The General Data Protection Regulation (GDPR)

and the Data Protection Bill

Contents

Matt Howgate

Matthew is a non-practising solicitor and was formerly Senior Legal Adviser and Head of Continuous Improvement at the Legal Services Commission (he predecessor body to the Legal Aid Agency). He was also Legal Standards Principal at the Co-operative Legal Services.

Since 2008, he has been providing expert organisational development, compliance and strategy consultancy. He has particular expertise in SRA and BSB compliance issues, data protection (and GDPR) compliance and is recognised as a leading expert on the legal aid scheme (indeed he is a member of the managing committee at the Legal Aid Practitioner's Group).

He also has a significant experience in public sector commissioning, working with local authorities and those bidding for public sector contracts.

Matthew regularly works with law firms and advice agencies advising and training on regulatory compliance and data security.

Much of his work centres around helping organisations plan and implement structural change to achieve efficiency, profitability and improved compliance and risk management. He is an experienced practice manager and a lead trainer on LAPG's Certificate in Practice Management.

Matthew's clients say:

> "*Matt Howgate offered us invaluable support as we took our think tank through a major restructure. He was thoughtful, generous and amazingly insightful at every step of the way. It felt as if he instantly understood our values and purpose and he designed organisational solutions that helped us redesign fundamental aspects of our governance while also building as wide support from staff and trustees as possible. We couldn't have changed without him."* **Marc Stears: CEO, New Economics Foundation**
>
> *"Matthew's encyclopaedic knowledge of regulatory matters, coupled with a down to earth, pragmatic approach to communicating his advice, have made him indispensable to us. Whether for urgent reassurance or help considering next steps, we feel in very safe hands."* **Jenny Beck, Director at Beck Fitzgerald Solicitors**
>
> *"I cannot recommend Matt Howgate highly enough. Matt has an unparalleled breadth and depth of knowledge across the entire legal services sector. He has a quick grasp of the key challenges impacting organisations and he takes the time to understand the specific context affecting your area of business. Moreover, his strategic and operational expertise are second to none ensuring that he is a significant asset as a consultant."* **Kirsty Thomson: Partner / Director, JustRight Scotland**

David Gilmore

David has worked with a wide range of local and national organisations including The Law Society, the Welsh Assembly Government, the Ministry of Justice, the Legal Services Commission, Citizens Advice, Advice UK, the Home Office (Office of the Immigration Services Commissioner), the Legal Aid Practitioners Group, Central Law Training, the Law Centres Network, Comic Relief, Unbound Philanthropy, the Diana Princess of Wales Memorial Fund and the Baring Foundation.

He has also provided advice and assistance to hundreds of law firms and other legal organisations. He delivers specialist consultancy and training on a wide range of topics including business management and strategy, tendering, compliance and quality assurance. He has also undertaken feasibility studies and conducted surveys. He is an expert in relation to legal aid contracting and auditing and is also a Law Society accredited Lexcel consultant.

David is a writer for LexisNexis and a member of the Consulting Editorial Board for LexisPSL. David has also been responsible for the writing of a solicitors' accreditation scheme assessment on behalf of the Law Society and leading the assessment marking team for over fifteen years.

David also founded and regularly contributes to LegalVoice, a not-for-profit online magazine for legal professionals. Prior to establishing DG Legal, David worked for Abbey, Marks & Spencer and the Legal Services Commission in varying senior management roles.

In 2016 David was appointed as a Commissioner advising Lord Bach on policy relating to Justice and Legal Aid.

The General Data Protection Regulation

The General Data Protection Regulation (along with the Data Protection Bill) will largely replace the Data Protection Act 1998. Much of its content mirrors the existing Data Protection Act but some provisions and obligations are entirely new.

The Players

ICO

The Information Commissioner's Office – The ICO - is the UK's independent body set up to uphold information rights.

Elizabeth Denham

The Information Commissioner who heads the ICO.

WP29

The Article 29 Working Party (Art. 29 WP) is an advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. Its main stated missions are to:

- Provide expert advice to the States regarding data protection;
- Promote the consistent application of the Data Protection Directive in all EU state members, as well as Norway, Liechtenstein and Iceland;
- Give to the Commission an opinion on community laws (first pillar) affecting the right to protection of personal data; and
- Make recommendations to the public on matters relating to the protection of persons with regard to the processing of personal data and privacy in the European Community.

Some Definitions

Personal data

The GDPR applies to "personal data". This is any information relating to an identifiable living person who can be directly or indirectly identified from that data. It includes things like name, identification number, location data or online identifier (reflecting changes in technology and the way organisations collect information about people).

Sensitive Personal Data / Special Category Data

Under the Data Protection Act you will have become familiar with what was called "sensitive personal data".

The GDPR refers to sensitive personal data as "special categories of personal data". It includes information about the data subject's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

It also includes data about children and data relating to criminal convictions and offences.

Data Controller

This is the person or organisation primarily responsible for holding and processing the data – this means you!

Data Processor

This is any third party which processes data on the Data Controller's behalf and on their instructions.

Preparing for GDPR

Guidance

ICO

The ICO has produced some excellent guidance on preparing for GDPR. The full range of introductory guidance can be found on the ICO website at:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Some of this guidance in this document is taken directly from the ICO website as it is helpful to understand how the ICO is interpreting your obligations under GDPR.

The ICO has also produced a helpful guide called: 'Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now'.

That can be found at:

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Those 12 steps are:

1. You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2. 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.

3. You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

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

5. You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

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

7. 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.

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

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

10. You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11. 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.

12. If your organisation operates in more than one EU member state (i.e. you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

Law Society

The Law Society is also providing some guidance at:

http://www.lawsociety.org.uk/support-services/practice-management/gdpr-preparation/

Solicitors Regulation Authority

The SRA's position on data security can be found at:

http://www.sra.org.uk/risk/outlook/priority-risks/information-security.page

Things to do to Prepare for GDPR

1. Understand your obligations;

2. Review (audit) and document your data and what / how you process it (and what legal basis you process it on);

3. Think about who processes data on your behalf and what the associated risks are;

4. Review your technical and operational security measures;

5. Work out what you need to do to become GDPR compliant;

6. Enter into written contracts with Data Processors;

7. Update Privacy Notices and Consents (i.e. in client care letters);

8. Update your policies and procedures (and templates);

9. Formally document the data you process and your processing activity;

10. Train your staff – create a culture of compliance.

Data Protection Officer (DPO)

Under the GDPR, you **must** appoint a DPO if you:

- are a public authority (except for courts acting in their judicial capacity);
- carry out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
- carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

Any organisation is able to appoint a DPO. Regardless of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and skills to discharge your obligations under the GDPR.

You may want to think about whether you should appoint a DPO, even if you are not legally obliged to do so.

The Law Society has produced some guidance at:

http://www.lawsociety.org.uk/Support-services/Practice-management/GDPR-preparation/specialist-guidance-for-law-firms/

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

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws;
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits;
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, clients etc).

You must ensure that:

- The DPO reports to the highest management level of your organisation – i.e. board level;
- The DPO operates independently and is not dismissed or penalised for performing their task;
- Adequate resources are provided to enable DPOs to meet their GDPR obligations.

A DPO can be an existing employee provided that the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests. You can also contract out the role of DPO externally[1].

The GDPR does not specify the precise credentials a DPO is expected to have. It does require that they should have professional experience and knowledge of data protection law. This should be proportionate to the type of processing your organisation carries out, taking into consideration the level of protection the personal data requires.

[1] You can outsource your DPO function to the team at DG Legal. This is not included within our normal retainer service but is available for an additional fee. If you are interested in this service, then please contact us after the training.

The Information Audit

Step 2 of the ICO's 12 steps is to "**document what personal data you hold, where it came from and who you share it with.** You may need to organise an information audit".

An information audit should include consideration of:

1. What types of personal data do you hold
2. Why do you hold it and what do you do with it?
3. Where and how is it stored?
4. What is the lawful basis for processing it (covering all of the ways that you use it)?
5. Does the data subject need to give specific consent and is that consent clear?
6. Is any of it Special Category Data and do you need additional consents to process it?
7. How do you notify the data subject that you are holding data?
8. Does that notification also inform the data subject of who you share it with and who processes it on your behalf?
9. How long do you hold it for and when is it deleted?
10. Is it deleted from all storage systems (paper files; case management system; emails; shared drive etc.)?
11. How secure is that data?

The ICO has provided an Information Audit template spreadsheet at:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/?q=online+identifiers

For DG Legal Retainer Clients, we have created an information audit and Article 30 template on the Compliance Caddy. You can use this to help you comply with your obligations under GDPR[2].

[2] Assisting you with completing this is not part of our normal retainer service. See the end of these materials for additional GDPR services.

The GDPR Principles

Article 5 of the GDPR requires that personal data shall be:

a) **processed lawfully**, fairly and **in a transparent manner** in relation to individuals;

b) collected for specified, **explicit** and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) **kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed**; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Lawful Basis for Processing

- You must have a valid lawful basis in order to process personal data;
- There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual;
- Most lawful bases require that processing is **'necessary'**. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis;
- You must determine your lawful basis before you begin processing, and you should document it. Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason;
- Your privacy notice should include your lawful basis for processing as well as the purposes of the processing;
- If your purposes change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent);

- If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data;

- If you are processing criminal conviction data or data about offences you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

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:

Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

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.

Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

Vital interests: the processing is necessary to protect someone's life.

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.

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.)

Consent versus Contract

The most likely lawful basis that law firm's will rely on as justification for processing data is that 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**" – the **contractual** basis for processing.

However, there may be some things that you do with client data that may not be necessary for the performance of your contract with the client. This may include:

- Making their data available to Lexcel auditors (unless they are legally aided clients where, it is at least arguable, the holding of a relevant quality standard it necessary for the performance of your legally aided retainer with that client;
- Marketing other services – though you can rely on an exemption provided that you are marketing similar services to those for which the data was originally provided;
- Sharing with funders, partners or others, other than for the necessary purposes of progressing the client's case.

In these cases, you may need to rely on consent. The ICO makes clear that the GDPR sets a high standard for consent and that consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build client trust and engagement, and enhance your

reputation. The ICO suggests that you check your consent practices and your existing consents and that you refresh your consents if they don't meet the GDPR standard. Remember:

- Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of default consent;
- Explicit consent requires a very clear and specific statement of consent;
- **Keep your consent requests separate from other terms and conditions;**
- Be specific and 'granular' so that you get separate consent for separate things. Vague or blanket consent is not enough;
- Be clear and concise;
- Name any third-party controllers who will rely on the consent;
- Make it easy for people to withdraw consent and tell them how;
- Keep evidence of consent – who, when, how, and what you told people;
- Keep consent under review and refresh it if anything changes; and
- Avoid making consent to processing a precondition of a service.

Processing Special Category Data (Sensitive Personal Data)

In addition, if you need to process Special Category Data, you need to ensure that at least one of the conditions in Article 9 apply. The most likely relevant conditions from Article 9(2) of the GDPR are:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing relates to personal data which are manifestly made public by the data subject;

(e) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

We need more guidance from WP29 (and from the Law Society, SRA and the Bar Standards Board) on how this applies to law firms and barristers.

Children's Personal Data

The ICO makes clear that children need particular protection when you are collecting and processing personal data relating to children because they may be less aware of the risks involved. If you process children's personal data then you should think about the need to protect them from the outset and design your systems and processes with this in mind. Compliance with the data protection principles and, in particular, fairness should be central to all your processing of children's personal data.

When relying on 'necessary for the performance of a contract', The ICO considers the child's competence to understand what they are agreeing to, and to enter into a contract. When relying on consent, the ICO makes sure that the child understands what they are consenting and that there has been no exploitation in any imbalance in power in the relationship between the child and the data processor.

Demonstrating Compliance

Article 5.2 of the GDPR introduces the accountability principle. This requires you to demonstrate that you comply with the principles. To do this you must:

- implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies;
- maintain relevant documentation on processing activities;
- where appropriate, appoint a data protection officer;
- implement measures that meet the principles of data protection by design and data protection by default;
- use data protection impact assessments where appropriate.

The GDPR contains explicit provisions about documenting your processing activities. You must maintain records on several things such as processing purposes, data sharing and retention.

You may be required to make the records available to the ICO on request. Records must be kept in writing and you may benefit from maintaining their records electronically. Records must be kept up to date and reflect your current processing activities.

WP29 is currently considering the scope of the exemption from documentation of processing activities for small and medium-sized organisations. At present you only need to document processing activities that:

- are not occasional;
- could result in a risk to the rights and freedoms of individuals; or
- involve the processing of special categories of data or criminal conviction and offence data.

It is important to undertake an information audit or data mapping exercise so that you fully understand what data you hold and how the GDPR impacts it.

The principle of accountability requires you to be able to demonstrate that you are complying with the GDPR and have appropriate policies and procedures. This means that you need to be able to show that you have properly considered which lawful basis applies to each processing purpose and can justify your decision.

You need therefore to keep a record of which basis you are relying on for each processing purpose, and a justification for why you believe it applies. There is no standard form for this, so long as you ensure that what you record is sufficient to demonstrate that a lawful basis applies. This will help you comply with accountability obligations and will also help you when writing your privacy notices.

It is your responsibility to ensure that you can demonstrate which lawful basis applies to the particular processing purpose.

Article 30 of the GDPR

Article 30 of the GDPR requires that you must document the following information:

- The name and contact details of your organisation (and where applicable, of other controllers, your representative and your data protection officer);
- The purposes of your processing;
- A description of the categories of individuals and categories of personal data;
- The categories of recipients of personal data;
- Details of your transfers to third countries including documenting the transfer mechanism safeguards in place;
- Retention schedules;
- A description of your technical and organisational security measures.

Should you document anything else?

As part of your record of processing activities, it can be useful to document (or link to documentation of) other aspects of your compliance with the GDPR and the UK's Data Protection Bill. Such documentation may include:

- information required for privacy notices, such as:
    - the lawful basis for the processing;
    - the legitimate interests for the processing;
    - individuals' rights;
    - the existence of automated decision-making, including profiling;
    - the source of the personal data.
- records of consent;
- controller-processor contracts;
- the location of personal data;
- Data Protection Impact Assessment reports;
- records of personal data breaches;
- information required for processing special category data or criminal conviction and offence data under the Data Protection Bill, covering:
    - the condition for processing in the Data Protection Bill;
    - the lawful basis for the processing in the GDPR;
    - your retention and erasure policy document.

For DG Legal Retainer Clients, we have created an information audit and Article 30 template on the Compliance Caddy. You can use this to help you comply with your obligations under GDPR.

Policies, Procedures & Risk Assessment

It is important that the policies and procedures you have in place (often contained in your Office or Quality Manual but may also be contained in your Compliance Plan, Business Continuity Plan, Document Destruction Schedule and/or Training Materials etc.) are updated to reflect the new GDPR requirements.

This means reviewing all of your policies and procedures (and associated templates and precedents) to ensure that they meet the requirements of the GDPR and reflect your actual practice.

You should also ensure that your Risk Assessment / Risk Register has been updated to reflect GDPR and data security risks.

For DG Legal Retainer Clients, we will provide a template "Data Security and Information Governance Manual" but we cannot advise on the specific wording of precedents and templates.

Training Staff

It is not enough to have the policies and procedures in place. It is critical that all of your staff have a clear and meaningful understanding of what is expected of them and how they can play their part in ensuring that personal data is processed lawfully and securely.

Creating a data protection culture is far more effective than just imposing systems and rules.

We can provide additional staff training but this is not included within our normal retainer fee.

This Party Data Processors

Another significant change (though one which reflects existing best practice) is that whenever you use a third-party data processor you must have a **written contract** in place. The contract is important so that both parties understand their responsibilities and liabilities and the GDPR sets out what needs to be included in the contract.

The most important thing to remember is that you are liable for your data processor's compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected.

In the future, using a processor which adheres to an approved code of conduct or certification scheme may help controllers to satisfy this requirement (though at present, no such schemes are available).

Your data processors must only act on your written / documented instructions. They will have direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply, but this doesn't absolve you of your obligations.

Your data processors may include:

- IT providers and cloud server hosts
- Your CMS / PMS provider
- Costs Draftsmen
- Process Servers
- Consultant Solicitors / Freelance Staff
- Experts
- Translators / Interpreters
- File Storage Companies
- Outsourced typists
- Outsourced call answering companies

This is far from an exclusive list.

For the moment, and pending more guidance from the Law Society, SRA and BSB, we have not included counsel or medical experts as both are regulated. However, counsel and medical experts both process data on your behalf and it is difficult to see the ICO allowing you to absolve yourself of responsibility when sending data to them.

Written Contracts

The GDPR defines what must be included in the written contract with a data processor. Such a contract must include:

- 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.

They must also set out that:

- the processor must only act on your written instructions (unless required by law to act without such instructions);
- the processor must ensure that anyone processing the data is subject to a duty of confidence (i.e. that their staff have signed confidentiality agreements);
- the processor must take appropriate measures to ensure the security of processing;
- the processor must only engage a sub-processor with your prior written consent and a written contract;
- the processor must assist you in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- the processor must assist you in meeting your GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments and must notify you **immediately** if any breaches occur whilst they are processing the data;
- the processor must delete or return all personal data to you as requested at the end of the contract; and
- the processor must submit to audits and inspections, provide you with whatever information you need to ensure that you are both meeting your obligations, and must tell you immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

Data Processors outside of the EU

If you use a data processor outside of the EU, you must ensure that the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. If in doubt, seek guidance from the ICO.

In addition, for those with legal aid contracts, it is important to remember that Clause 16.7 of the Legal Aid Contract Standard Terms provides:

> *"You will not transfer the LAA Data or Shared Data outside of the European Economic Area without our express prior written approval."*

Data Subject Rights

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erase
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing. Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing.

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.

You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests. The fee must be based on the administrative cost of providing the information.

Information must be provided without delay and at the latest **within one month** of receipt though this can be extended by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where you refuse to respond to a request, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

You must verify the identity of the person making the request, using 'reasonable means'. If the request is made electronically, you should provide the information in a commonly used electronic format.

Data Security

Under the GDPR, you have a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities.

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

The Law Society and SRA have published significant amounts of guidance on Information Security. The Law Society make clear that *"the following good practice recommendations offer a foundation relevant to all practice sizes and types in developing their own, risk-based policies and procedures for information security.*

> ***Written policy***
> *You should set out your information security practices in a written policy. The policy should reflect solicitors' professional and legal obligations. You should supplement this with implementation procedures. You should monitor these and review them at least annually.*
>
> ***Responsibility***
> *You should appoint a senior member of staff to own the policy and procedures and ensure implementation.*
>
> ***Reliable people***
> *You should implement and maintain effective systems to ensure the continuing reliability of all persons, including non-employees, with access to information held by the firm.*
>
> ***General awareness***
> *You should ensure that all staff and contractors are aware of their duties and responsibilities under the firm's information security policy. This includes understanding how different types of information may need to be managed.*
>
> ***Effective systems***
> *You should identify and invest in suitable organisational and technical systems to manage and protect the confidentiality, integrity and availability of the various types of information you hold."*

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

You may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

Reporting Breaches

The GDPR will introduce a duty on all organisations to report certain types of data breach to the relevant supervisory authority. In some cases, organisations will also have to report certain types of data breach to the individuals affected.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

You only have to notify the relevant supervisory authority of a breach where it is likely to result in a **risk to the rights and freedoms of individuals**. If unaddressed, such a breach is likely to have a significant detrimental effect on individuals. For example, the breach might result in:

- discrimination;
- damage to reputation;
- financial loss;
- loss of confidentiality, or
- any other significant economic or social disadvantage.

This has to be assessed on a case by case basis. For example, you will need to notify the relevant supervisory authority about a loss of client details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly.

A 'high risk' means the threshold for notifying individuals is higher than for notifying the ICO.

What information must a breach notification contain? This would include:

- The nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; and
    - the categories and approximate number of personal data records concerned.
- The name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach;
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

A notifiable breach has to be reported to the ICO within 72 hours of the organisation becoming aware of it.

Failing to notify a breach when required to do so can result in a significant fine up to 10 million Euros or 2 per cent of your global turnover.

ICO Requirements:

- You should make sure that your staff understands what constitutes a data breach, and that this is more than a loss of personal data;
- You should ensure that you have an internal breach reporting procedure is in place. This will facilitate decision-making about whether you need to notify the ICO or the public;
- In light of the tight timescales for reporting a breach - it is important to have robust breach detection, investigation and internal reporting procedures in place.

Sanctions

The following sanctions can be imposed:

- warning in writing in cases of first and non-intentional non-compliance;
- regular periodic data protection audits;
- a fine up to 10,000,000 Euro or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater, where there has been an infringement of the provisions;
- a fine up to 20,000,000 Euro (£17,000,000) or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater, where there has been an infringement of the following provisions:
    - the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
    - the data subjects' rights pursuant to Articles 12 to 22;
    - the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
    - any obligations pursuant to Member State law adopted under Chapter IX;
    - non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

However, Elizabeth Denham, the ICO, has recently stated:

> "***It's true we'll have the power to impose fines much bigger than the £500,000 limit the Data Protection Act allows us… But it's scaremongering to suggest that we'll be making early examples of organisations for minor infringements or that the maximum fine will become the norm.***
>
> ***What's important is that organisations take an approach to their GDPR preparations that is specifically tailored to the key areas of risk they face. If organisations start to think they'll be fined significant amounts for everything, that could create more panic than is necessary and could be unhelpful when they should be trying to put the right focus on areas to correct."***

Some examples of fines under the Data Protection Act:

Example 1

A fine of £60,000 was imposed on employment services company A4e over the theft of a laptop containing personal information about 24,000 people who had used community legal advice centres in Hull and Leicester.

Example 2

Hertfordshire County Council was fined £100,000 for accidentally faxing highly sensitive information about cases involving child sex abuse and care proceedings to the wrong recipients on two occasions in the space of two weeks.

Example 3

The ICO served Aberdeen City Council with a monetary penalty of £100,000 following a serious data breach involving sensitive information about vulnerable children being published online by an employee working from home.

Example 4

A £15,000 fine was imposed on a nursing home which was found to have failed to properly protect the sensitive personal data it held. The data in question related to employees as well as the nursing home's vulnerable residents and covered details including dates of birth, health, resuscitation status as well as sickness absence records and details of disciplinaries. The loss of the data was considered likely to cause substantial damage and distress to the individuals concerned.

Example 5

Andrew Crossley, a solicitor who made money by accusing computer users of illegal file sharing, has been fined £1,000. The penalty was imposed for a data breach which saw the personal details of 6,000 computer users, targeted by his firm, exposed online…

Data Protection by Design & Default

Under the GDPR, you have a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities.

Privacy by design has always been an implicit requirement of data protection that the ICO has consistently championed.

Data Protection Impact Assessment

Data protection impact assessments (also known as privacy impact assessments or DPIAs) are a tool which can help you identify the most effective way to comply with your data protection obligations and meet individuals' expectations of privacy.

An effective DPIA will allow you to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur. You must carry out a DPIA when:

- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals.

Processing that is likely to result in a high risk includes (but is not limited to):

- systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals;
- large scale processing of special categories of data or personal data relation to criminal convictions or offences.

Cyber Essentials

Cyber Essentials is a Government backed scheme that will help you to protect your firm, whatever its size, against a range of the most common cyber-attacks. Cyber Essentials helps you to guard against the most common cyber threats and demonstrate your commitment to cyber security.

Cyber-attacks come in many shapes and sizes, but the vast majority are very basic in nature.

You can find out more about Cyber Essentials at:

https://www.cyberessentials.ncsc.gov.uk/about.html

Where did the Cyber Essentials scheme originate from?

Cyber essentials (CE) pre-dates GDPR by some time and arose out of concerns from GCHQ, amongst others, about the Impact of cyber-attacks on government and those who provide services to government.

The Government worked with the Information Assurance for Small and Medium Enterprises (IASME) consortium and the Information Security Forum (ISF) to develop Cyber Essentials.

The scheme was launched in 2014 and is backed by the Federation of Small Businesses, the Confederation of Business Industry and a number of insurers.

The National Cyber Security Centre say that most attacks are very basic in nature and are carried out by relatively unskilled Individuals.[3] CE Is designed to resist these attacks. Cyber Essentials is designed to be suitable for all organisations, of any size, in any sector.

From 1 October 2014, Government requires all suppliers bidding for contracts involving the handling of certain sensitive and personal information to be certified against the Cyber Essentials scheme[4]. The Government is keen for all suppliers of essential services to be accredited. However, the Ministry of Justice, and, in particular, the Legal Aid Agency appear to have been silent about the scheme. There was a question of the MOJ's approach to Cyber Essentials posed in the House of Commons but the ministry declined to answer the question on the grounds of cost. This is reproduced overleaf.

[3] https://www.cyberessentials.ncsc.gov.uk/about.html

[4] https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

Q
Asked by Jon Trickett, (Hemsworth) **Asked on: 06 October 2017**

Ministry of Justice
Ministry of Justice: Cybercrime
105666
To ask the Secretary of State for Justice, pursuant to the Answer of 12 September 2017 to Question 8042, on Ministry of Justice: cybercrime, whether his Department requires contractors to have obtained a certificate from the Government Cyber Essentials scheme; and how many and what proportion of contractors doing work for his Department have obtained such a certificate.

Answered by: **Dr Phillip Lee**
Answered on: 16 October 2017
The Ministry of Justice follows the approach outlined in Procurement Policy Note 09/14, which - where appropriate - requires its suppliers and contractors to demonstrate adherence to the Cyber Essentials requirements. In many situations, suppliers are contractually obliged to exceed this standard, such as when involved in the delivery of the department's IT services. As assurance is carried out on a case by case basis, by individual departments and programmes, compilation of an exhaustive list of current contractor numbers would mean an answer to this question would exceed the disproportionate cost threshold (DCT).

What is Cyber Essentials and what must you do?

Cyber essentials focusses upon five technical controls which were identified by the government as those that, if they had been in place, would have stopped the majority of the successful cyber-attacks over the last few years.

These technical controls are:

Firewalls

A firewall effectively creates a buffer zone between your network and external networks. The firewall decides whether incoming traffic should be allowed onto your network. An operating system is usually included within your operating system but a complicated network with different types of devices could benefit from a boundary firewall.

Security settings for your devices and software

Manufacturers of hardware and software often supply their goods with very basic passwords such as 'admin' which are easy to guess and provide cyber attackers with opportunities to access your data. Default passwords should therefore be changed to something that should be easy to remember and hard for others to guess.

For particularly sensitive areas such as IT administration and banking, consideration should be given to using two factor authentication.

Old software which is no longer used should be removed.

Access Control

Staff should have access to the software and settings that they need to perform their online role. Additional permissions should only be given to those that need them. The point here is that administrative privileges should only be given to those who need them because hackers with access to such an account can cause significant damage.

Viruses and Malware

Malware is software or content on the internet designed to cause damage.

Amongst the steps firms can take to minimise the risk of being infected is to keep antivirus software up to date and to use the most up to date version of the internet browser available.

Devices and Software

Weaknesses are regularly identified and exploited in operating systems and installed software. These are regularly reported in the news. It is critical to ensure that updates are installed regularly.

Examples include Microsoft Windows and Apple's Operating Systems. Both companies regularly release 'patches' to fix any vulnerabilities identified.

Firms should maintain a register of all software used and ensure that there is a system in place for keeping all software up to date.

Levels of Engagement

As a minimum, all firms should understand and act on the five technical controls listed above. Given that firms in the legal sector control sensitive personal information it is recommended that accreditation is achieved.

There is a self-assessment option available which is simple and costs around £300. Firms can opt to buy in assistance to achieve accreditation if they need it.

Cyber Essentials Plus covers the same areas but verification of your cyber security is undertaken independently by a Certification Body.

Cyber Essentials - The Law Society view

There has been support from The Law Society for firms to consider adopting Cyber Essentials. For instance, Tim Hill, technology policy adviser to the Law Society encourages firms to think about Cyber Essentials when adopting a cyber security program. See http://www.legalvoice.org.uk/cybersecurity-shoe-string/

However, Cyber Essentials is not currently mandatory and the Law Society is unlikely to suggest that all firms must have it. For instance, a firm providing legal advice to businesses akin to an in-house lawyer without case files is not as vulnerable as a firm providing advice to children or criminal clients.

Cyber Essentials - Benefits of Accreditation

Becoming accredited addresses the most common internet based threats to your business.

Accredited firms are permitted to use the CE logos on their stationery, email signatures, website and promotional material in accordance with the branding guidelines.[5] Clients and potential clients will be reassured that these firms take data protection seriously.

The cost of obtaining accreditation is relatively modest compared with most accreditation schemes.

Cyber Security - Other Tools

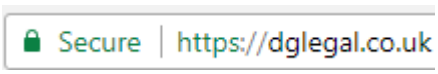
Secure your website

A significant number of law firms still do not have secure websites. Secure websites start with the address https://

Chrome and Firefox users are able to see warnings on unsecured sites: 'Your connection to this site is not secure'. If you do not have a secure website, this will scare off some potential clients away from using your site.

In order to 'secure' your website, you should purchase a SSL certificate. The cost should be in the region of £50 to £300 depending upon the number of websites and domains requiring protection. Once purchased, the browser bar linked with your website will turn partially green.

For instance, the browser bar on the DG Legal website displays the image below.



[5] https://www.portcullis-security.com/wp-content/uploads/2014/11/Branding-Guidelines-for-BADGE-v1-0.pdf

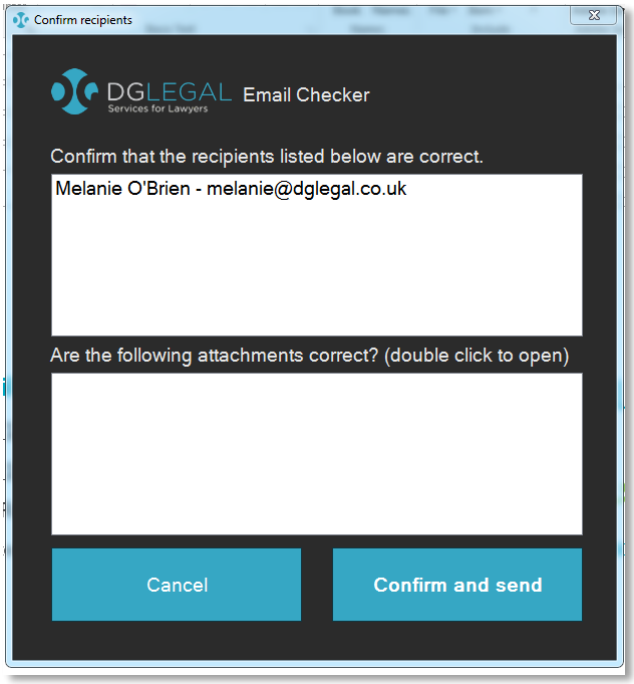
Further, according to numerous I.T. experts, having a secure website boosts your Google search engine ranking.

Email Pop Up Checker

Perhaps the most common data security breach in law firms is sending an email to an unintended recipient or attaching the incorrect document.

Firms should consider using a pop-up checker which asks the sender to confirm the recipients listed and any documents attached are correct.

For instance, the software we have developed displays the following message:



Such software lowers the risk of making an embarrassing or negligent error. However, some lawyers may not appreciate the delay of a few seconds caused by introducing this step.

Alternatively, firms can adjust their email settings in order to delay the sending of software by a few minutes to give lawyers an opportunity to retrieve an email if necessary. Instead firms could disable the auto-address feature in Outlook and other email programs but that might cause a rebellion!

Additional DG Legal GDPR Services

At DG Legal we are doing everything we can to help our retainer clients prepare for GDPR. This includes:

- Running this and other free training courses;
- Introducing a Data Security and Information Governance manual to assist with GDPR obligations;
- Amending our templates to reflect GDPR changes;
- Providing these Guidance Notes to help firms better understand their obligations under the GDPR.

However, we are already aware that some of our clients need additional help and assistance which is not covered under the terms of our retainer agreement. Therefore, we have developed the following services:

On-site Consultancy

If you need some additional on-site consultancy to help you undertake your information audit and comply with GDPR then we can assist by sending in one of our expert consultants. The daily rate for this assistance is £950 plus VAT. The number of days required will depend on the size and nature of your practice but will typically be between 2-5 days to work on-site and then to prepare the necessary report, recommendations and assistance.

Help with the Compliance Caddy Information Audit

For those who need less help, we can provide telephone / email-based assistance with your completion of the Compliance Caddy information audit template. This is priced from £500 plus VAT.

In-house Training

We can provide in-house GDPR training to your staff. A typical 2-hour session for up to 30 staff (at your venue – so excluding venue costs) starts at £750 plus VAT. This includes all training materials.

Outsourced DPO Services

If you want to outsource your DPO function to DG Legal we can assist by making one of our expert consultants your DPO. Pricing for this service is available on request.

Updates to these materials

Updates to these materials will be announced via the weekly Friday LegalVoice update and hosted on the DG Legal website.