **Using secure communication for patient communication.**

Reviewing contracts with third-party providers to ensure compliance with data protection laws. Consult with relevant stakeholders: In certain cases, especially for larger practices, consultation with patients or dental staff can provide insights into potential data protection risks and concerns.

6. **Document the DPIA:**

Keep a record of the assessment, including details about data processing, identified risks, and mitigation strategies. This documentation can be provided to a data protection authority if requested.[8]

Data Breaches and Ransomware

The ICO define a data breach as: "A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes."[9]

Data breaches in dental practice have become increasingly common and sensitive patient data information is a prime target for cybercriminals.

Data breaches could occur because of:

- **Stolen or Lost Devices** - Laptops, tablets, and other portable devices containing patient information can be lost or stolen if not properly secured.

- **Unsecured Networks** - Using outdated software or not encrypting patient data can make systems vulnerable to attacks.

- **Weak Password Use** - Weak, reused, or improperly managed passwords are a common vulnerability that attackers exploit to gain unauthorised access to

systems and data. Passwords should not be shared within the dental team, they should be updated regularly and encrypted on the system.

- **Phishing Attacks** - Cybercriminals use fraudulent emails to trick staff into revealing login credentials or other sensitive information.

- **Ransomware** - Hackers encrypt a practice's data and demand a ransom to unlock it.

- **Employees** – Employees may accidentally or intentionally compromise patients' data.

Data breaches can impact the practice in different ways for example, financially, they could damage patient trust in the practice, and they could result in legal ramifications for the practice.

To reduce the risk of data breaches a practice should have the following in place:

- ✓ Control access to sensitive data.
- ✓ Conduct regular staff training.
- ✓ Have robust risk assessments and audit controls in place.
- ✓ Perform regular software and antivirus updates.
- ✓ Conduct backups and test the system of backups regularly.
- ✓ Have a policy in place to adhere to should a data breach occur.

Reporting a Data Breach

Practices may need to notify the Information Commissioner's Office (ICO) of a breach if it is likely to present a risk to the rights and freedoms of individuals. If there is a breach and a risk assessment has determined that there is no risk to the rights and freedoms of the individuals concerned, and the data can be restored in a timely manner, then the practice does not need to report it. This decision would be made following an assessment of the situation. GDPR does not advise when to self-report. The dental practice needs to decide and the decision should be documented.

The ICO should be notified within 72 hours of a known data breach.

Further information on reporting data breaches can be found here: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/

Storing and Using Employment Information

Complying with the GDPR in handling employee data is crucial for dental practices. It demonstrates a commitment to protecting employee privacy, enhances data security, and builds trust with employees. Employees are granted several rights under GDPR, including:

- The right to access their data.
- The right to object to data processing.
- The right to amend their data.
- The right to request deletion of their data.[10]

A record should be maintained of each employee's consent to recording their data including the date of consent, the method used to obtain consent and the purpose of processing their data. This record should be regularly reviewed and renewed.

Under the GDPR, organisations should establish clear retention periods for employee data which should be recorded. Once the retention period for employee data has expired, practices should ensure secure disposal to prevent unauthorised access or misuse.[11]

What Information Can Be Stored?

You may collect information that is essential for employment purposes, such as:

- **Personal details**: Name, address, contact information, date of birth.
- **Employment history**: CVs, references, qualifications, and training certificates.
- **Financial details**: National Insurance number, bank details for payroll. Pension information.
- **Health information**: Necessary for occupational health assessments, or compliance with health and safety laws. Sickness and Injury records.
- **Performance data**: Appraisals, disciplinary records, attendance, and training records. References from previous employers.

- **Equality and Diversity Information**: Information about ethnicity, religion, disability.[11,12]

Using Employment Information

Employee data may be used for:

- Payroll, contractual and benefits administration.
- Compliance with regulatory requirements: GDC registration checks, the Care Quality Commission may require certain employment information for inspections.
- Health and safety compliance.
- Performance management: Appraisals, Continuing Professional Development records, training and development.

Practices must be transparent and inform employees via a privacy notice about how their data will be used. They should only collect and use data necessary for specific purposes and should avoid using data in ways employees wouldn't reasonably expect.[11]

Who Can Employees Data Be Shared With?

Employee data may be shared with:

- HMRC: For tax and National Insurance reporting.
- Pension providers: For auto-enrolment purposes.
- Regulatory bodies: For compliance with GDC or CQC regulations.
- Occupational health providers: For necessary health assessments.

Personal data should not be shared without a legal basis or explicit consent and the practice should ensure third parties comply with data protection laws. Properly managing employee data is critical to maintaining trust and legal compliance. Employers should establish robust policies and practices to protect personal data while meeting business needs.

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 Commissioner's Office (2025) Available fromhttps://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/ (accessed 24/11/2025).

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 24/11/2025).

3. Information Commissioner's Office (2025) Available from: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-are-controllers-and-processors/#1 (accessed 24/11/2025).

4. Information Commissioner's Office (2025) Available from: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-does-it-mean-if-you-are-a-controller/ (accessed 24/11/2025).

5.Information Commissioner's Office (2025) Available from: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/ (accessed 24/11/2025).

6. Information Commissioner's Office (2025) Available from: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-does-it-mean-if-you-are-a-processor/#1(accessed 24/11/2025).

7.Dental Protection (2018) Available from: https://www.dentalprotection.org/ireland/publications-resources/articles/article/how-does-the-new-gdpr-affect-my-practice (accessed 24/11/2025).

8. Information Commissioner's Office (2025) Available from: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/what-is-a-dpia/#what1 (accessed 24/11/2025).

9. Information Commissioner's Office (2025) Available from: https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/personal-data-breaches/#:~:text=A%20personal%20data%20breach%20means,than%20just%20losing%20personal%20data. (accessed 24/11/2025).

10.Privacy Affairs (2024) Available from:https://www.privacyaffairs.com/employee-data-processing (accessed 24/11/2025).

11.GDPR Advisor (2023) Available from: https://www.gdpr-advisor.com/gdpr-and-employee-data-balancing-privacy-rights-and-hr-practices/ (accessed 24/11/2025).

12.ICO (2024) Available from: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/employment-practices-and-data-protection-keeping-employment-records/ (accessed 12/10/2024).