1. Introduction
   1.1.1. What is GDPR?
   1.1.2. Brexit
   1.1.3. Compliance
   1.1.4. This Guide

2. Data Protection Officer
   2.1.1. What does ‘core activities’ mean?
   2.1.2. What does ‘large scale’ mean?

3. Holding Data
   3.1.1. Individuals Rights
   3.1.2. Access requests
   3.1.3. Right to be forgotten
   3.1.4. Documentation
   3.1.5. Privacy Notices

4. Processing Data
   4.1.1. Data Protection by Design and Data Protection Impact Assessments
   4.1.2. Consent
   4.1.3. Lawful Basis
   4.1.4. Children

5. Breach Notification

6. Protecting Data
   6.1.1. Assess the threats and risks to your business
   6.1.2. Get in line with Cyber Essentials
   6.1.3. Secure your data on the move and in the office
   6.1.4. Secure your data in the cloud
   6.1.5. Back up your data
   6.1.6. Train your staff
   6.1.7. Keep an eye out for problems
   6.1.8. Know what you should be doing
   6.1.9. Minimise your data
   6.1.10. Make sure your IT contractor is doing what they should be

7. MT Services

This Guide is intended to provide an overview of GDPR and is not a definitive statement of the law
Introduction

What is GDPR?
The General Data Protection Regulation (GDPR) is an EU regulation which is intended to strengthen and unify data protection for all individuals within the EU. It will come into effect on the 25th May 2018 and immediately replace the UK Data Protection Act (DPA).

While the current UK DPA already includes the vast majority of the regulations included in GDPR many of these have been strengthened and the maximum fine has been raised to €20 Million or 4% of global revenues (whichever is higher).

Brexit
Brexit will have no bearing on GDPR as any company that carries out business within the EU or holds any personal information on an EU citizen will need to comply to GDPR.

More importantly the UK Information Commissioner’s Office (ICO) intends to enforce the rules anyway.

Compliance
There is currently no certification or accreditation for GDPR which means that you can not physically achieve GDPR compliance. If you do misuse/leak/lose any personal data, the ICO will take into account the processes, workflows and security you have put in place for GDPR when determining the size of any fine.

It is also worth noting that although the GDPR law has been passed and documented, there is an EU Article 29 working party (which includes the ICO) who have been tasked with providing guidelines for complying with GDPR. This work however, is still ongoing and so far finalised guidelines are only available for Data Portability, Data Protection Officers and Lead Supervisory Authority.

It is also worth noting that the official GDPR regulation document includes a number of references to special considerations being made for SMEs, but there is currently no clarification of what this means.

This Guide
This document aims to give an overview of what your business needs to consider regarding the GDPR regulation and contains information from the following sources:

- Information Commissioner’s Office (ICO)
- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
- Article 29 Working Party

It is also based on the information available as of July 2017, which may be subject to change. Please note: MT Services does not accept any responsibility or liability for any information included in this guide.
Data Protection Officer

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 (DPO). You must designate a DPO if:

- The processing is carried out by a public authority or body (irrespective of data being processed)
- The core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale
- The core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences

What does ‘core activities’ mean?
These include all activities where the processing of data forms as inextricable part of your activity. For example, processing health data, such as patient’s health records, should be considered as one of any hospital’s core activities and hospitals must therefore designate DPOs.

On the other hand, all organisations carry out certain supporting activities, for example, paying their employees or having standard IT support activities. These are examples of necessary support functions for the organisation’s core activity or main business. Even though these activities are necessary or essential, they are usually considered ancillary functions rather than the core activity.

What does ‘large scale’ mean?
The GDPR does not define what constitutes large-scale processing. The following factors, should, be considered when determining whether the processing is carried out on a large scale:

- the number of data subjects concerned - either as a specific number or as a proportion of the relevant population
- the volume of data and/or the range of different data items being processed
- the duration, or permanence, of the data processing activity
- the geographical extent of the processing activity

Examples of large scale processing include:
- processing of patient data in the regular course of business by a hospital
- processing of travel data of individuals using a city’s public transport system (e.g. tracking via travel cards)
- processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in these activities
- processing of customer data in the regular course of business by an insurance company or a bank
- processing of personal data for behavioural advertising by a search engine
- processing of data (content, traffic, location) by telephone or internet service providers

Examples that do not constitute large-scale processing include:
- processing of patient data by an individual physician
- processing of personal data relating to criminal convictions and offences by an individual lawyer
Holding Data

Individuals Rights

One of that main focuses of GDPR is the protection of individuals’ rights regarding their personal data. On the whole in the UK, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some significant enhancements.

The GDPR includes the following rights for individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

The ICO ‘Overview of the General Data Protection Regulation (GDPR)’ guide provides more information on the above.

Access requests

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.

These are similar to existing subject access rights under the UK DPA.

- In most cases, you will not be able to charge for complying with a request.
- You will have a month to comply, rather than the current 40 days.
- You can refuse or charge for requests that are manifestly unfounded or excessive.
- If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month.

Right to be forgotten

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 whether there is no compelling reason for its continued processing.

The right to erasure does not provide an absolute ‘right to be forgotten’. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
• The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
• The personal data must be erased to comply with a legal obligation.
• The personal data is processed in relation to the offer of information society services to a child.

Documentation
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 across the organisation or within particular business areas.

The GDPR requires you to maintain records of your processing activities. It updates rights for a networked world. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own records. You won’t be able to do this unless you know what personal data you hold, where it came from and who you share it with.

You should document this. Doing this will also help you to comply with the GDPR’s accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

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

The GDPR says that the information you provide to people about how you process their personal data must be:

• concise, transparent, intelligible and easily accessible;
• written in clear and plain language, particularly if addressed to a child;
• and free of charge.

You may need to include more information in their privacy notices, but the ICO believes that if you follow the good practice recommendations in their ‘Privacy notices, transparency and control’ code you will be well placed to comply with the GDPR regime. There is still discretion for data controllers to consider where the information required by GDPR should be displayed in different layers of a notice.
Processing Data

Data Protection by Design and Data Protection Impact Assessments

The GDPR makes privacy by design an express legal requirement, under the term ‘data protection by design and by default’. It also makes PIAs – referred to as ‘Data Protection Impact Assessments’ or DPIAs – mandatory in situations where data processing is likely to result in high risk to individual’s rights and freedoms.

Examples of high risk processing:

- A systematic and extensive evaluation of personal aspects which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the person or similarly significantly affect the person.
- Processing on a large scale of special categories of or of personal data relating to criminal convictions and offences.
- A systematic monitoring of a publicly accessible area on a large scale.

Special categories include - racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a person, data concerning health or data concerning a person’s sex life or sexual orientation.

The EU working party have also produced the following list of processing ‘likely to result in a high risk’:

- Evaluation or scoring
- Automated-decision making with legal or similar significant effect
- Systematic monitoring
- Sensitive data
- Data processed on a large scale
- Datasets that have been matched or combined
- Data concerning vulnerable data subjects
- Innovative use or applying technological or organisational solutions
- Data transfer across borders outside the European Union
- When the processing in itself “prevents data subjects from exercising a right or using a service or a contract”

If any of your data processing is (or is likely to be) high risk please refer to the ICO ‘Conducting privacy impact assessments code of practice’ guide.

Consent

The basic concept of consent, and its main role as one potential lawful basis (or condition) for processing, is not new and is currently included in the DPA. The GDPR sets a high standard for an individual’s consent to use their personal data building on the DPA standard of consent in several areas.

- Check your consent practices and your existing consents. Refresh consents if they don’t meet the GDPR standard.
- Consent means offering individuals genuine choice and control.
• Consent requires a positive opt-in. Don’t use pre-ticked boxes or any other method of consent by default.
• 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. Vague or blanket consent is not enough.
• Be clear and concise.
• Name any third parties 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 a precondition of a service.
• Public authorities and employers will find using consent difficult.
• Remember – you don’t always need consent. If consent is too difficult, look at whether another lawful basis is more appropriate.

If your current consents meet the DPA standard, you are not required to automatically ‘repaper’ or refresh your data. However, if existing DPA consents don’t meet the GDPR’s high standards or are poorly documented, you will need to seek fresh GDPR compliant consent, identify a different lawful basis for your processing (and ensure continued processing is fair), or stop the processing.

It is worth noting that consent is only one of the five ‘lawful basis for processing personal data’ and if you have difficulty meeting the consent standard you may be better looking at another lawful basis.

Lawful Basis
There are five types of ‘lawful basis for processing personal data’ under the GDPR and you should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

The five types are:

• **Consent from the individual**: See consent section.

• **A contract with the individual**: for example, to supply goods or services they have requested, or to fulfil your obligations under an employment contract. This also includes steps taken at their request before entering into a contract.

• **Compliance with a legal obligation**: if you are required by UK or EU law to process the data for a particular purpose, you can.

• **Vital interests**: you can process personal data if it’s necessary to protect someone’s life. This could be the life of the data subject or someone else.

• **A public task**: if you need to process personal data to carry out your official functions or a task in the public interest – and you have a legal basis for the processing under UK law – you can. If you are a UK public authority, our view is that this is likely to give you a lawful basis for many if not all of your activities.
• **Legitimate interests**: if you are a private-sector organisation, you can process personal data without consent if you have a genuine and legitimate reason (including commercial benefit), unless this is outweighed by harm to the individual’s rights and interests.

**Private-sector organisations will often be able to consider the ‘legitimate interests’ basis, if they find it hard to meet the standard for consent and no other specific basis applies. This recognises that you may have good reason to process someone’s personal data without their consent – but you must ensure there is no unwarranted impact on them, and that you are still fair, transparent and accountable.**

**Children**

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.

For the first time, the GDPR will bring in special protection for children’s personal data, particularly in the context of commercial internet services such as social networking. If your organisation offers online services (‘information society services’) to children and relies on consent to collect information about them, then you may need a parent or guardian’s consent in order to process their personal data lawfully.

The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger then you will need to get consent from a person holding ‘parental responsibility’. 
Breach Notification

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

Currently some organisations are already required to notify the ICO when they suffer a personal data breach. The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals.

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, for example, 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 ICO 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.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases. You should put procedures in place to effectively detect, report and investigate a personal data breach.

You may wish to assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred.

Failure to report a breach within 72 hours of being aware, when required to do so could result in a fine, as well as a fine for the breach itself.
Protecting Data

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.

While the fine of 4% of annual revenue or €20 million (whichever is higher) for non-compliance of GDPR is widely publicised, this is the maximum fine possible. It is up the National Data Protection Authorities (NDPAs), in our case the ICO to issue the fine and they will take into account what steps you have try and meet GDPR compliancy and the rather vague term ‘special considerations for SMEs’ included in GDPR which is still to be defined.

On an organisational level, you should look at what data you store and how you process it, as detailed previously in this document.

With regard to Technical Measures the best solution for SMEs is to meet the ICO’s own IT security recommendations contained in its ‘A practical guide to IT security - Ideal for the small business’. Which includes the following 10 recommendations:

- Assess the threats and risks to your business
- Get in line with Cyber Essentials
- Secure your data on the move and in the office
- Secure your data in the cloud
- Back up your data
- Train your staff
- Keep an eye out for problems
- Know what you should be doing
- Minimise your data
- Make sure your IT contractor is doing what they should be

Assess the threats and risks to your business
The ICO recommends that review your personal data you hold and assess the risks to that Data. This is also a requirement of GDPR (see Documentation).

Also audit your end users devices to for any unauthorised software (shadow ware) or data, which they be using.

Get in line with Cyber Essentials
Cyber Essentials is a government-backed cyber security certification scheme that sets out a good baseline of cyber security suitable for all organisations in all sectors. The scheme addresses five key controls that, when implemented correctly, can prevent around 80% of cyber-attacks.

The government requires all suppliers bidding for certain sensitive and personal information handling contracts to be certified against the Cyber Essentials scheme. Also, a number of insurance organisations are offering incentives for businesses who are certified.

Cyber Essentials certification requires implementation of the five following controls and completion of a comprehensive questionnaire, followed by an external vulnerability scan and normally costs around £300.
1. Boundary firewalls and internet gateways
This will be your first line of defence against an intrusion from the internet. A well configured firewall can stop breaches happening before they penetrate deep into your network. An internet gateway can prevent users within your organisation accessing websites or other online services that present a threat or that you do not trust.

2. Secure configuration
Almost all hardware and software will require some level of set-up and configuration in order to provide the most effective protection. You should remove unused software and services from your devices to reduce the number of potential vulnerabilities. Older versions of some widespread software have well documented security vulnerabilities. If you don’t use it, then it is much easier to remove it than try to keep it up-to-date. Make sure you have changed any default passwords used by software or hardware – these are well known by attackers.

3. Access control
Restrict access to your system to users and sources you trust. Each user must have and use their own username and password.

Each user should use an account that has permissions appropriate to the job they are carrying out at the time. You should also only use administrator accounts when strictly necessary (e.g. for installing known and trusted software).

A brute force password attack is a common method of attack, perhaps even by casual users trying to access your Wi-Fi so you need to enforce strong passwords, limit the number of failed login attempts and enforce regular password changes.

Passwords or other access should be cancelled immediately if a staff member leaves the organisation or is absent for long periods.

4. Malware protection
You should have anti-virus or anti-malware products regularly scanning your network to prevent or detect threats. You will also need to make sure they are kept up-to-date and that it is switched on and monitoring the files that it should be. You should also make sure you receive and act upon any alerts issued by the malware protection.

5. Patch management and software updates
Computer equipment and software need regular maintenance to keep it running smoothly and to fix any security vulnerabilities. Security software such as anti-virus and anti-malware needs regular updates in order to continue to provide adequate protection.

Keep your software up-to-date by checking regularly for updates and applying them. Most software can be set to update automatically.

If your system is a few years old, you should review the protection you have in place to make sure that it is still adequate.

Secure your data on the move and in the office
The physical security of equipment is important to consider as devices containing personal data could be stolen in a break-in at your office. You should ensure that personal data on your systems is protected against these types of threats.

You also need to ensure that the same level of security is applied to personal data on devices being used away from the office. Many data breaches arise from the theft or loss
of a device (e.g. laptop, mobile phone or USB drive) but you should also consider the security surrounding any data you send by email or post.

As well as physical security, you should consider which users need to have access to personal data and secure this data so only these users can access it.

Encryption is a means of ensuring that data can only be accessed by authorised users. Typically, a (strong) password is required to ‘unlock’ the data.

Secure your data in the cloud
Processing data in the cloud represents a risk because the personal data for which you are responsible will leave your network and be processed in those systems managed by your cloud provider. You therefore need to assess the security measures that the cloud provider has in place to ensure that they are appropriate.

Make sure you know what data is being stored in the cloud as modern computing devices and services, especially those targeted at consumers, can have cloud backup or sync services switched on by default.

Consider the use of two factor authentication especially for remote access to your data in the cloud.

If you permit employees or other users to connect their own devices to your network you will be increasing the range of security risks and these should also be addressed.

Back up your data
Loss of personal data is also treated as a breach of GDPR.

You need to have a robust data backup strategy in place to protect against disasters but also malware, such as ransomware. At least one of your back-ups should be off-site.

Train your staff
Your employees may have a limited knowledge of cyber security but they could be your final line of defence against an attack. Accidental disclosure or human error is also a leading cause of breaches of personal data. This can be caused by simply sending an email to the incorrect recipient or opening an email attachment containing malware.

Employees at all levels need to be aware of what their roles and responsibilities are. Train your staff to recognise threats such as phishing emails and other malware or alerting them to the risks involved in posting information relating to your business activities on social networks.

Keep an eye out for problems
Cyber criminals or malware can attack your systems and go unnoticed for a long time. Many people only find out they have been attacked when it is too late even though the warning signs were there.

Check your security software messages, access control logs and other reporting systems you have in place on a regular basis. You should also act on any alerts that are issued by these monitoring services.
Run regular vulnerability scans and penetration tests to scan your systems for known vulnerabilities – make sure you address any vulnerabilities identified.

**Know what you should be doing**

A good policy will enable you to make sure you address the risks in a consistent manner. Well written policies should integrate well with business processes.

Some organisations do not have adequate levels of protection because they are not correctly using the security they already have, and are not always able to spot when there is a problem. You should also consider what actions you should put into place should you suffer a data breach. Good incident management can reduce the damage and distress caused to individuals.

**Minimise your data**

Personal data should be accurate, up-to-date and kept for no longer than is necessary. Over time you may have collected large amounts of personal data. Some of this data may be out-of-date and inaccurate or no longer useful.

If you have data you need to keep for archive purposes but don’t need to access regularly, move it to a more secure location. This will help prevent unauthorised access.

If you have data you really no longer need, you should delete it. This should be in line with your data retention and disposal policies. You might need specialist software or assistance to do this securely.

**Make sure your IT contractor is doing what they should be**

Many small businesses outsource some or all of their IT requirements to a third party. You should be satisfied that they are treating your data with at least the same level of security as you would.
MT Services

MT Services provide several services which help you protect your data and get in line with Cyber Essentials guidelines, these include:

- SonicWall Gateway Firewalls and Security Services
- Eset Endpoint Antivirus/Antimalware Security
- MailProtect Managed Antispam
- Deslock Endpoint Encryption
- Server/Workstation Monitoring
- Server/Workstation Patch Management
- Email Data Loss Protection
- Managed Online Backup (with Archive)

Further resources from the ICO, HM Government & the EU are available at www.mtservices.co.uk/gdpr