Wellers Law Group LLP

The General Data Protection Regulation 2016 (GDPR)

Your guide to the changes to data protection legislation.

Contents

What is the legislation? 3

Who does it apply to? 3

What are the risks to your organisation? 3

The Law 4

What is meant by 'personal data'? 5

Extending the rights of data subjects 5

A lawful basis for processing data 6

What to consider if you rely on consent 7

Data subject rights – access and control 9

Accountability and governance 11

Contracts 12

Documenting your actions and procedures 13

Data protection impact assessments (DPIAs) 14

Data Protection Officers 15

Data breaches 16

Security 17

The need for an audit 18

Data protection – legal services from Wellers Law Group 19

What is the legislation?

The General Data Protection Regulation 2016 (GDPR) governs how organisations handle personal data - information which identifies an individual. Compliance with GDPR is required from 25th May 2018 when it replaces the Data Protection Act 1998.

Who does it apply to?

No matter what kind of organisation you are (corporate/charity/small business/sole trader/public body) the changes introduced by this legislation will apply to you and they will apply directly to data processors as well as data controllers.

For clarity, a controller determines the purposes and means of processing personal data.
A processor is responsible for processing personal data on behalf of a controller.

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach. However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the regulations.

The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

What are the risks to your organisation?

The new rules essentially aim to create a cultural change in the way in which data is controlled and used by organisations, with a view to protecting the privacy rights of individuals. It applies to all kinds of data held by organisations and almost every action an organisation carries out relating to that data.

On a practical level there are three reasons why complying with the GDPR is urgent:

One, because the rules introduce lots of new 'must do's'. If anything ever goes wrong with your data (a cyber-attack or leak) you have to be able to prove to the regulator that you've taken steps to prevent that happening.

Two, because the fines for failing to comply with the new rules are potentially huge. They are increased from the current maximum of £500,000 to up to 4% of annual worldwide turnover or €20m (for serious breaches) – 40 times higher than the current regime! So data protection compliance is now a major risk for organisations which they ignore at their peril;

Three, because a failure to comply with the regime can lead to catastrophic reputational damage and loss of consumer confidence in an entity, be it charitable or corporate.

The Law

The GDPR sets out the key principles that constitute the main responsibilities for organisations in relation to personal data. These are that data should 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; 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.
- **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; 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
- **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.
- **Accountability**
  A further key development is the principle of accountability. The regulations state that the data controller shall be "responsible for, and be able to demonstrate, compliance with the principles. " The new emphasis on demonstrable compliance will be critical in changing attitudes.

> "Responsible for, and be able to demonstrate, compliance with the principles."

What is meant by 'personal data'?

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.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that have been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

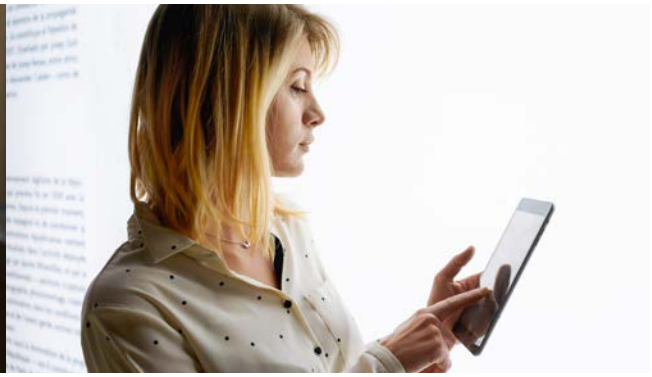
The GDPR also recognises that there are areas of sensitive personal data that require additional protections. The special categories specifically include personal data such as genetic data, biometric data where processed to uniquely identify an individual, data on sexual orientation, political or religious beliefs and health details. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to processing this type of data.

The rules apply to corporate data where an individual can be identified just as much as consumer data and it is not restricted to your clients and prospects as a business. It applies to employees, suppliers, donors and volunteers (in the case of a charity) patients and your shareholders or other relationships your organisation maintains.

Extending the rights of data subjects

Under GDPR data subjects have new and extended rights which broadly fall into the following categories:

- **A lawful basis for processing** - A data controller or processor requires a lawful basis for processing personal data in the first place. This encompasses a number of categories mainly based on the legitimate requirements of an organisation in transacting business with the data subject.
- **Including new standards for obtaining consent** - Included in the above is consent from the data subject, however the bar for what constitutes consent has risen significantly and will affect all businesses that use personal data for marketing purposes.
- **Data access and control** - Data subjects also acquire a set of other rights in relation how their data is held and accessed, such as the right have their data updated, erased or to prevent certain types of processing.
- **Data must be secure** - Personal data is to be processed in a manner that is secure, to minimise the risk of loss, destruction or damage, with the onus on the data controller to demonstrate that data protection measures have been put in place.



A lawful basis for processing data

For processing of personal data to take place under the GDPR, you need to identify a lawful basis. It is important that you document what this basis is.

Your lawful basis for processing has an effect on individuals' rights. For example, if you rely on someone's consent to process their data, they will generally have stronger rights, for example to have their data deleted.

These provisions are particularly relevant to public authorities and highly regulated sectors.

The list below sets out the lawful bases available for processing personal data and special categories of data, starting with obtaining consent.

Consent

Consent requires a positive 'opt in' rather than a failure to 'opt out' which has been the norm under the previous regime. So pre-ticked boxes and consent by default are things of the past.

It also needs to be clear what exactly the data subject is consenting to, no longer can it be vague or general. Consent should be specific and granular. If data may be processed for a variety of reasons then those reasons and the organisations doing the processing must be explicitly stated in a clear and concise way.

Keep your consent requests separate from other terms and conditions. Avoid having consent as a precondition of signing up for a service and in particular trying to hide it within a set of terms of business. It is likely the data protection aspects of an agreement with a client, will need to be a separate document.

The principle of accountability means that you will have to keep evidence of consent – who, when and how and what you specifically asked or told data subjects. Remember if your relationship with a data subject changes (they leave your employment or the buy a new service, the consent they gave may need to be overwritten or updated - organisations will be expected to make it easy to withdraw consent.

Remember – you don't always need consent. If consent is too difficult, look at whether another lawful basis is more appropriate.

What to consider if you rely on consent

If you rely on consent in order to process data then you need to check your process for collecting consent and the validity of your existing consents. Is your wording granular enough to cover all uses? Do you have a process for all routes by which you collect data e.g. enquiries on your website. Do you have an audit trail and is consent separated from your general terms of doing business are key questions?

You will have to refresh consents if they don't meet the GDPR standard.

As mentioned earlier, you don't always need consent, it may be that another lawful basis is more appropriate.

The following options are the other lawful reasons for your business to be processing personal data:

- **Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract**
- **Processing is necessary for compliance with a legal obligation**
- **Processing is necessary to protect the vital interests of a data subject or another person**
- **Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.**
- **Processing necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.**

The GDPR recognises that special categories of data require tighter safeguards but also that they have value in a wider context and therefore a more extensive list of criteria for processing has been constructed. These include such situations as processing necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.

In the area of healthcare, processing may be acceptable for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services. Similarly processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes.

A fuller list of additional processing criteria for special categories of data can be found on the ICO website **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-bases-for-processing/**

REVIEW HOW LONG YOU NEED THE DATA

Alongside determining the lawful basis for processing data you should also now determine how long you need to keep the data for that purpose.

Clearly some long term contracts require you to keep records for many years, however the need to keep data resulting from short-term transactional relationships will be more limited.

Remember to document your policy to show you have thought this through.

Data subject rights – access and control

Previous legislation had made some strides in allowing individuals to request what data was held on them by organisations, however the GDPR again takes these rights to a new level, extending previously available rights and introducing new ones.

The right to be informed – Organisations must provide data subjects with 'fair processing information'. This includes, amongst other things, an explanation of what data they hold, the lawful basis for processing, what purpose it is being used for, how long it will be held for and how to withdraw consent. The emphasis is on providing a clear, concise and transparent explanation. This information is likely to be provided by organisations via a privacy notice when data is collected.

The right to access – Individuals have the right to access their personal data and supplementary information that has been added to it through processing or from a third party. The right of access allows individuals to be aware of and verify the lawfulness of the processing. Access must be free of charge although a reasonable fee may be charged for excessive or unfounded requests for access.

The right to rectification – Individuals have the right to have personal data rectified if it is inaccurate or incomplete and organisations must also inform any third parties they have disclosed the data to, about the rectification and let the individual know who else has the incorrect data.

The right to erasure – The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. However this is not an absolute right and it can be denied if for example data is required in relation to a legal claim or if it is in the public interest.

The right to restrict processing – Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future. If you have disclosed the data to third parties, you would have a responsibility to inform them of the restriction.

The right to data portability – This is a potentially complex area for businesses to comply with and the benefits may be specific to a limited number of situations. The right allows data provided to one organisation to be transferred to another, for the purposes of obtaining a better deal. A typical example might be moving bank accounts or a new utility provider.

The right to object – Based on grounds relating to their 'particular situation' an individual has the right to object to the processing their data for direct marketing (including profiling), scientific/historical research and even on legitimate interests or the performance of a task in the public interest/exercise of official authority. Organisations must cease processing unless they have compelling grounds to continue which would override this right or the processing relates to a legal claim. Either way organisations must inform individuals of their right to object clearly and separately from other information "at the point of first communication" and in your privacy notice.

Rights related to automated decision making, including profiling – This provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. The right exists for decisions that may have a legal effect or similarly significant effect on an individual. If this is the case you must ensure individuals are able to obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it. As with other rights granted under GDPR if the automated process is required by law or necessary to the terms of a contract then the right does not apply.

It should be noted that automated decision making on issues concerning a child or using sensitive personal data is not permitted (unless specific consent has been given or there is a substantial public interest).

As a general rule you will need to respond to data subjects using these rights (for example providing access to data, rectification, portability) 'without undue delay' and within a month, although an extension of a further two months is allowed you will need to tell the data subject within a month why it will take longer.

WOULD YOUR SYSTEMS BE ABLE TO COPE WITH THESE RIGHTS?

Most organisations use administrative, marketing and HR systems created by specialist providers. A key step to your own compliance is to check with the providers what steps they are taking to comply with the GDPR. And remember to document that process, so you have evidence in the form of an audit trail.

Accountability and governance

As mentioned earlier, a central principle behind this new legislation is accountability. The accountability principle requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

Demonstrable compliance brings with it the need to implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies including staff training, internal audits of processing activities, and reviews of internal HR policies.

In particular, organisations need to recognise that they should not just design processes to meet the regulations, they need to maintain relevant documentation on processing activities. The regulations are seeking data protection by design and by default and this means that every time you instigate an activity (systems change, product launch, acquisition or sale for example) you will be required to assess the impact that might have on the data protection environment.

It is asking organisations to think about issues such as minimising data - how much data they really need to retain and for how long. Could it be anonymised? How well have data subjects been informed about what happens to their data and what risks it might pose for them if the data is lost or stolen?

Contracts

Whenever a data controller uses a processor it needs to have a written contract in place. The contract is important so that both parties understand their responsibilities and liabilities.

The GDPR sets out what needs to be included in the contract. In the future, standard contract clauses may be provided by the European Commission or the ICO, and may form part of certification schemes. However at the moment no standard clauses have been drafted.

Controllers are liable for their 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 – although again, no such schemes are currently available.

Processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply.

The legislation sets out a comprehensive list of inclusions in the contract from setting the scope by stating the subject matter, duration of the processing, the nature and purpose of the processing, the type of personal data, categories of data subject and the obligations and rights of the controller through to the specific instructions to the processor and the requirement for appropriate security measures to be in place.

A contract should also cover the fact that a processor may sub-contract an element of the processing to a third party (sub-processor). They have not only to inform the data controller but must seek permission before going ahead. They are also responsible for the compliance of the third party with the GDPR in carrying out this sub-contracting work.

Processors will need to comply with a wider range of requirements than controllers. They will be have to be responsive, assisting the data controller in meeting its obligation in relation to data subject rights, submit to audits and inspections to check compliance and of course provide suitable levels of security for the processing they carry out.

Naturally a processor must co-operate with supervisory authorities (such as the ICO) and ensure that they keep accurate records of processing activities, notify any personal data breaches to the data controller and employ a data protection officer.

Documenting your actions and procedures

As well as your obligation to provide comprehensive, clear and transparent privacy policies, if your organisation has more than 250 employees, you must maintain additional internal records of your processing activities. If your organisation has less than 250 employees you are required to maintain records of activities related to higher risk processing, such as:

- **Processing personal data that could result in a risk to the rights and freedoms of individual; or**
- **Processing of special categories of data or criminal convictions and offences.**

You must record the following information:

- **Name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer)**
- **Purposes of the processing**
- **Description of the categories of individuals and categories of personal data**
- **Categories of recipients of personal data**
- **Details of transfers to third countries including documentation of the transfer mechanism safeguards in place**
- **Retention schedules; and**
- **Description of technical and organisational security measures.**

You may be required to make these records available to the relevant supervisory authority for the purposes of an investigation.

Whatever the size of your organisation it would be wise to document your policies and actions in relation to the GDPR. For example a document that sets out the location of all the data you hold (both within your IT infrastructure and held in hard copy would be valuable in examining the consequences of organisational changes. A record of all the activities you have undertaken to meet the requirements of the regulations is also important. We live in an imperfect world, often dependent on the activities of other businesses, and there may be problem areas in implementing the necessary changes, but an audit trail that highlights the actions you have taken where an issue has fallen down through no fault of your organisation may have value.

REVIEW CONTRACTS WITH PROCESSORS

A major element of compliance with the GDPR is having contracts in place with data processors which ensure the protection of personal data.

Data protection impact assessments (DPIAs)

Data protection impact assessments (also known as privacy impact assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage.

You must carry out a DPIA when using new technologies and when 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 in relation to criminal convictions or offences.**

This includes processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms e.g. based on the sensitivity of the processing activity such as large scale systematic monitoring of public areas (CCTV).

What information should the DPIA contain?

- **A description of the processing operations and the purposes, including where applicable, the legitimate interests pursued by the controller.**
- **An assessment of the necessity and proportionality of the processing in relation to the purpose.**
- **An assessment of the risks to individuals.**
- **The measures in place to address risk, including security and a demonstration that you comply.**

Data Protection Officers

Only certain types of organisation need to create the role of Data Protection Officer to meet the needs of the new regulations. 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)**
- **Carry out large scale processing of special categories of data or data relating to criminal convictions and offences.**

You may appoint a single data protection officer to act for a group of companies or for a group of public authorities, taking into account their structure and size.

However any organisation is able to appoint a DPO, regardless of whether the GDPR obliges you to. It should be borne in mind that if a DPO is appointed, they would be treated and judged as if it was a mandatory appointment. On positive note, the presence of a DPO within an organisation could contribute to a business's or charity's credibility and provide reassurance to potential clients. Data security and protection is a new element in the branding mix.

Whether you appoint a DPO or not, for most medium sized organisations, having a specific individual focused on data protection is likely to help meet compliance standards and a clear indication of the efforts being made to comply.

The DPO's minimum tasks are defined 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, advising on data protection impact assessments training staff and conducting internal audits.**
- **To be the first point of contact for supervisory authorities and for individuals whose data is processed such as employees and customers.**

The DPO is required to report into the highest decision making level in the organisation, it would not be acceptable to sideline the role by having it report into lower or mid-level management structure. It is also wise in terms of compliance to introduce a standing agenda item on data protection for the board or executive team meetings.

Data breaches

What breaches do I need to notify the relevant supervisory authority about?

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, if it could 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 customer 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.

You have a responsibility to notify individuals affected 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 relevant supervisory authority.

What information must a breach notification contain?

- **The nature of the personal data breach including, where possible:**
- **the categories and approximate number of individuals concerned**
- **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 relevant supervisory authority within 72 hours of the organisation becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases.

If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay.

As an organisation you will need a formal process in place to notify the relevant supervisory authority.

Security

Clearly a key component of data protection is the security put in place by an organisation. In part this will be achieved through technology and in part through creating a culture that takes security seriously – the days of writing computer passwords on a post it note and sticking it on a terminal are over.

Any review of security is likely to address the following areas:

Access to IT systems holding data:

- Assess firewall settings
- Is malware protection up to date?
- Is your software up to date?
- Precautions needed for mobile working
- Who has system access and how is this controlled – access authority review?
- Are passwords regularly reset and strong?
- What rules are set for use of personal lap tops and phones?

Encryption is likely to be important:

- Sending and receiving data – the need for encryption for email, remote desktops and file sharing over a network so that others cannot see the data.
- Devices – USB sticks and drives are easy to lose therefore data is likely to require encryption
- Back-ups – encryption of data being backed-up online.

In the event of data loss:

- Is there a regular (daily) back-up?
- What is the process to restore data from back-ups?

Access to hard copy data:

- Who has physical access and how is this controlled – access authority review?

Protecting sensitive data:

- Likely to require encryption
- Can data be anonymised to make it more difficult to use if stolen?

The ICO website lists a wide range of guidance on standards of security that organisations should seek.

The need for an audit

Most organisations, whether large or small and however well run may find it difficult to comply with such wide ranging changes to the existing data protection regime. It is likely that the most effective route to compliance is to start with an audit of all the data you hold, process and have processed by other parties.

GDPR Compliance issues to be audited
• Where the data is held/processed? – Which systems is it on? – Where are hard copies filed and archived?
• What types of data are held?
• What is your lawful basis for processing that data?
• Do you have the correct consents in place?
• How could you reduce the data? – Minimising the amount you hold – Determining how long you need to hold it
• Who has access to it?
• Who has responsibility for access?
• What security rules are in place to prevent others accessing it?
• Are existing security rules communicated and adhered to?
• Can you meet data subject rights on your systems e.g. the right of erasure, the rights to rectification, access and to restrict processing?
• Who processes your data?
• Contracts with processors that need to be reviewed
• Contracts with suppliers that need to be reviewed
• Does your staff handbook and contracts of employment recognise the importance of data protection?

Data protection – legal services from Wellers Law Group

Wellers Law Group offers three levels of service for businesses, charities and public bodies seeking compliance with GDPR.

Comprehensive data audit with a focus on:

- Clients, donors, constituents, volunteers
- Staff (relevant to your business)

- Red, Amber, Green rated assessment of present performance

Recommendations for compliance

- Recommendation of a full set of documentation to meet GDPR standards from privacy policy, Terms of Business, consent requirements, standard contracts for suppliers and data processors.

Further additional advice can include

Advice on policies to be implemented. e.g. breach reporting and security measures (if required)

- Staff training can be arranged as appropriate
- Independent outsourced Data Protection Officer for businesses, charities and public bodies that do not wish to make an internal appointment

Medium data audit based on the assumption that the business is broadly aware where high priority issues exist - covering:

- Clients, donors, constituents, volunteers
- Staff (relevant to your business)

- Red, Amber, Green rated assessment of present performance

Recommendations for compliance

Advice on policies to be implemented e.g. breach reporting, security measures. (if required)

Basic Audit based on the assumption that the business is aware where high priority issues exist and only basic advice is needed - covering:

- Clients, donors, constituents, volunteers
- Staff (relevant to your business)

- Red, Amber, Green rated assessment of present performance

Additional services:

- Standard documentation to meet GDPR is further available:
  - Privacy policy
  - Terms of Business (where applicable)
  - Consent requirements
  - Standard contracts for suppliers
  - Data processor contracts
  - Guidance on policies e.g. Breach reporting, security measures

Wellers Law Group LLP

Wellers Law Group LLP, 65 Leadenhall Street, London EC3A 2AD

Email: enquiries@wellerslawgroup.com

London City office: **020 7481 2422**

www.wellerslawgroup.com

BUSWLG 003 0118