

Beginner's Guide to being a Data Protection Officer

*"or... everything you always wanted to know
about GDPR and DPOs, but were afraid to ask..."*

Joe McCrea

Who am I?...

- Started life in the ministerial corridor at DoH 21 years ago
- Worked in health comms and organisational consultancy for and with Acute Trusts, Community Trusts, Commissioners, NHS England, NHS Improvement, NHS Change Day, NHS Citizen, NHS Providers, NHS Confederation
- Head of Communications – ELR CCG 2015-2016
- Head of Communications for ELR GP Federation since 2015 to present



Who am I?...

- Director at RSM Robson Rhodes – audit, assurance and compliance mapping
- Supported NAO Home Office External Audit Team
- Strategic Partner to DWP Internal Audit Division
- NAO Working Group on implementation of FOI
- Cabinet Office Senior Civil Service Management Team in the Office of the e-Envoy
- Member of e-Government Unit introducing e-GIF and e-GMF
- Data Protection Officer for 27 GP practices across East Leicestershire and Rutland



What are we going to
do today?...

What we're going to do today...

- Get a common sense, no jargon understanding of GDPR
- Confirm what's new, what's not
- Understand where YOU are, what YOU think and what you NEED
- Understand the role of the DPO – what it is, what it isn't
- Look at key elements of GDPR compliance – in particular for GP Practices
- Discuss and debate the priority areas needing clarity and support



You'll learn about...

Data Protection Officer (DPO)	Lawful basis for processing personal data	Legitimate Interests
Consent	Vital interests	Research activities
Data Protection Fee and Registering DPO	Right to be informed including privacy information	Right of access
Right to restrict processing	Right to rectification and data quality	Right to erasure including retention and disposal
Right to restrict processing	Right to object	Information Audit
Information Asset Register	Privacy Notice	Accountability
Processor contract		

What we're NOT going to do...

- Suffer a 4-hour long lecture
- Spend all our time with ME talking at YOU
- Allow YOU to get away with not contributing YOUR views or opinions



We'll tell each other about...

- Our opinion and knowledge of GPDR
- Our fears and challenges
- The problems we're facing
- The hurdles we're encountering
- What's working, what's not
- The solutions we're adopting
- The 'handy hints' we may have
- What advice we still need from the ICO



Your voice WILL be heard...

- We will capture the outputs and lessons learned from today's session
- We will publish them in a "Learning Lessons" Report
- We'll submit it to NHS England and the local CCGs
- We'll send it to the Information Commissioner's Office



We're going to be interactive...

- You all have a voting pad to use throughout the session
- I'll tell you when each vote is open
- You'll see the votes build in real time
- Then you'll see the correct answer or ranking results
- We'll be testing your **knowledge**
- And we'll be asking your **opinion**




How you vote...

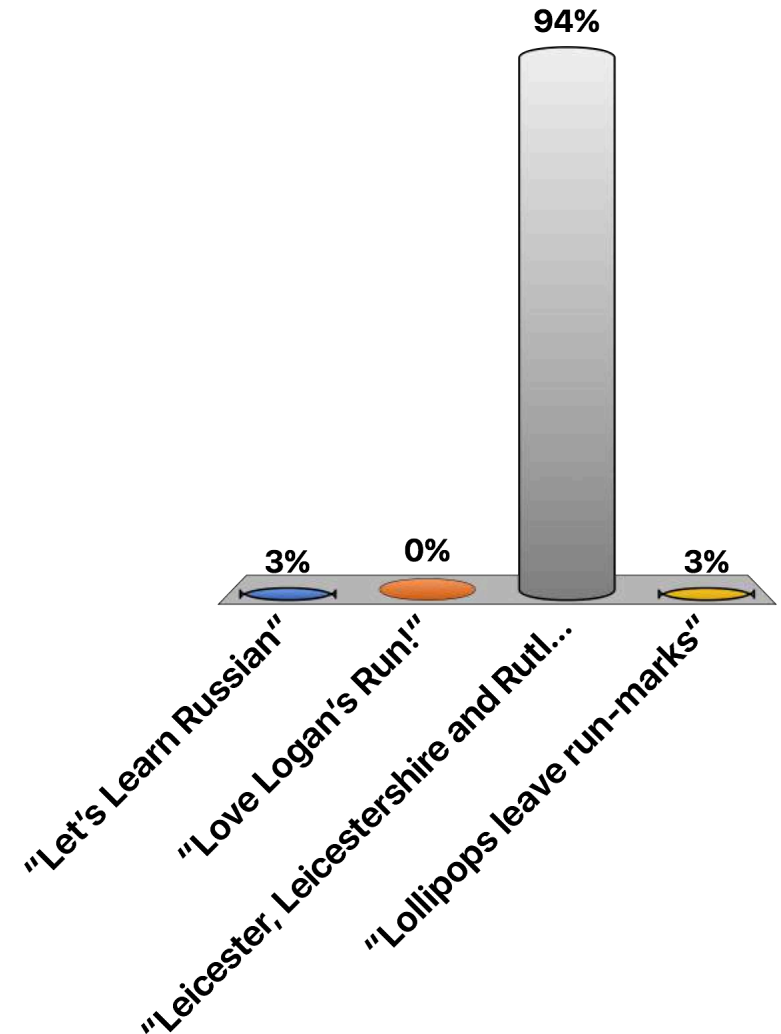
- Select the button corresponding to your answer choice
- On a single choice, only your first answer counts
- On a ranking question, you have up to three votes – your first choice scores more heavily than your second, which scores more heavily than your third



Let's give it a try...

LLR stands for...

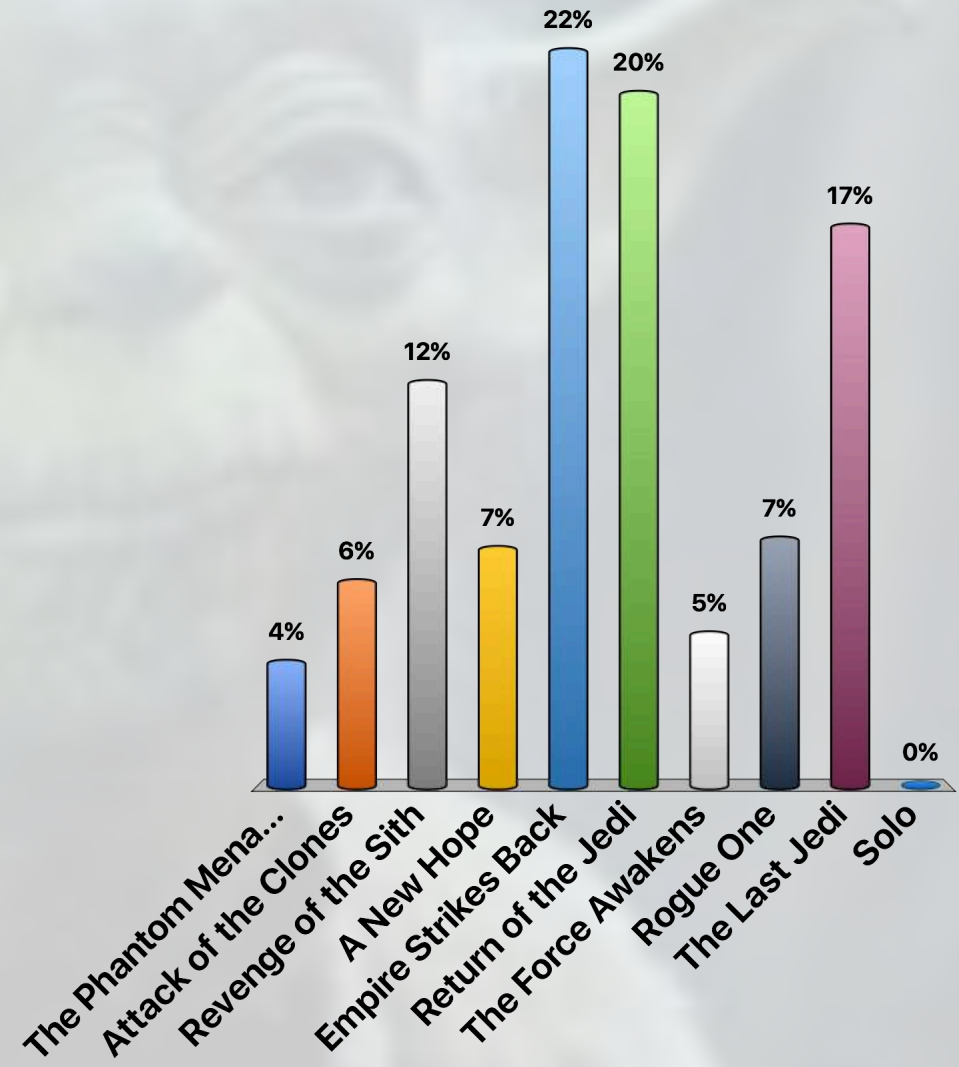
- A. "Let's Learn Russian"
- B. "Love Logan's Run!"
-  C. "Leicester, Leicestershire and Rutland"
- D. "Lollipops leave run-marks"



Example of up to 3 answers

The Force is with...

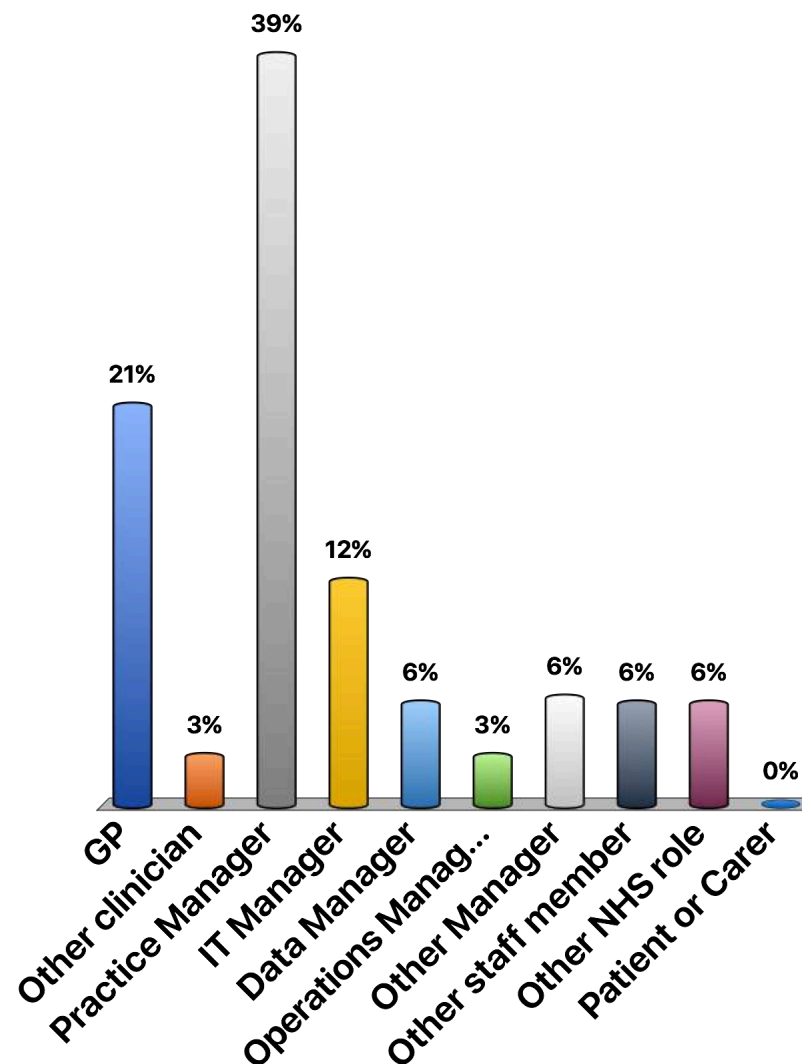
- A. The Phantom Menace
- B. Attack of the Clones
- C. Revenge of the Sith
- D. A New Hope
- E. Empire Strikes Back
- F. Return of the Jedi
- G. The Force Awakens
- H. Rogue One
- I. The Last Jedi
- J. Solo



Let's find out about
you...

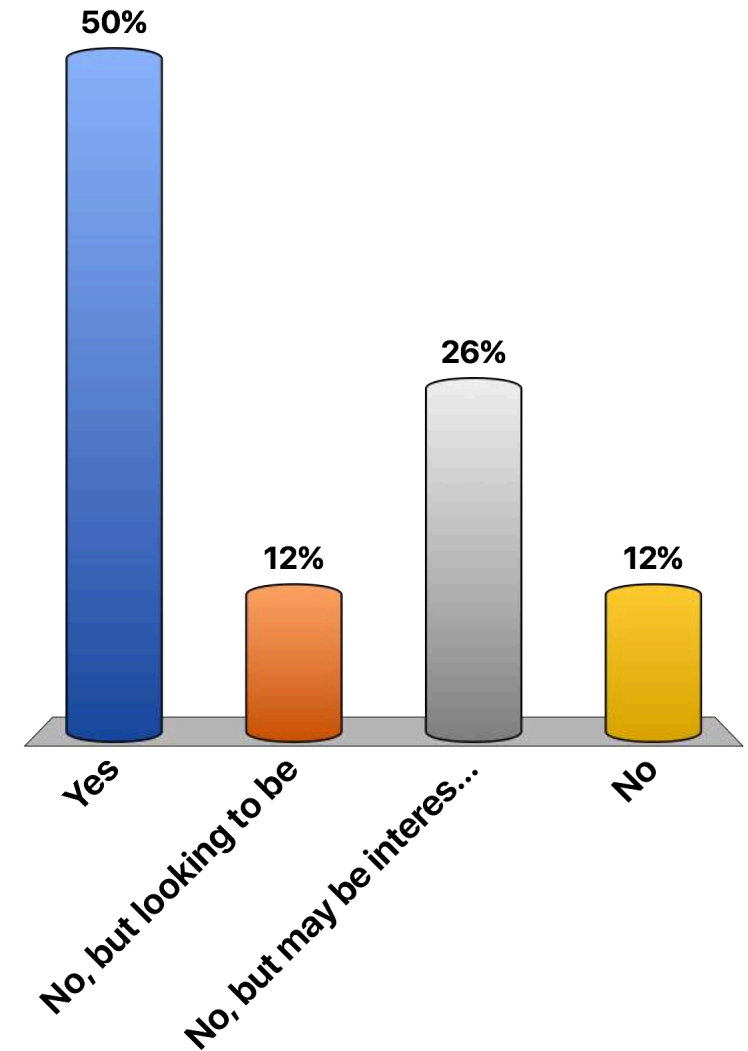
What's your job title?

- A. GP
- B. Other clinician
- C. Practice Manager
- D. IT Manager
- E. Data Manager
- F. Operations Manager
- G. Other Manager
- H. Other staff member
- I. Other NHS role
- J. Patient or Carer



Are you a DPO?

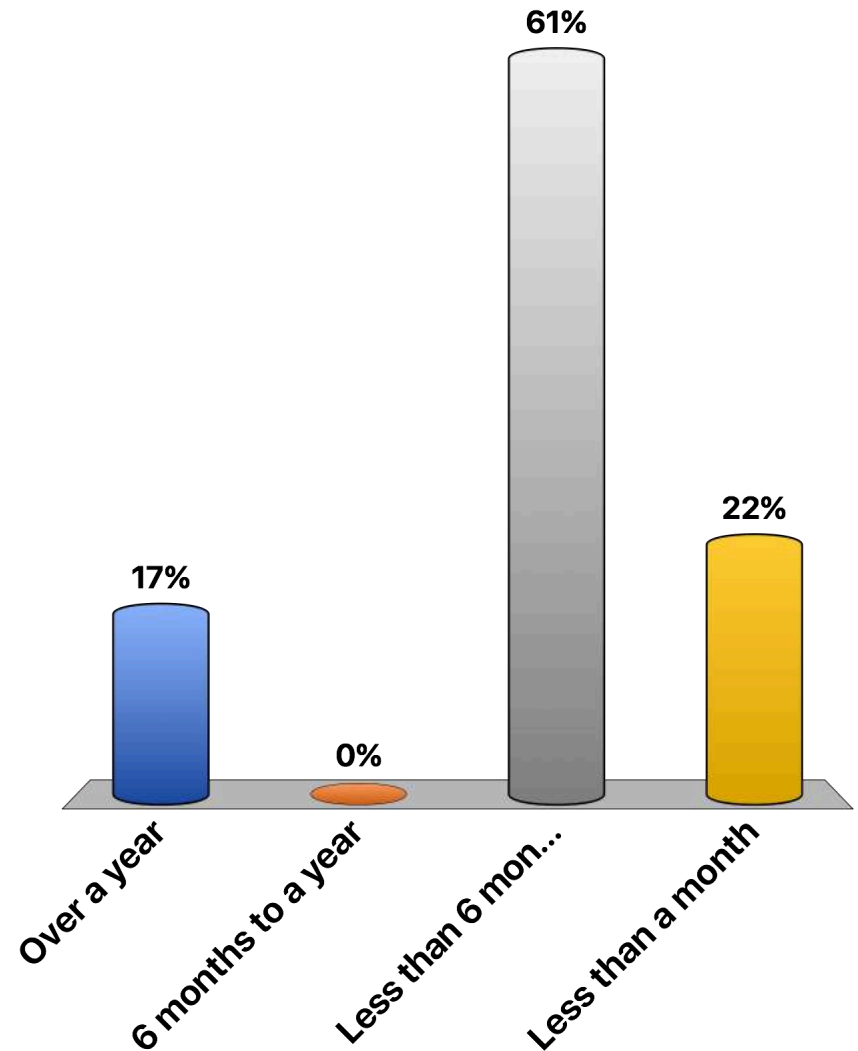
- A. Yes
- B. No, but looking to be
- C. No, but may be interested
- D. No



Single answer

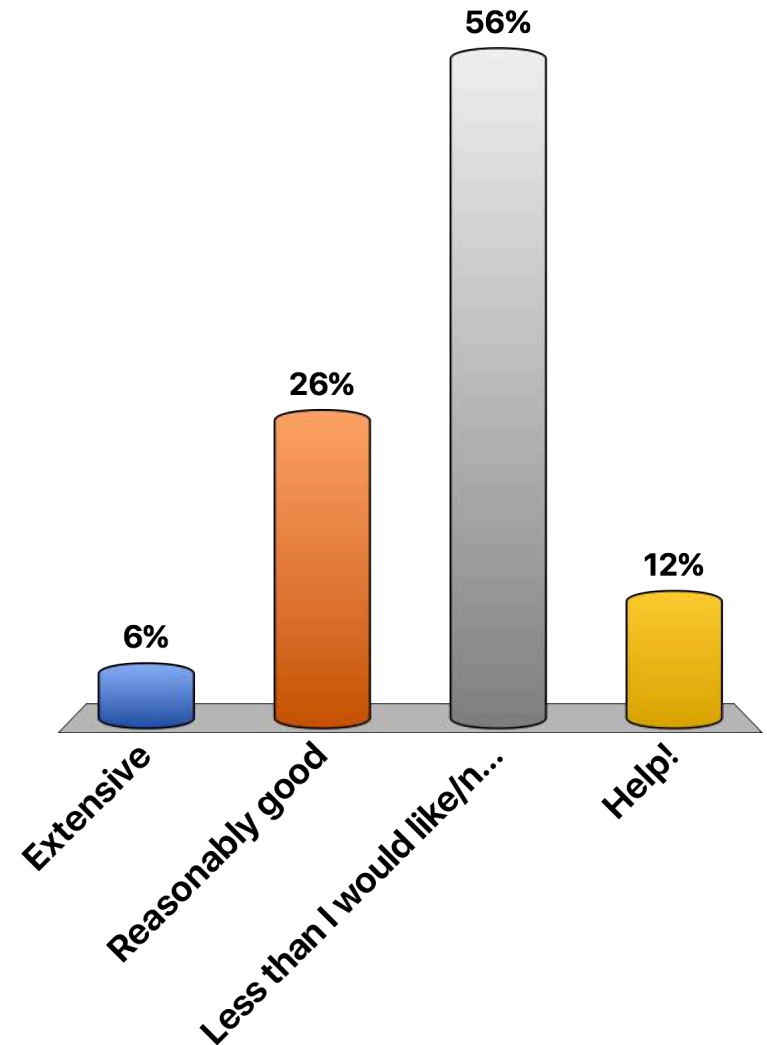
How long have you been a DPO?

- A. Over a year
- B. 6 months to a year
- C. Less than 6 months
- D. Less than a month



How would you rate your knowledge of GDPR?

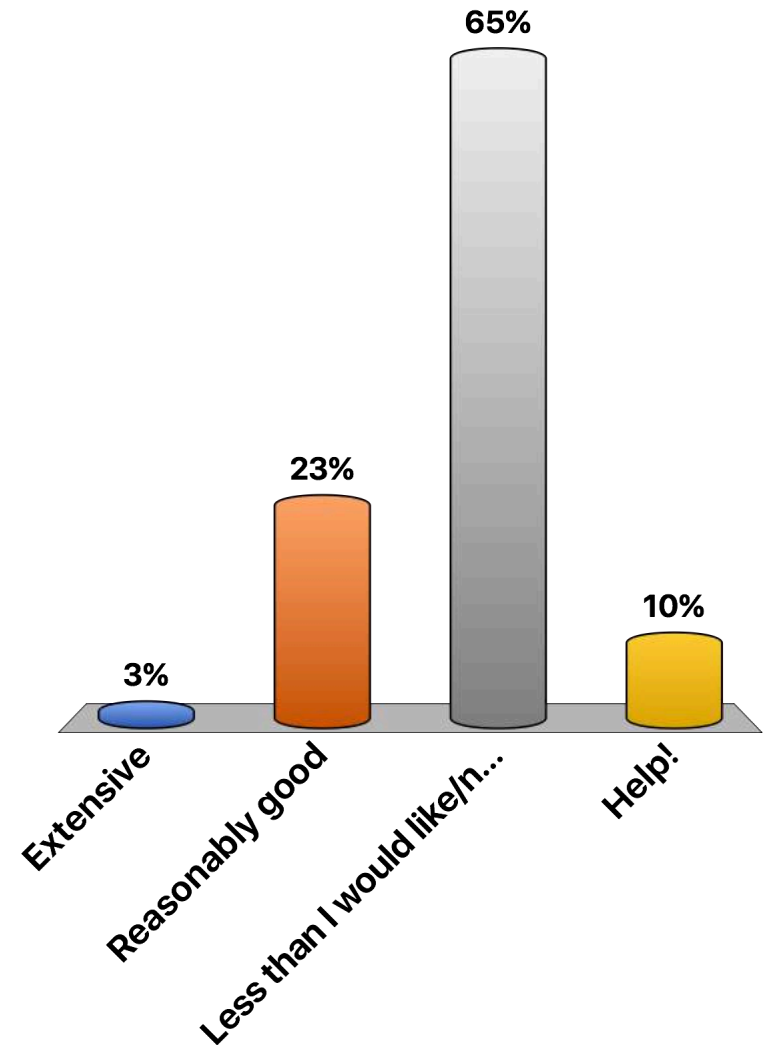
- A. Extensive
- B. Reasonably good
- C. Less than I would like/need
- D. Help!



Single answer

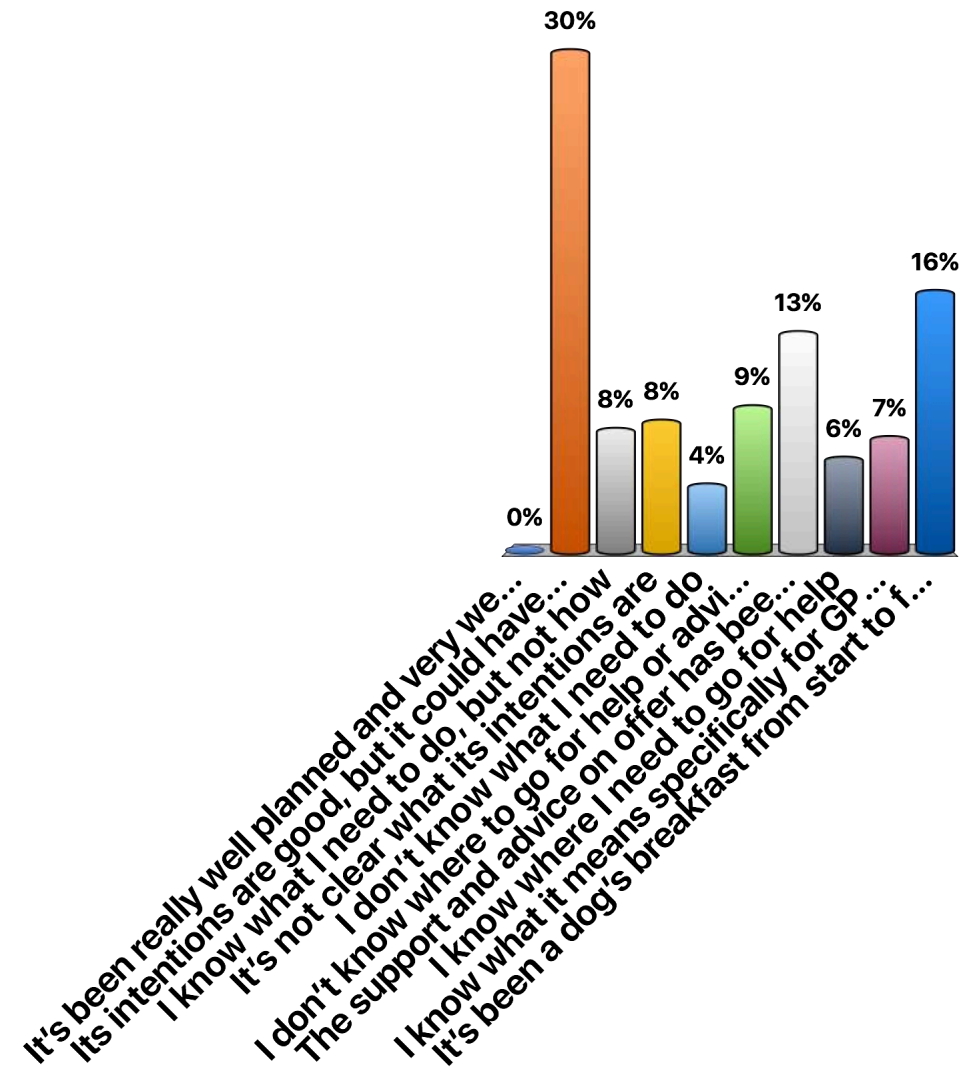
How would you rate your knowledge of the DPO role?

- A. Extensive
- B. Reasonably good
- C. Less than I would like/need
- D. Help!



What's your view of GDPR?...

- A. It's been really well planned and very well explained
- B. Its intentions are good, but it could have been better explained
- C. I know what I need to do, but not how
- D. It's not clear what its intentions are
- E. I don't know what I need to do
- F. I don't know where to go for help or advice
- G. The support and advice on offer has been reasonable but not accessible
- H. I know where I need to go for help
- I. I know what it means specifically for GP Practices
- J. It's been a dog's breakfast from start to finish

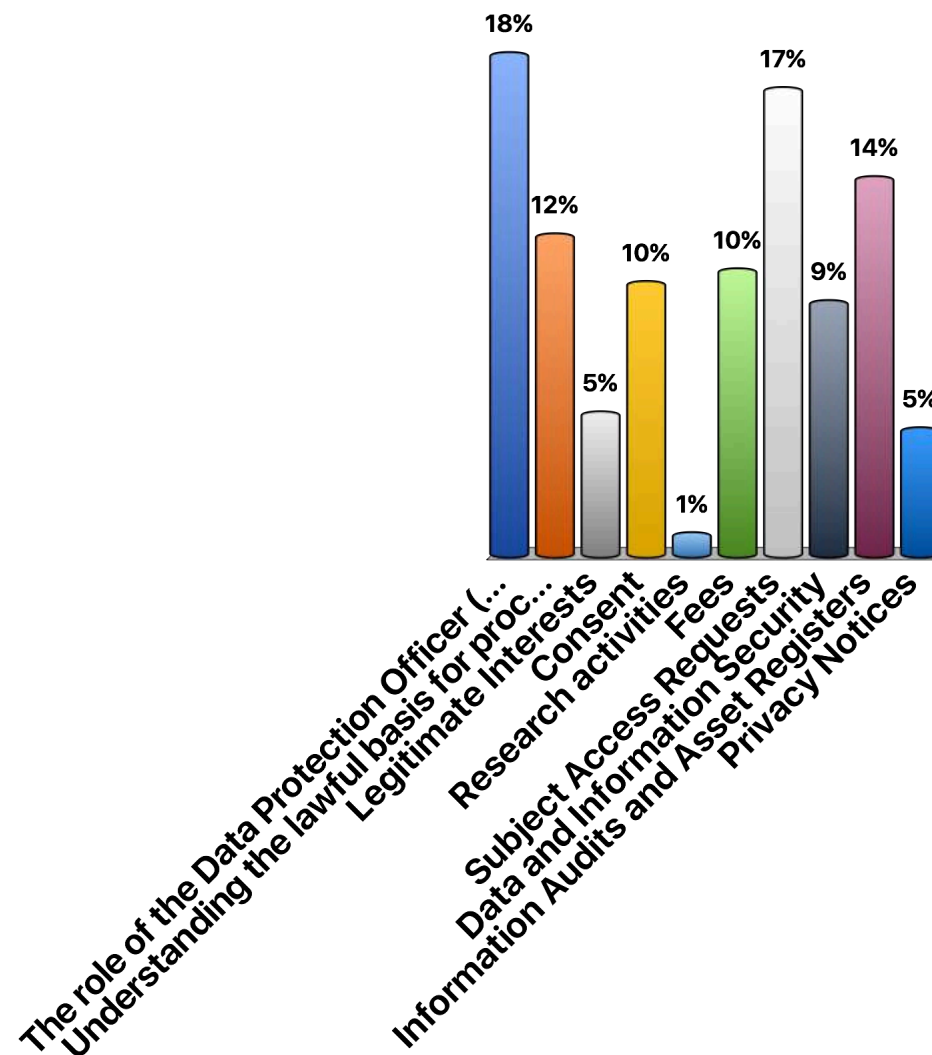


Up to 3 answers

What's your top 3 GDPR areas where you need help?

ELR GP
Federation

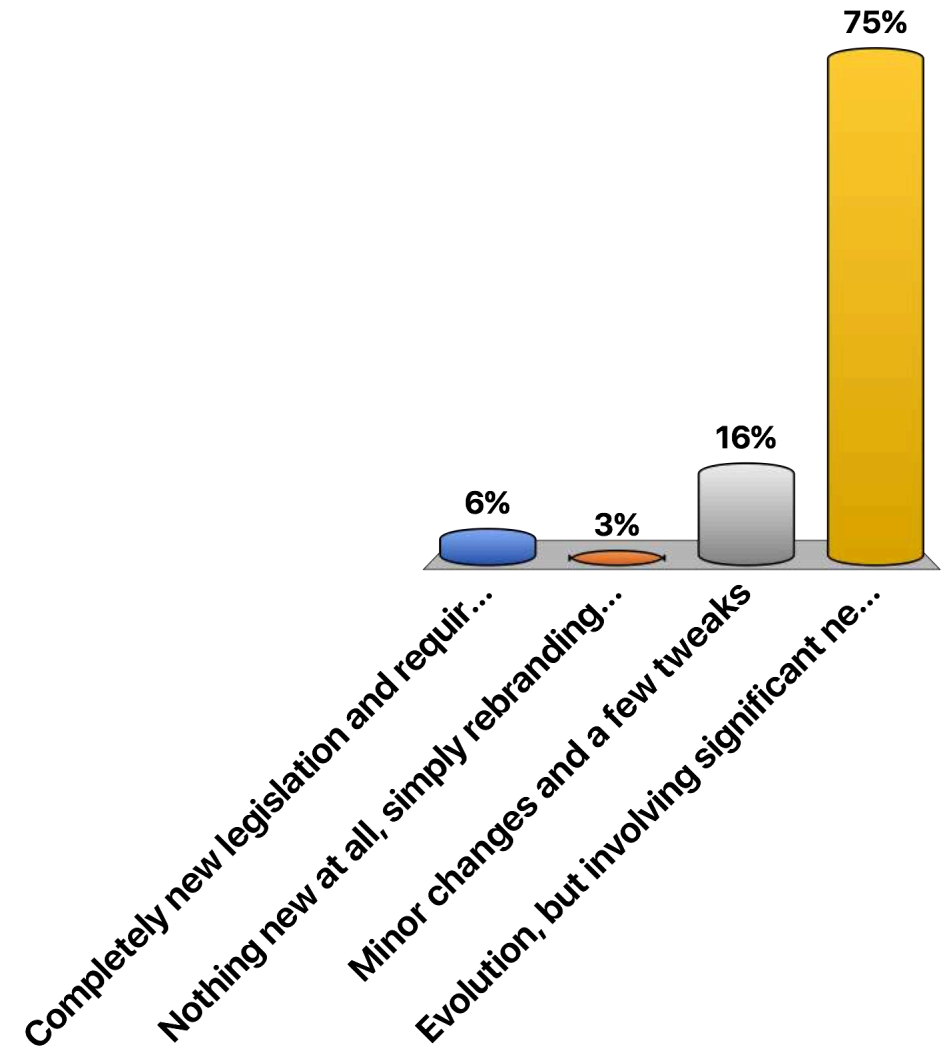
- A. The role of the Data Protection Officer (DPO)
- B. Understanding the lawful basis for processing personal data
- C. Legitimate Interests
- D. Consent
- E. Research activities
- F. Fees
- G. Subject Access Requests
- H. Data and Information Security
- I. Information Audits and Asset Registers
- J. Privacy Notices



After the break...
understanding what's
new and not new about
the GDPR and the role of
the DPO

The GDPR is...?

- A. Completely new legislation and requirements
- B. Nothing new at all, simply rebranding of existing law
- C. Minor changes and a few tweaks
- ✓ D. Evolution, but involving significant new requirements



GDPR– what the ICO says

“The General Data Protection Regulation (GDPR) is a **new, Europe-wide law that replaces the Data Protection Act 1998** in the UK. It is part of the wider package of reform to the data protection landscape. The GDPR sets out requirements for how organisations will need to handle personal data from 25 May 2018.”



GDPR– what the ICO says

“The GDPR applies to **‘personal data’**, which means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. There are **additional rules** in the GDPR for organisations processing **special category data**. This includes information about an individual’s health.”



GDPR– what the ICO says

“Not completely new, but there are **some** new requirements.

- There is a new requirement on all public authorities (including GP Practices) to **appoint a Data Protection Officer** and register the DPO with the Information Commissioner.



GDPR– what the ICO says

“The requirement to have a **lawful basis** in order to process personal data is not new. It replaces and mirrors the previous requirement to satisfy one of the ‘conditions for processing’ under the Data Protection Act 1998. However, the GDPR places **more emphasis on being accountable** for and **transparent** about your lawful basis for processing.”



GDPR– what the ICO says

“You need to identify both a **lawful basis** for processing and a **special category condition** for processing. You should document both your lawful basis for processing and your special category condition so that you can demonstrate compliance and accountability.”



GDPR– what the ICO says

“The GDPR also removes the right to charge a **fee for subject access requests** in most cases. In future, where a request is manifestly unfounded or excessive you may charge a “reasonable fee” for the administrative costs of complying with the request. You can also charge a reasonable fee if an individual requests further copies of their data following a request.”



GDPR– what the ICO says

“One of the biggest changes introduced by the GDPR is around accountability – a new data protection principle that says organisations are responsible for, and must be able to demonstrate, compliance with the other principles. Although these obligations were implicit in the Data Protection Act 1998 (1998 Act), the GDPR makes them explicit.”



GDPR– what the ICO says

“Documentation is a new requirement under the GDPR. It is mainly about keeping internal records of your processing activities. It reflects the increased importance of accountability and your obligation to ensure (and demonstrate) that what you do with people’s personal data is in line with the GDPR.”



GDPR– what the ICO says

“Good practice tools that the ICO has championed for a long time, such as **privacy impact assessments** and privacy by design, are now formally recognised and legally required in some circumstances.”



GDPR– what the ICO says

“The GDPR makes written contracts between controllers and processors **a general requirement**, rather than just a way of demonstrating compliance with the seventh data protection principle (appropriate security measures) under the DPA. These contracts **must now include certain specific terms**, as a minimum.”



GDPR and Health— what the ICO says

“If you are a public authority as defined under the Freedom of Information Act 2000, or Freedom of Information (Scotland) Act 2002, as many GP practices, dental practices, other health practitioners and pharmacies that carry out NHS work are, you are a public authority for the purposes of the GDPR.”



The common sense view

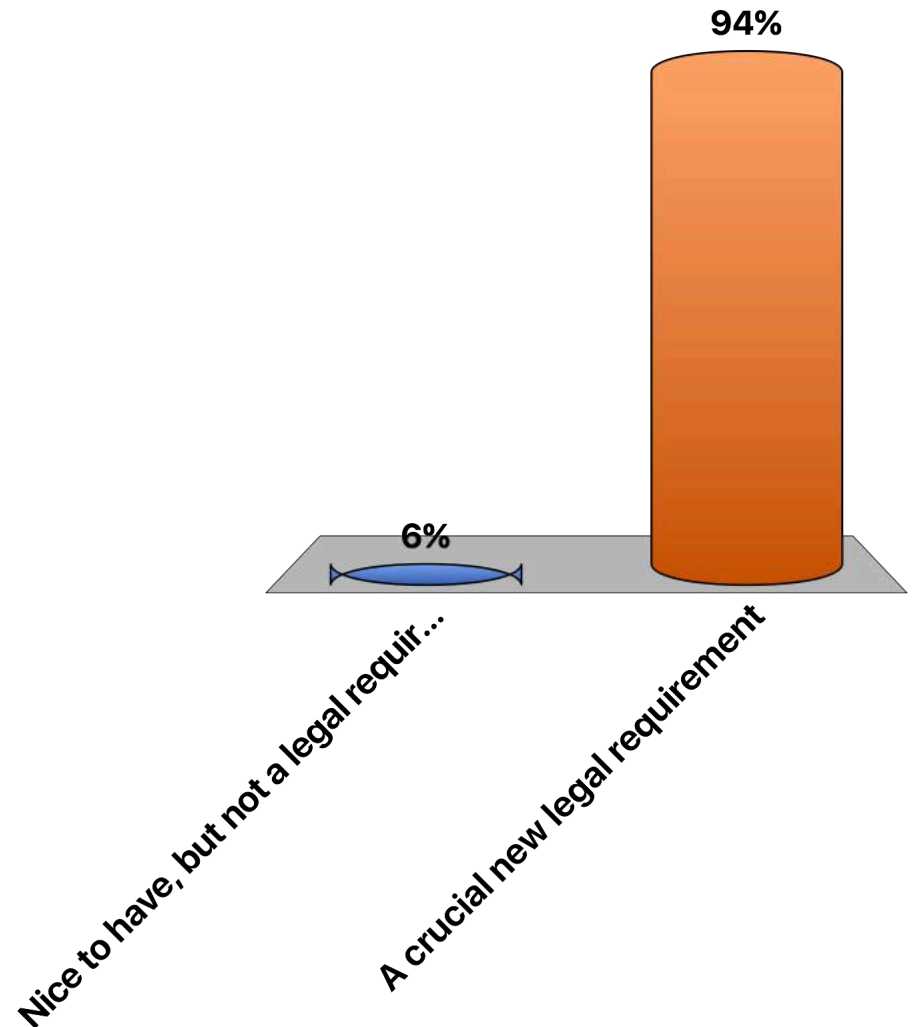
- You need to understand but not be afraid of the main new legal requirements
 - DPO
 - Confirm lawful basis and special category for processing data
 - Demonstrate and document accountability and processes
 - Avoid fees in most cases
 - Contracts with sub-processors



The DPO is...?

A. Nice to have, but not a legal requirement

✓ B. A crucial new legal requirement

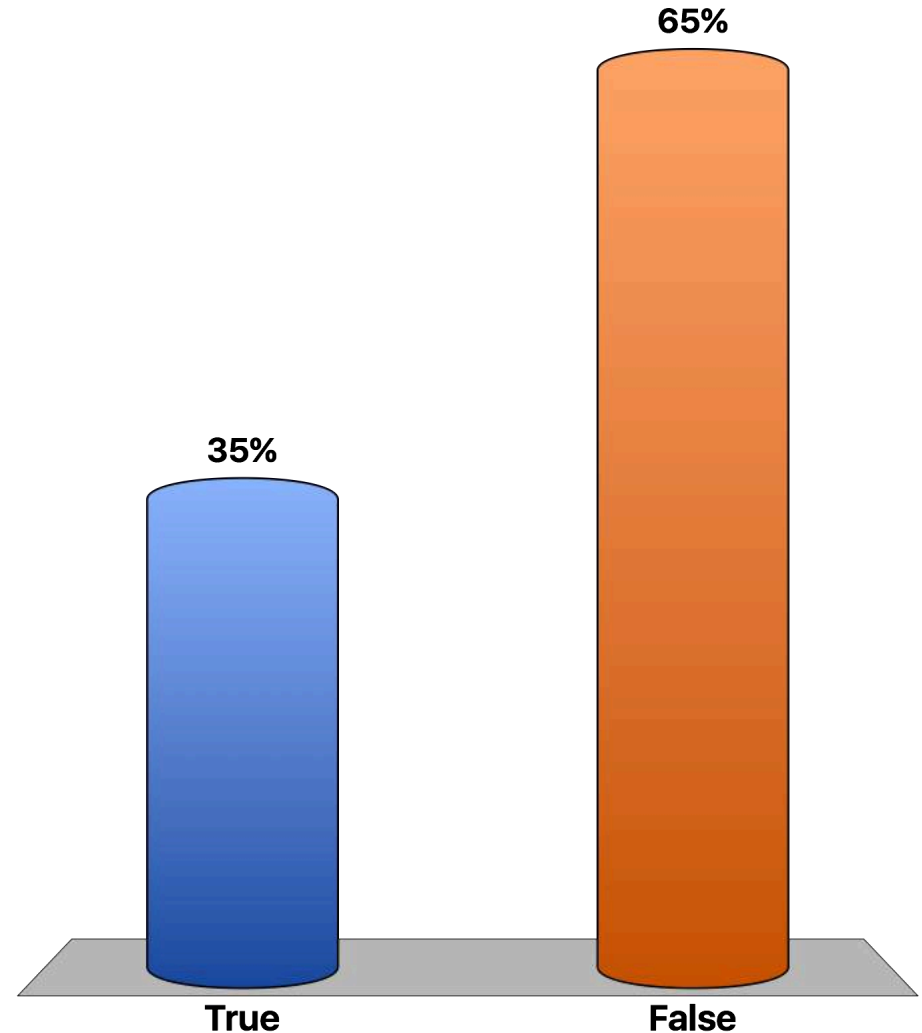


Single answer

The DPO can be the same person who handles our data requests and management

A. True

✓ B. False



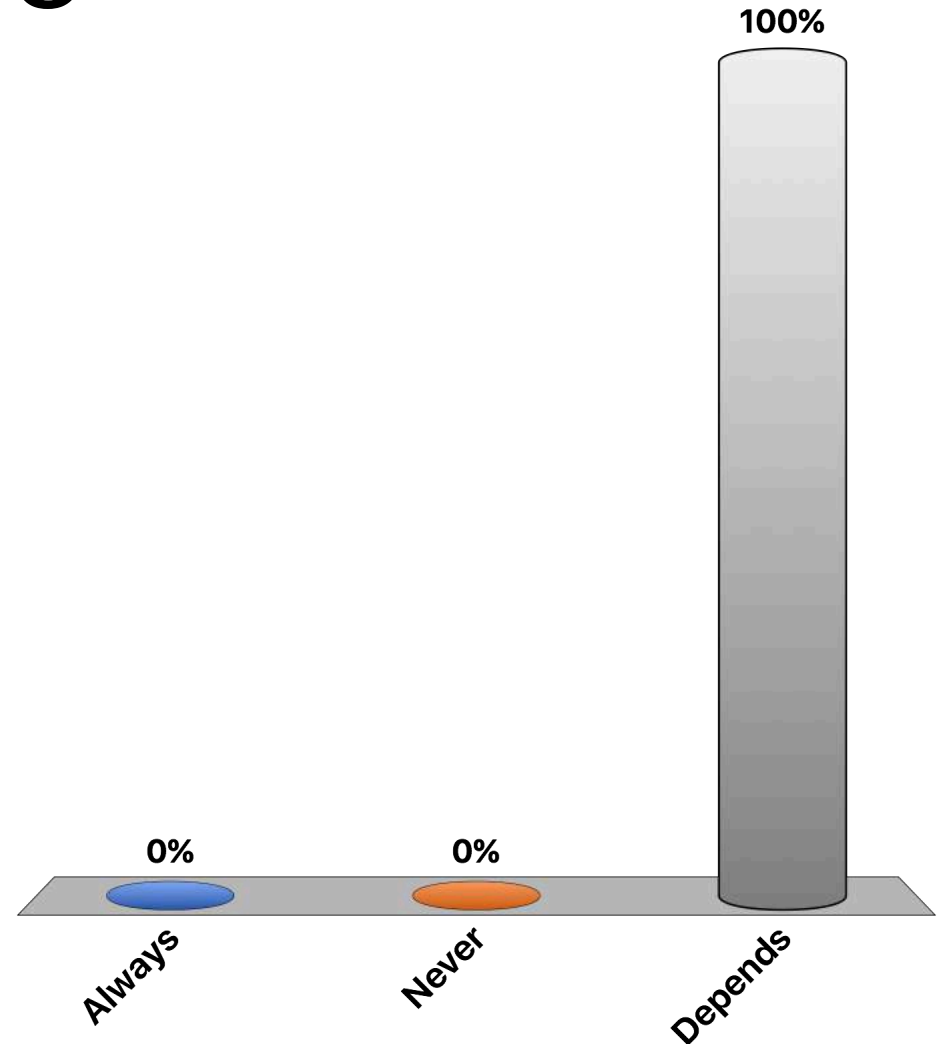
Single answer

Our Practice Manager can also be our DPO

A. Always

B. Never

✓ C. Depends

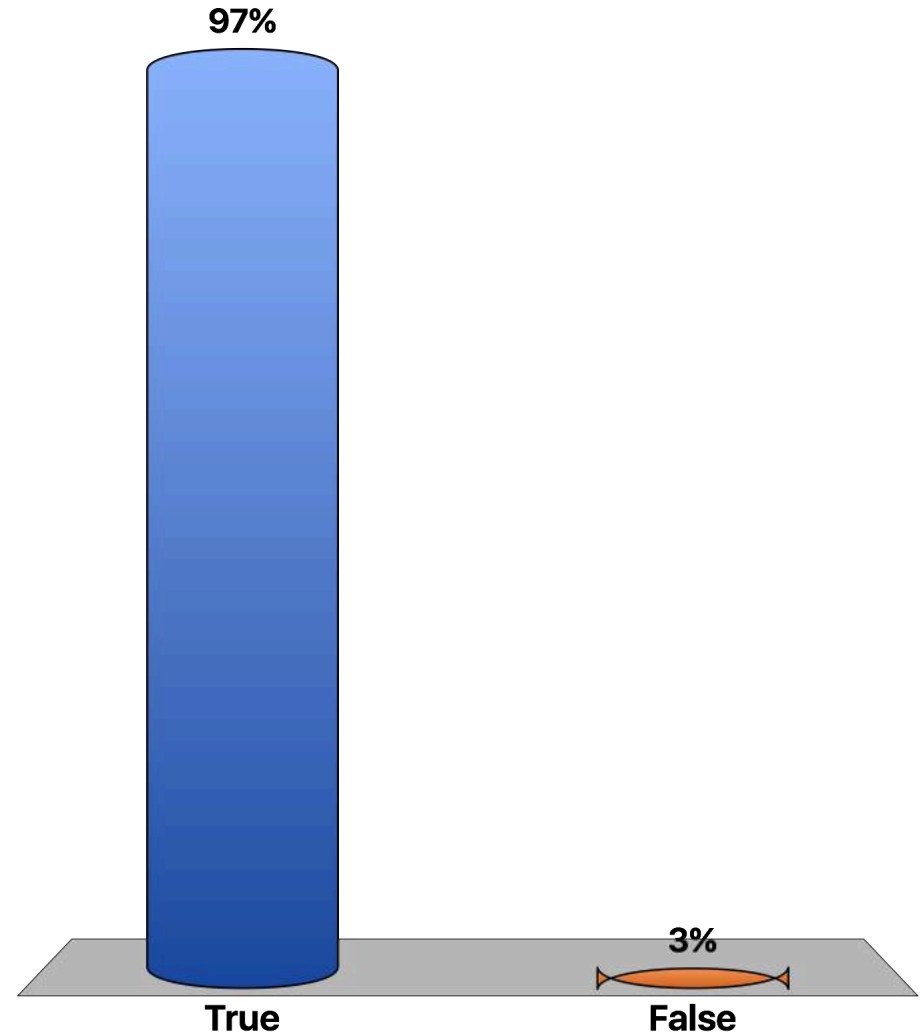


Single answer

We can share a DPO with other organisations...

ELR GP
Federation

- ✓ A. True
- B. False



DPO– what the ICO says

“Any and all public bodies are required by law to appoint a DPO”



DPO– what the ICO says

The person you appoint as a DPO can be an existing employee **provided that their professional duties are compatible with the duties of the DPO and do not lead to a conflict of interest.**

- In this context, ‘conflict of interest’ means a conflict with other possible tasks and duties. The DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data.
- The EU guidance on this area states:
- *“As a rule of thumb, conflicting positions may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing.”*



DPO– what the ICO says

“You may appoint a single data protection officer to act for a group of public authorities or bodies (e.g. GP Practices) taking into account their organisational structure and size.”



DPO– what the ICO says

“A DPO should have experience and expert knowledge of data protection law, proportionate to the type of processing you carry out, taking into consideration the level of protection the personal data requires. It would be an advantage for a DPO to also have a good knowledge of its industry or sector, as well as its data protection needs and processing activities.”



DPO– what the ICO says

The DPO's tasks are defined in Article 39 of GDPR as:

- to **inform and advise** you and your employees **about your obligations** to comply with the GDPR and other data protection laws;
- to **monitor compliance** with the GDPR and other data protection laws, and with your data protection policies, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- to **advise on, and to monitor**, data protection impact assessments;
- to cooperate with **the supervisory authority**; and
- to be the **first point of contact** for supervisory authorities and for individuals whose data is processed (employees, customers etc).



DPO— what the ICO and EU says

“As part of these duties to monitor compliance, DPOs may, in particular:

- *collect information to identify processing activities,*
- *analyse and check the compliance of processing activities, and*
- *inform, advise and issue recommendations to the controller or the processor.”*



DPO– what the EU says

- “The EU guidance on the responsibilities of data controllers (i.e. GP Practices) in protecting the independence of the DPO are clear. They state:
- *“Several safeguards exist in order to enable the DPO to act in an independent manner as stated in recital 97:*
- *No instructions by the controllers or the processors regarding the exercise of the DPO’s tasks*
- *No dismissal or penalty by the controller for the performance of the DPO’s tasks*
- *No conflict of interest with possible other tasks and duties.”*



DPO– what the ICO and EU says

- “The DPO isn’t personally liable for data protection compliance. As the controller or processor it remains your responsibility to comply with the GDPR.”
- The DPO role is to advise data controllers and processors on what they need to do, and to provide independent external assurance, not to carry out the activities themselves.”
- The EU guidance on this area is equally clear:
- *“DPOs are not personally responsible for non-compliance with the GDPR. The GDPR makes it clear that it is the controller or the processor who is required to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation’ (Article 24(1)). Data protection compliance is the responsibility of the controller or the processor.”*
-



The common sense view

You need to appoint a DPO based upon:

- Their independence from your data and information management processes
- Their knowledge of the work you do AND of data and information governance
- The most efficient and effective use of your resources (e.g sharing where sensible)



The common sense view

You need to ensure

- the DPO is independent
- the DPO has direct access to your senior management if necessary (e.g. Practice Partners)
- You understand it is YOU not the DPO who is liable for compliance



The common sense view

The DPO role is very similar to an auditor:

- Advises and assures, rather than carries out the work
- Cannot have a conflict of interest
- Independent, experienced and informed



After the break... some
of the crucial aspects
of GDPR in detail

Time to delve into the detail

- A high level summary, not a thesis
- Checking your understanding of the key points through Q&A rather than a lecture



Lawful Basis for Processing

A foundation for your GDPR compliance is to be clear about **the lawful basis** on which you rely for processing personal data. Under the GDPR the data controller is the organisation that 'determines the purposes and means of the processing of personal data'.



Lawful Basis for Processing

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

- **(a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- **(b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- **(c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- **(d) Vital interests:** the processing is necessary to protect someone's life.
- **(e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- **(f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)



Lawful Bases for Processing

The primary lawful basis for processing special category health data for direct care is that processing is: *'necessary... in the exercise of official authority vested in the controller'* (Article 6(1)(e))

It is also possible for NHS GP practices to rely on 'processing is necessary for compliance with a legal obligation to which the controller is subject' (Article 6(1)(c))

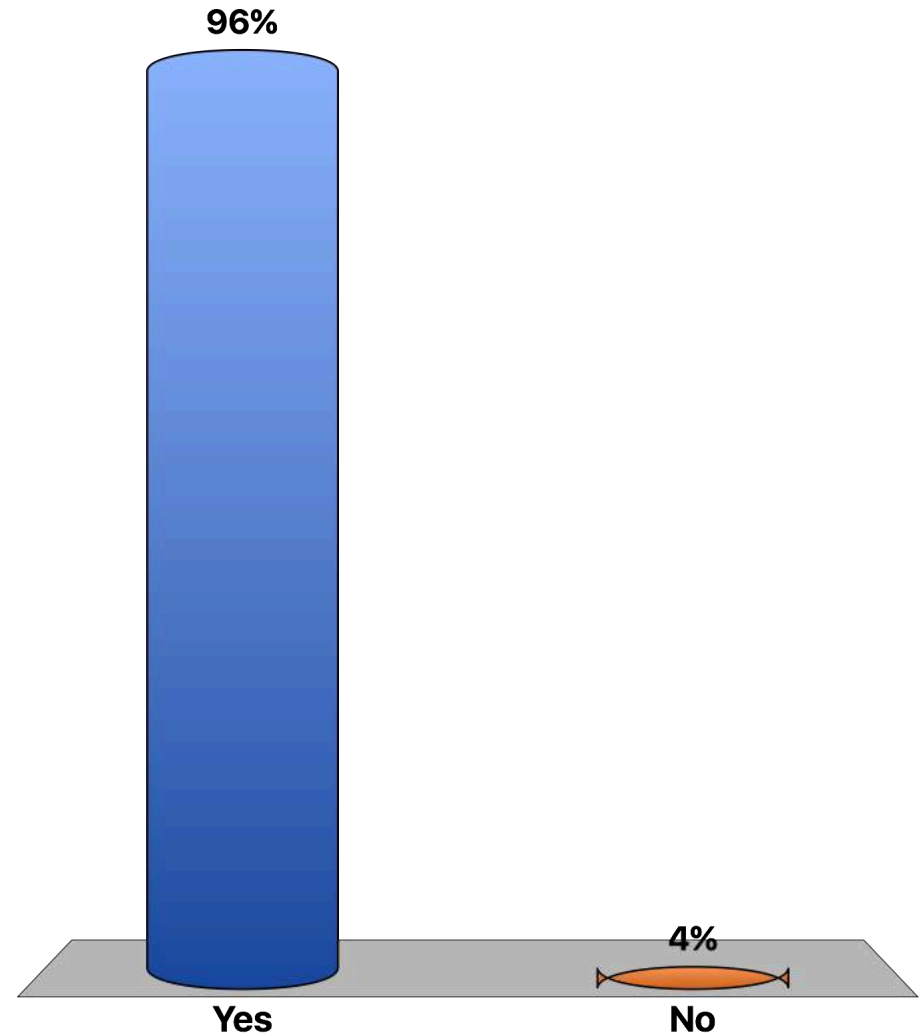
The special category condition for processing for direct care is that processing is: *'necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services...'* (Article 9(2)(h)).

When relying on Articles 6(1)(e) and 9(2)(h) to share data for the provision of direct care, consent under GDPR is not needed.



Is your Practice responsible for
medical diagnosis, the
provision of health or social
care or treatment or the
management of health or social
care systems and services
under contract to the NHS

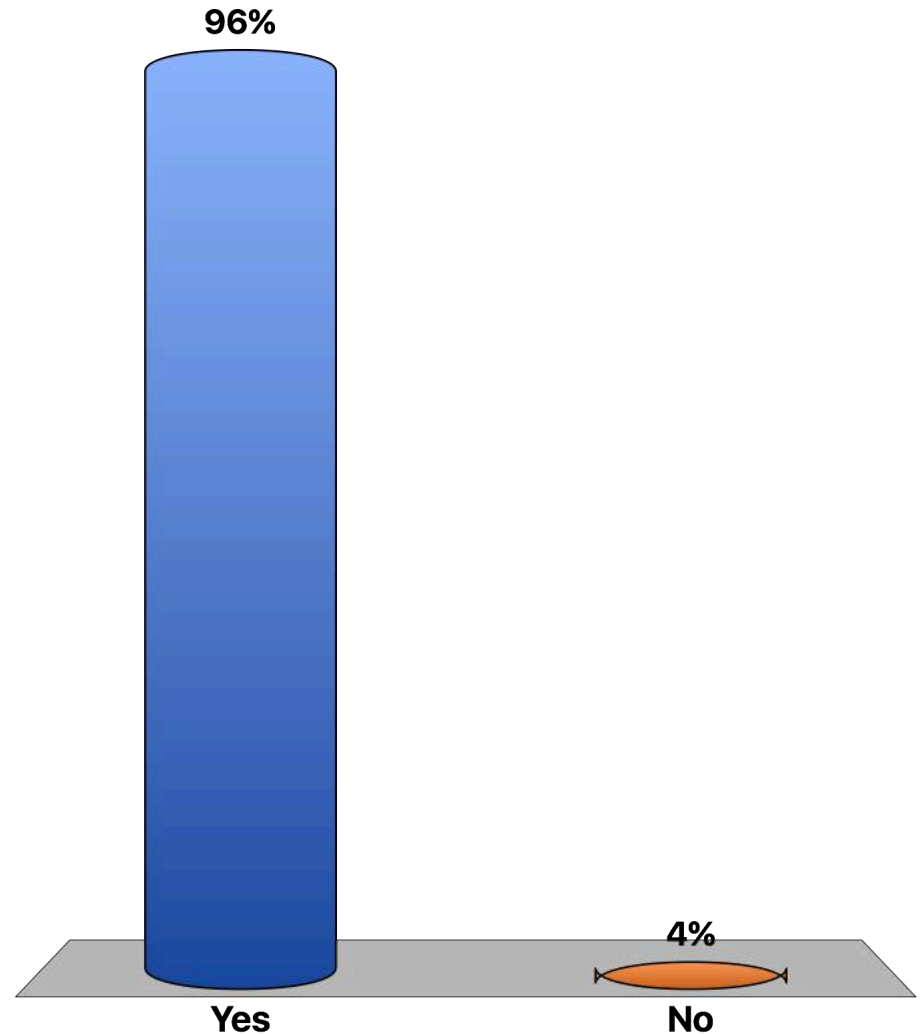
- ✓ A. Yes
- B. No



Single answer

Are you clear that this
can be the primary
lawful basis for which
you process personal
data for the purposes
of GDPR?

- ✓ A. Yes
- B. No



Lawful Bases for Processing

Where there is a legal requirement to disclose, for example, a direction under the Health and Social Care Act 2012 or disclosures under public health legislation, the lawful basis for processing would be: ‘... for compliance with a legal obligation...’ (Article 6(1)(c)).

In the majority of cases, the most appropriate special category condition for processing in the face of a legal requirement to disclose will remain as: ‘...for the purpose of preventative...medicine...the provision of health or social care or treatment or the management of health or social care systems and services...’ (Article 9(2)(h)).



Lawful Bases for Processing

When processing data for medical research the Article 6 lawful basis is 6(1)(e) ‘... for the performance of a task in the public interest...’



The special category condition is Article 9(2)(j) ‘...research purposes...’.

Legitimate Interest

- Legitimate interests is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate. It is likely to be most appropriate if you use people's data in ways they would reasonably expect and which have a minimal privacy impact; or there is a compelling justification for the processing.
- The GDPR specifically mentions use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests, but this is not an exhaustive list. It also says that you have a legitimate interest in disclosing information about possible criminal acts or security threats to the authorities.
- If you want to rely on legitimate interests, you can use the three-part test, or a legitimate interests assessment (LIA), to assess whether it applies.



Legitimate Interest Assessment

- **Firstly, identify the legitimate interest(s)**
- **Secondly, apply the necessity test. Consider:**
 - Does this processing actually help to further that interest?
 - Is it a reasonable way to go about it?
 - Is there another less intrusive way to achieve the same result?
- **Thirdly, do a balancing test. Consider the impact of your processing and whether this overrides the interest you have identified.**



Explicit Consent

- For purposes other than the provision of direct care or the additional lawful bases set out on the previous page, your practice may choose to rely on explicit consent as the lawful basis for processing personal data.
- If this is the case, the GDPR sets out certain requirements in order for consent to be valid: *consent must be 'freely given, specific, informed and an unambiguous indication of the data subject's agreement'*.
- If explicit consent does not meet these four criteria it will almost certainly be invalid for the purpose of the GDPR.



Vital Interest

You may be required to process data to protect the vital interests of an individual. Your practice should clearly document the circumstances where it will be relevant and inform individuals where necessary.

This lawful basis is very limited in its scope, and generally only applies to matters of life and death.

It is likely to be particularly relevant for emergency medical care, when you need to process personal data for medical purposes but the individual is incapable of giving consent to the processing.

It is unlikely to be appropriate for medical care that is planned in advance or for processing on a larger scale.



Single answer

Are you clear about the additional
lawful bases you can rely upon?

Consent

Contract

Legal obligation

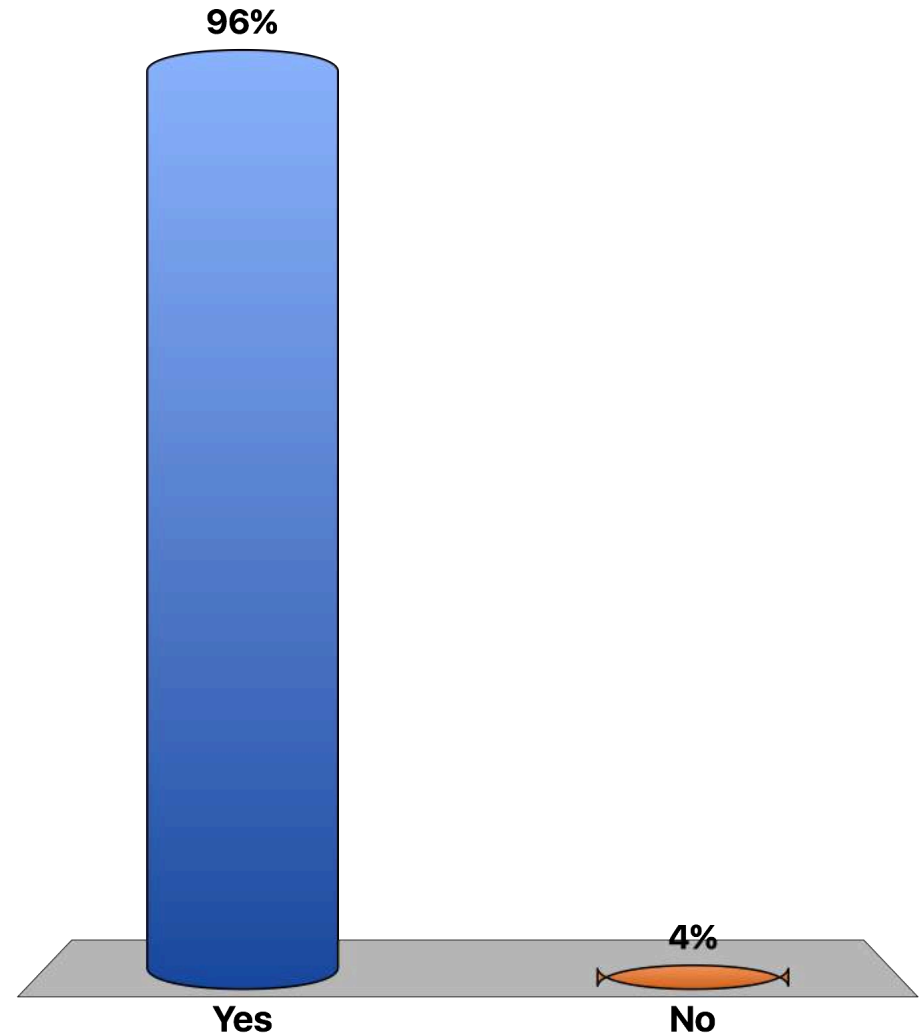
Vital interests

Public task

Legitimate interests:

A. Yes

B. No



The common sense view

The primary legal basis on which you can rely for processing data under GDPR is likely to be the provision of health or social care or treatment or the management of health or social care systems and services under contract to the NHS



The common sense view

It is a complete red herring to believe that the GDPR imposes radical new requirements on you to obtain explicit consent from patients in every single way you process their data.



Individuals' Rights

Under GDPR, there are a number of rights for individuals in relation to processing their personal data. These include

- Right to be informed including privacy information
- Right of access
- Right to rectification and data quality
- Right to erasure including retention and disposal
- Right to restrict processing
- Right to object



Right to be informed

Individuals need to know that you are collecting their data, why you are processing it and who you are sharing it with.

- You should publish this privacy information in a Privacy Notice displayed in your practice, on your website and within any forms or letters you send to individuals.
- The information must be:
 - concise, transparent, intelligible and easily accessible
 - written in clear and plain language, particularly if addressed to a child; and
 - free of charge.



Right of access

- The right of access is also known as Subject Access Rights
- Individuals have the right to obtain:
 - confirmation that you are processing their data;
 - access to their personal data; and
 - other supplementary information – this largely corresponds to the information that you should provide in a privacy notice.
- Individuals can request information verbally or in writing. You must provide a copy of the information free of charge.
- However, you can charge a ‘reasonable fee’ when a request is:
 - manifestly unfounded or excessive, particularly if it is repetitive, unless you refuse to respond; or
 - for further copies of the same information (that’s previously been provided).



Right to rectification and data quality

- Individuals have the right to have personal data rectified if it is inaccurate or completed if it is incomplete.
- An individual can make a request for rectification verbally or in writing.
- You should respond to a request without delay and at least within one month of receipt.
- You should calculate the time limit from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.



Right to erasure including retention and disposal

- Individuals have the right to be forgotten and can request the erasure of personal data when:
 - it is **no longer necessary for the purpose you originally collected/ processed it** for;
 - the individual withdraws consent;
 - you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing
- here is no absolute 'right to be forgotten'.
- People can ask for their personal data to be erased – but only when there is no compelling reason for its continued processing.
- There is no absolute 'right to be forgotten'.
- Care providers will likely have a very good reason for processing much of the personal data they hold for the purposes of providing medical care.



Right to restrict processing

- Individuals have a right to block or restrict the processing of their personal data.
- Individuals can make a request verbally or in writing. You must verify the identity of the person making the request, using “reasonable means”.
- You should respond to a request without delay and at least within one month of receipt.
- If you consider the request, but **conclude that you do have a lawful basis or legitimate interest in continuing to processing the data**, you should inform the individual of the outcome of this conclusion and advise them that they have the right to consult the Information Commissioner if they disagree with your conclusion.



Right to object

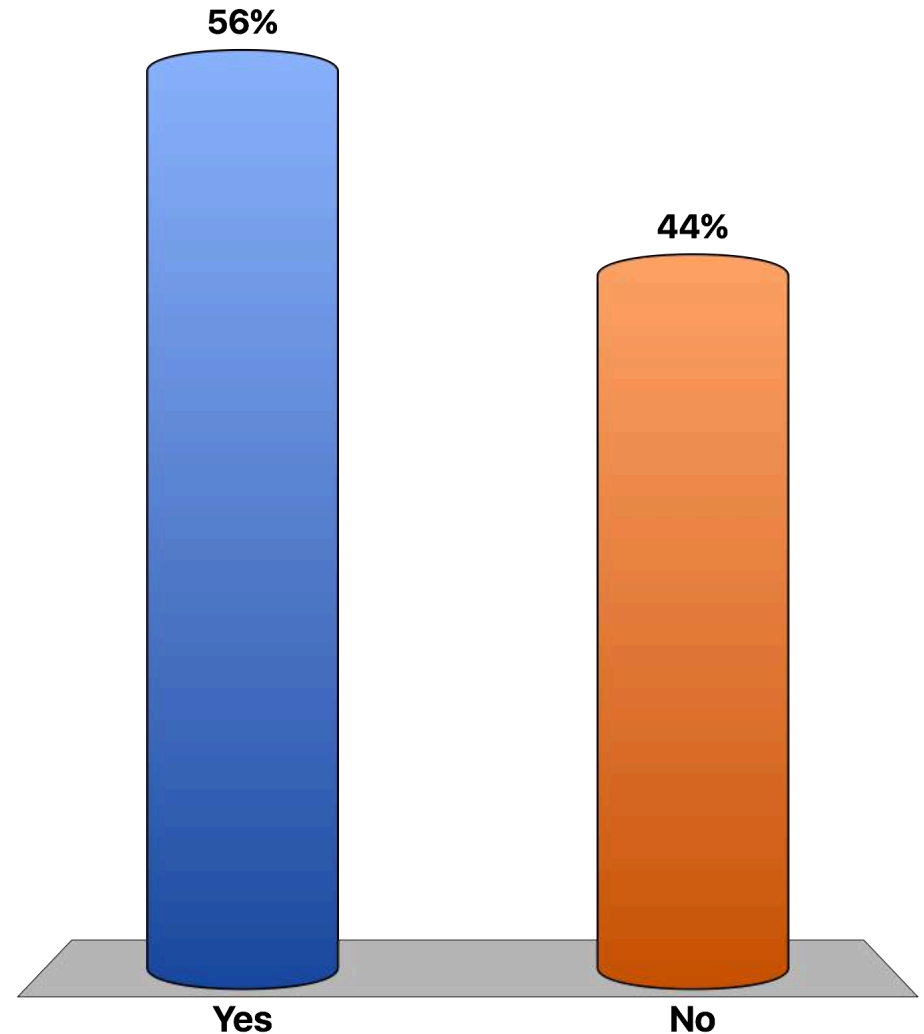
- The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.
- Individuals have an absolute right to stop their data being used for direct marketing.
- In other cases where the right to object applies you may be able to continue processing if you can show that you have a compelling reason for doing so.
- There is no absolute 'right to be forgotten'.
- Requests will have to be assessed on their own merits. However, care providers, for example, will likely have a very good reason for processing much of the personal data they hold for the purposes of providing medical care.



Are you clear about the
range of Individuals'
Rights under GDPR?

A. Yes

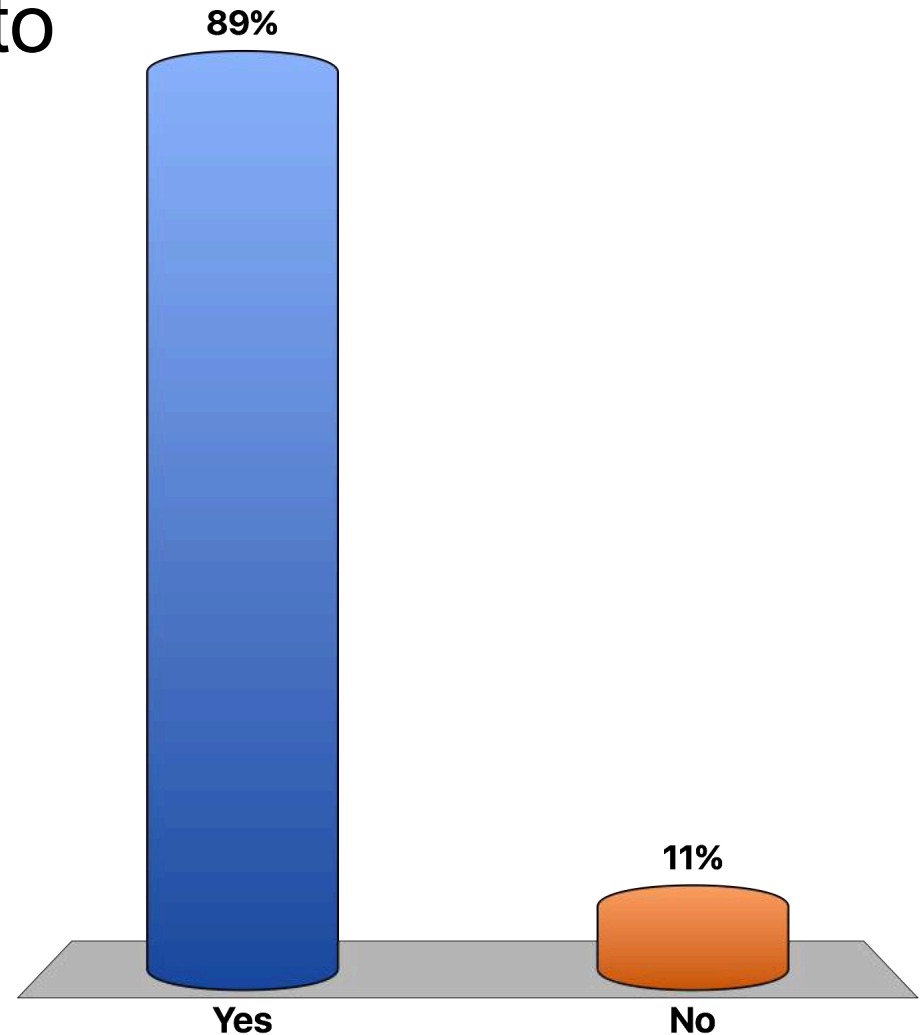
B. No



Are you clear about your OWN rights under GDPR to continue to process personal data if it is necessary for you to fulfil your contractual duties to the NHS and protect legitimate interests?

A. Yes

B. No



The common sense view

The rights to be informed and rights of access are something that can be easily covered by your Privacy Notices

You should be prepared in most cases to waive a SAR fee

Many individuals rights are overridden for GP practices by your continuing need to process data to carry out your contractual duties to the NHS and public interest in providing healthcare



Documentation

- **Documentation is a new requirement** under the GDPR. It is mainly about keeping internal records of your processing activities. It reflects the increased importance of accountability and your obligation to ensure (and demonstrate) that what you do with people's personal data is in line with the GDPR."



Documentation

- **Don't Panic!**
- Most of what you need to do can be completed through two main and related activities
 - Information Audit; the results of which are captured in...
 - Information Asset Register



Information Audit

The Information Commissioner's Officer recommend that a good way to start is by doing an information audit or data-mapping exercise to clarify what personal data your organisation holds and where.

It is important that people across your organisation are engaged in the process; this can help ensure nothing is missed when mapping the data your organisation processes.

It is equally important to obtain senior management buy-in so that your documentation exercise is supported and well resourced.



Information Audit – 3 step process

- **Devise a questionnaire** – you can distribute this to the areas of the organisation you have identified as processing personal data. Use straightforward (jargon-free) questions that will prompt answers to the areas requiring documentation.
- **Meet directly with key business functions** – this will help you gain a better understanding of how certain parts of your organisation use data.
- **Locate and review policies, procedures, contracts and agreements** – as well as feeding directly into the documentation exercise, this can help you compare and contrast intended and actual data processing activities.



Information Asset Register

When carrying out your Information Audit, bear in mind the core requirements from ICO in terms of what should be captured in an Information Asset Register.



Information Asset Register

The IAR must contain:

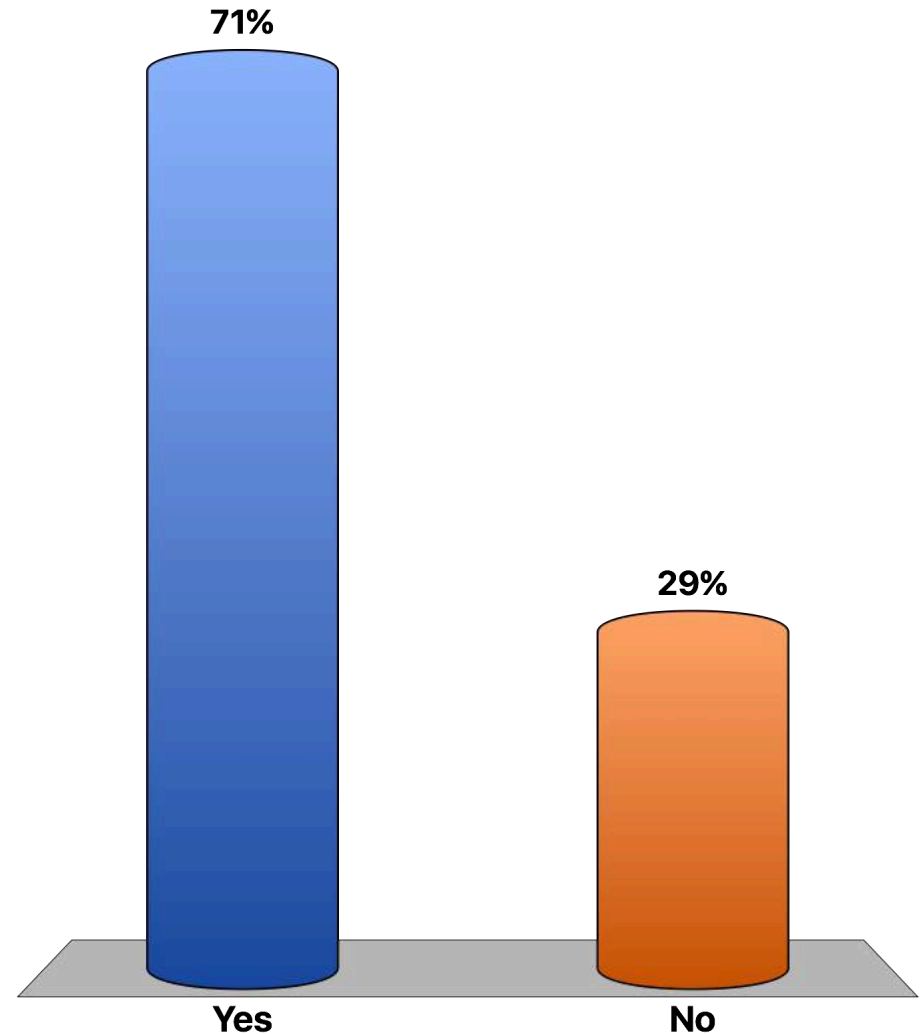
- The name and contact details of any joint controllers
- The purposes of the processing
- The categories of individuals – the different types of people whose personal data is processed, e.g. employees, customers, members.
- The categories of personal data you process
- The categories of recipients of personal data
- The name of any third countries or international organisations that you transfer personal data to – any country or organisation outside the EU.
- If possible, the retention schedules for the different categories of personal data – how long you will keep the data for.
- A general description of your technical and organisational security measures – your safeguards for protecting personal data, e.g. encryption, access controls, training.



Are you clear about how to go about carrying out an Information Audit and Information Asset Register?

A. Yes

B. No



The common sense view

Of all of the areas of GDPR where GP Practices should be more prepared than others, it is for Information Audits and IARs – as this is at the core of much you have done for years for NHS IG compliance.

Make sure you only carry additional tasks and audits if you have first checked that you have not already captured this for IG purposes.



Processor contracts

“The GDPR makes written contracts between controllers and processors a **general requirement**, rather than just a way of demonstrating compliance with the seventh data protection principle (appropriate security measures) under the DPA. These contracts **must now include certain specific terms**, as a minimum.”



Processor contracts

“Contracts must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the controller.”



Processor contracts

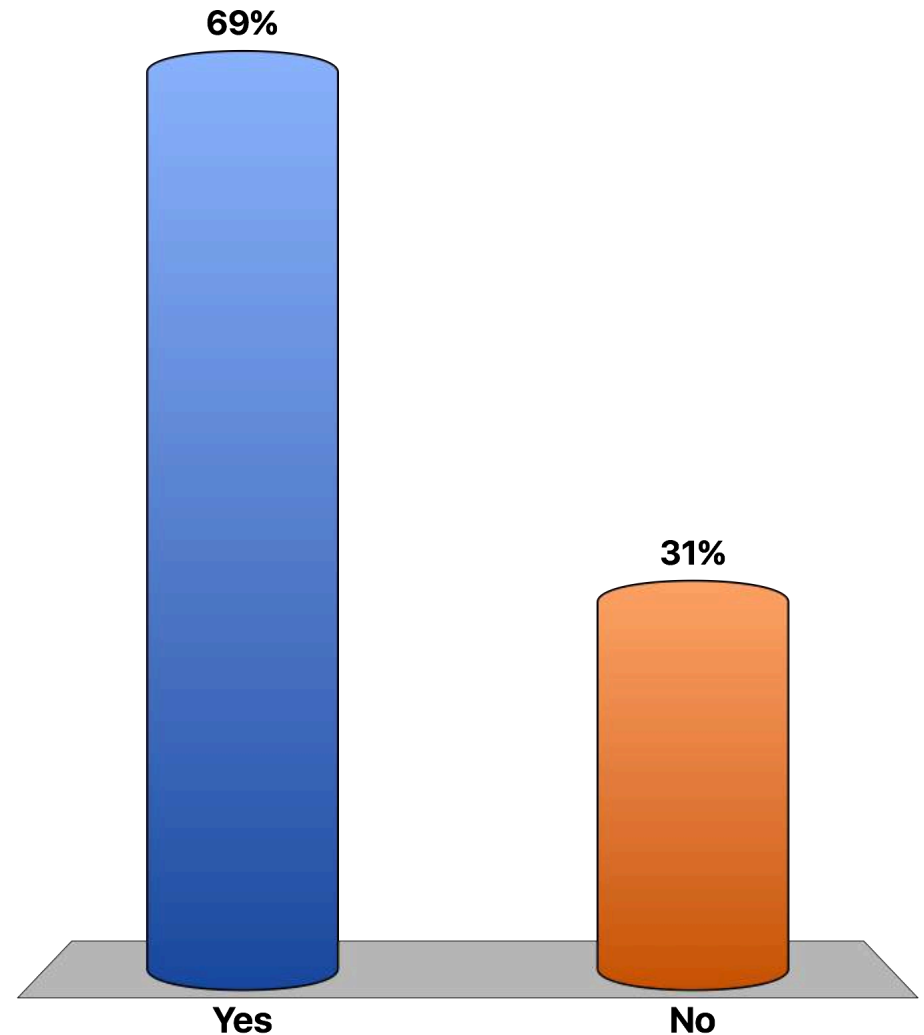
- “Contracts must also include as a minimum the following terms, requiring the processor to:
- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.



Are you clear about what is needed for contracts with sub-processors of data?

A. Yes

B. No



The common sense view

The DPO cannot and should not be asked to draw up or advise on specific contracts.

The DPO can point you to the advice from the ICO in this regard

You wouldn't draw up a legal contract in other areas without professional legal advice and support – GDPR is no different



After the break... life
as a DPO and YOUR
views to the ICO

Life as a DPO – avoiding the banana skins

- The GDPR is new legislation and emerging practice
- Even though the ICO has made VERY clear it is not in the game of hunting down and punishment, there has been plenty of ‘doom and gloom’ mongers inaccurately predicting Armageddon
- The role of the DPO is to provide Assurance and RE-Assurance



Life as a DPO – avoiding the banana skins

- However, you should make very clear at the outset, that the DPO
 1. Is NOT liable for compliance, that remains with the practice
 2. Can NOT carry out the necessary work for practices, but is there to ASSURE the work and ADVISE on any gaps in compliance



Life as a DPO – avoiding the banana skins

Sometimes you will be asked for information on things that have nothing to do with GDPR per se, but are actually about NHS Information Governance.

In these cases, it is NOT the role of the DPO to give detailed wider IT or Information Management advice or support.



Life as a DPO – avoiding the banana skins

Sometimes you will be asked to effectively give a “ruling” on things that are still the subject of debate within the ICO or between the ICO and doctors’ leaders.

If something is not clear, you need to explain to our organisation that it is not yet clear

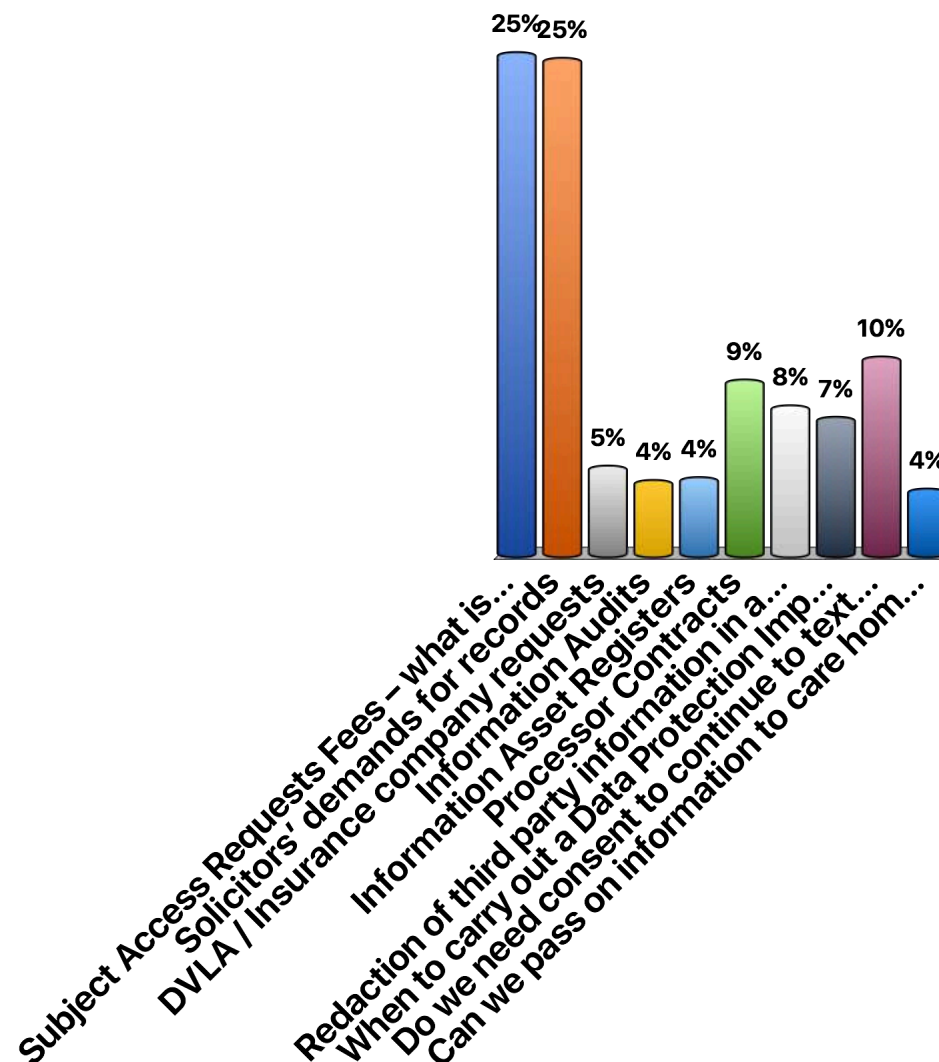
A classic at the moment is “when is a SAR excessive” – particularly in relation to requests from solicitors on behalf of patients



Up to 3 answers

Which of THESE issues resonates most with you?

- A. Subject Access Requests Fees – what is excessive?
- B. Solicitors' demands for records
- C. DVLA / Insurance company requests
- D. Information Audits
- E. Information Asset Registers
- F. Processor Contracts
- G. Redaction of third party information in a patient record
- H. When to carry out a Data Protection Impact Assessment
- I. Do we need consent to continue to text message patients?
- J. Can we pass on information to care home staff?



Missed anything?

- We will capture the outputs and lessons learned from today's session
- We will publish them in a "Learning Lessons" Report and submit it to NHS England, CCGs AND importantly the ICO
- Is there any burning issue or question you would like us to include in our Report?



And finally...



Data Protection Officer Service

Data Protection Officer Service

- Registered with ICO by 27 out of 31 practices in ELR
- Experience and expert knowledge of data protection law, proportionate to the type of processing you carry out
- Detailed knowledge of GP practices, as well as their data protection needs and processing activities



Data Protection Officer Service

Available to any GP Practice or other organisation outside East Leicestershire and Rutland looking for expert advice and support via a cost-effective DPO Service

Data Protection Officer Service

- Self-assessment toolkit covering everything we have covered today

GDPR Self-Assessment

Step 2 of 20

10%

Welcome to the GDPR self-assessment toolkit

This self-assessment toolkit is part of the ELR GP Federation GDPR DPO Service. It should take you no more than 1 hour to complete. The self-assessment toolkit covers:

Data Protection Officer (DPO)	Lawful basis for processing personal data	Consent
Vital interests	Research activities	Data Protection Fee and DPO Registration
Right to be informed including privacy information	Right of access	Right to restrict processing
Right to rectification and data quality	Right to erasure including retention and disposal	Right to restrict processing
Right to object	Information Audit	Information Asset Register
Privacy Notice	Accountability	Processor contract
Information risks	Data Protection Impact Assessments (DPIA)	Security policy
Breach notification		

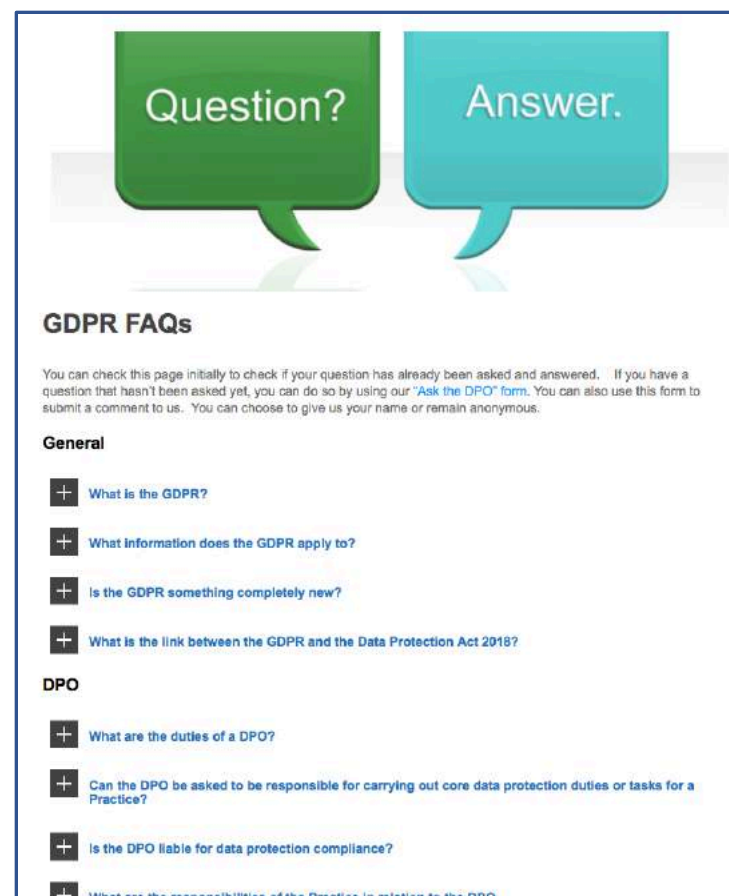
Data Protection Officer Service

- High quality Individual Practice Data Protection Officer Review to demonstrate compliance and advise on next steps



Data Protection Officer Service

- Members' Only access to comprehensive GDPR FAQs – over 100 and counting
- Constantly updated, including answers to Practice enquiries



Data Protection Officer Service

- “Ask the DPO” form, for any questions or queries not covered by the FAQs



Ask the DPO

You can check our [GDPR FAQs page](#) initially to check if your question has already been asked and answered. If it hasn't been asked yet, you can do so by using our “Ask the DPO” form below. You can also use this form to submit a comment to us. You can choose to give us your name or remain anonymous.

Data Protection Officer Service



For further information:
dpo@elrgpfed.com

What we said we'd do today...

- Get a common sense, no jargon understanding of GDPR
- Confirm what's new, what's not
- Understand where YOU are, what YOU think and what you NEED
- Understand the role of the DPO – what it is, what it isn't
- Look at key elements of GDPR compliance – in particular for GP Practices
- Discuss and debate the priority areas needing clarity and support



Beginner's Guide to being a Data Protection Officer

*"or... everything you always wanted to know
about being a DPO, but were afraid to ask..."*

Joe McCrea