



GDPR

How to Implement an Effective System

March 2018



- Founder of DG Legal Ltd
- Formerly Senior Manager at the Legal Services Commission
- Worked with several hundred law firms over the past 20 years

David Gilmore
Email: david@dglegal.co.uk
Phone: 01509 214999





- Consultant at DG Legal Ltd
- Non-practising Solicitor
- Formerly Senior Legal Adviser to the Legal services Commission
- Formerly Legal Standards Principal at the Cooperative Legal Services Ltd
- Committee Member at the Legal Aid Practitioners Group

Matthew Howgate
Email: matt@dglegal.co.uk
Phone: 07852 977722



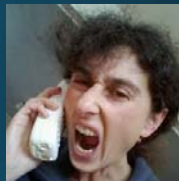


For the love of
God, please.....





Is it 1999 all
over again?



Content of today's course...

- GDPR Awareness
- Assessing your readiness
- Cyber Essentials



General Data Protection Regulation

Comes in to force on 25th May 2018

Definitions: Personal Data

"any information relating to an identified or identifiable natural person"

"The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier."

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people."

Definitions: Special Category Data

Sensitive Personal Data

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.

Definitions

Data Controller: YOU

Data Processor: A processor is responsible for processing personal data on behalf of a controller.

Preparing 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.

DPO – what they do...

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.

You can outsource the DPO function.

The Information Audit

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

The GDPR Principles...

Personal data shall be:

- processed lawfully, fairly and in a **transparent** manner in relation to individuals;
- collected for specified, **explicit** and legitimate purposes and not further processed in a manner that is incompatible with those purposes...;
- adequate, relevant and limited to what is **necessary** in relation to the purposes for which they are processed;
- 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**;

- 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...**;
- 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

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.)

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."

BUT is the only purpose for which you are using the personal data the performance of the contract / retainer—or are you also using it for other purposes?

Consent

- 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.
- Avoid making consent to processing a precondition of a service.

Processing Special Category Data

- (a) the **data subject has given explicit consent** to the processing of those personal data for one or more specified purposes...;
- (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 relates to personal data which are manifestly made public by the data subject;
- (d) **processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;**

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.

Article 30 of the GDPR requires that 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.

Compliance Caddy and Quality Manual (Policies, procedures etc.)

WARNING: Data Processors

- Whenever you use a third-party data processor you must have a **written contract** in place.
- 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.
- 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.

Data Processors: The Contract

- 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.

- 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 Subject Rights

- The right to be informed
- The right of access
- The right to rectification
- The right to erase
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Subject access...

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).

- 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.
- 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 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. You must carry out a Data Protection Impact Assessment when:

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

Reporting Breaches

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 ICO 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.

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.

Sanctions under GDPR

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 some provisions,
- a fine up to **20,000,000 Euro** (£27,000,000) 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).

But...

"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."

Elizabeth Denham, the Information Commissioner

Example 1

A fine of £60,000 was imposed on employment services company Age 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 disciplinarys. 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...



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.

What are your organisational data security measures?

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."



Where did Cyber Essentials come from?

- Arose out of concerns from amongst other, GCHQ, about the impact of cyber attacks on government and those who provide services for government
- The Government worked with a number of stakeholders to develop the cyber essentials (CE) scheme
- CE focusses upon a small number of 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

Where did Cyber Essentials come from?

- It is backed by industry including the Federation of Small Businesses, the CBI and a number of insurance organisations which are offering incentives for businesses.
- It is designed to be suitable for all organisations, of any size, in any sector.

Source: <https://www.cyberessentials.ncsc.gov.uk/about.html>

What is Cyber Essentials?

- A simple but effective Government backed scheme that will help you to protect your organisation against a whole range of the most common cyber attacks
- It focusses upon 5 technical controls which if effectively implemented stop the majority of cyber attacks
- Cyber Essentials is designed prevent these attacks...

Cyber Essentials –What must you do?

- Use a firewall
- Take care with security settings for your devices and software
- Maintain Access Control
- Avoid Viruses and malware
- Keep devices and software up to date

Cyber Essentials – 3 Levels of Engagement

- [Familiarise yourself with](#) cyber security terminology
- [Go for basic, or entry level Cyber Essentials certification](#)
- For those who want to take cyber security further, you can go for [Cyber Essentials Plus certification](#).


Cyber Essentials – TLS view

- '65% of law firms have been a victim of a cyber incident'
 - Source: <http://www.lawsociety.org.uk/news/blog/are-you-the-65-percent-or-the-35-per-cent-65-percent-of-law-firms-cyber-attack-victim/>
 - Graham Murphy, CQS Manager, The Law Society
 - 'Cyber Essentials will help you ensure your business has the basic level of protection against the most common online threats.'
 - Tim Hill, technology policy adviser to The Law Society
- Source: <http://www.legalvoice.org.uk/cybersecurity-shoe-string/>

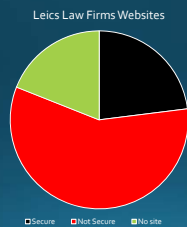
Cyber Essentials – Benefits

- Addresses the most common Internet-based threats to your business
- Reassures clients that you take data protection seriously
- Is low cost – around £300 for accreditation

Cyber Security – Other Tools

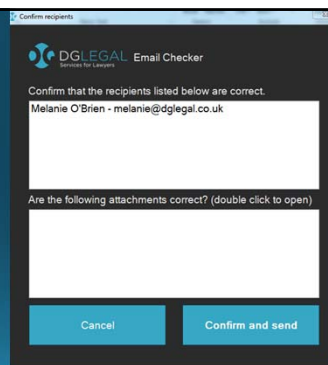
- Consider having a SSL certificate to secure your website
- These websites begin with https: e.g.  Secure | <https://dlegal.co.uk>
- Chrome and Firefox users are able to see warnings on unsecured sites: 'Your connection to this site is not secure'
- Google gives some search engine ranking credit to sites with a SSL certificate

Secure websites – a survey



Cyber Essentials – Other Tools

- Consider using an Email pop-up checker



ANY
QUESTIONS?

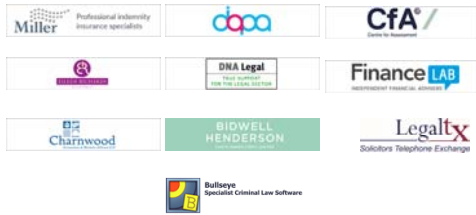


A FREE electronic magazine about Access to Justice

Updates about this and other courses are released via LegalVoice and the DG Legal websites

We shall send you a free newsletter every Friday unless you'd prefer to opt-out or you may unsubscribe

Thank you to the following LegalVoice supporters





www.dglegal.co.uk
