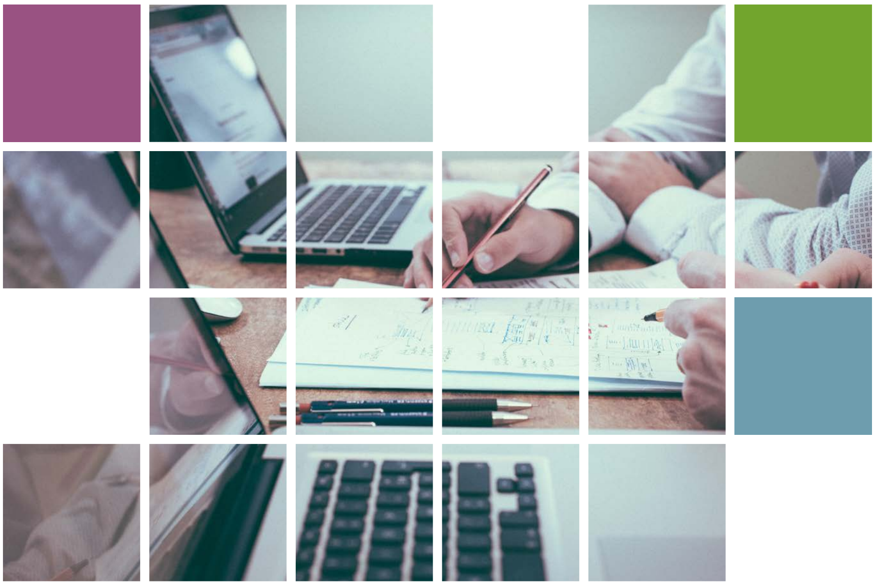
The essential guide to

GETTING YOUR BUSINESS READY FOR GDPR

With **new GDPR rules** coming into force in May, it's imperative you understand how your IT systems and processes are affected.

Read our essential guide to the new GDPR rules to find out what action you need to take to ensure your business is ready.



1010
ten ten
systems

A new way to handle data

The EU's General Data Protection Regulation (GDPR) comes into force on 25th May 2018. While it has much in common with the current UK Data Protection Act 1998 (DPA), GDPR standardises legislation across all EU member states. Even though Britain is due to exit the EU in March 2019, this legislation cannot be ignored as the UK government has suggested it intends to implement equivalent GDPR rules post-Brexit.

What is GDPR?

GDPR has been driven by the new ways in which data is now collected and used and aims to give people more control over what companies can do with their data.

It applies to any business which holds personal information such as names, addresses, telephone numbers, email addresses, payment information and even online identifiers such as IP addresses. The rules apply to small and large businesses, and you may find that firms you contract with begin to include GDPR compliance in their terms and conditions.

Being prepared

Your organisation will need to take particular actions to safeguard and manage information in accordance with the rules. There are things you need to do to protect data and ensure it is secure, and you must have efficient and effective procedures in place to perform particular actions upon request, such as amend or delete records. In addition, you must follow specific procedures to report and rectify data breaches.

If you haven't yet prepared for GDPR, you need to begin as soon as possible as the penalties for non-compliance are severe.

Early GDPR compliance will send the right message to your customers, helping to give you competitive advantage and protecting your reputation. You need to get ahead of the curve, otherwise you put your business at risk of enforcement action which could cost you dearly.

Steve Birks
Managing Director
Ten Ten Systems

The principles of GDPR

The foundation of the GDPR legislation is a list of rights which people will have in relation to the personal information organisations store. Understanding these rights is key to preparing your business.

Right to be informed

This deals with how transparent you are with the use of personal data. It includes aspects such as retention period, the right to withdraw consent at any time, the source the personal data originates from and whether it came from publicly accessible sources.

Right of access

Individuals will need to have access to the personal data you hold about them. Businesses must provide a copy of the information free of charge though you can charge a 'reasonable fee' when a request is 'manifestly unfounded or excessive, particularly if it is repetitive'. Information must be provided at the latest within one month of receipt.

Right to rectification

Individuals can have personal data rectified if it is inaccurate or incomplete. If you have passed information to other organisations you will need to inform them of the need to rectify any inaccuracies. You must respond within one month of a request for rectification and where you are not taking action you must explain the reasons why and ensure the person concerned is aware of their right to complain.

Right to erasure

The right to erasure enables an individual to request the removal of personal data where there is no compelling reason for your organisation to continue using it, or where the individual withdraws consent.

You can refuse to comply with a request for erasure under particular circumstances, for example, where personal data is processed to exercise the right of freedom of expression and information; for public health purposes in the public interest or the exercise or defence of legal claims, among others.

Right to restrict processing

An individual will have the right to restrict the processing of personal data which would mean you could store it but not further process it.

Right to data portability

This allows individuals to obtain and re-use their personal data for their own purposes across different services. It allows people to move, copy or transfer personal data easily from one IT environment to another safely and securely.

Right to object

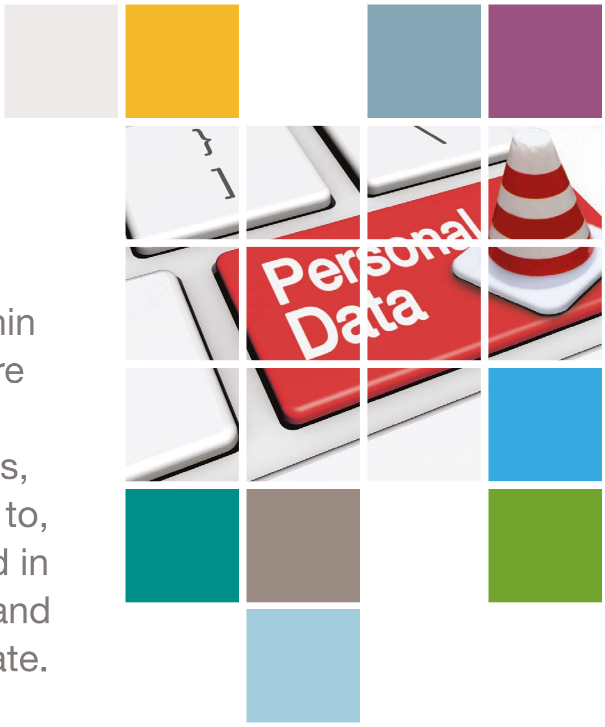
Individuals can object to data handling issues such as direct marketing and the processing of data for purposes of research and statistics. In these circumstances you must stop processing the personal data unless you can demonstrate compelling grounds for processing or if you are processing the data for legal reasons.

Rights related to automated decision-making

GDPR impacts automated individual decision-making and profiling (where there is no human involvement). There are specific criteria which you must adhere to with automated decision-making and profiling and, if applicable, your organisation must introduce simple ways for individuals to request human intervention and carry out regular checks to make sure that your systems are working as intended.

Handling a data breach

GDPR means all organisations have a duty to report certain types of personal data breach within 72 hours of becoming aware of the breach, where feasible. A personal data breach is defined as 'a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'. This applies to data which is held in electronic form as well as paper-based records and covers breaches that are accidental and deliberate.



The ICO cites examples of data breaches as:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

Reporting

GDPR requires you to report breaches to the ICO if they are likely to result in a risk to the 'rights and freedoms' of individuals. This covers breaches which may result in emotional distress and physical and material damage.

On becoming aware of a breach, your organisation will need to take action to contain it and assess the potential consequences. You must report a notifiable breach to the ICO within 72 hours of knowing about it.

Your report should detail:

- A description of the nature of the personal data breach.
- The name and contact details of the data protection officer (if you have one) or other contact point.
- A description of the likely consequences of the breach.
- A description of the measures taken or proposed to be taken to deal with the breach.

You need only report the breach to the individual(s) concerned if there is a 'high risk' to their rights and freedoms. It's important to keep records of all breaches, whether or not they are reported.

Penalties

The penalties for non-compliance are severe. Failure to notify the ICO of a breach when required to do so can result in a fine up to 10 million euros or 2% of global turnover.

Becoming GDPR compliant – step-by-step

Your IT systems and business processes are central to GDPR compliance. Our team of experts can help you understand what action you need to take before the new laws are introduced. Here's an overview of the key areas to focus on.

Keep records of all personal data collected

You need to keep accurate records of all the personal data you collect. The Information Commissioner's Office defines personal data as 'any information relating to an identifiable person who can be directly or indirectly identified in particular reference to an identifier'.

Take action

- Do an audit of the information you collect.
- Make sure you collect only the information you need to provide the goods/services you sell.
- Put in place a system to track the information over time, including information you may have archived or kept as back-up. You need to be able to delete data after it is no longer required.

> The information lifecycle within your organisation is key. Personal data, the definition of which is very broad under GDPR, is pervasive, so tracking it throughout the organisation is imperative. Personal data is also durable, so keeping tabs on it over time is also essential. This includes back-up copies of data, which may be stored off-site and offline. Data retention policy should be part of this as data needs to be deleted after it is no longer required.
>
> **Trevor Scanlon**
> Operations Director
> Ten Ten Systems Limited

Becoming GDPR compliant – step-by-step

Remember third parties

When reviewing what information is held and where, it's important to remember that third parties may hold information on your behalf. For example, there may be data implications for your web host, offsite backup storage and cloud data storage, among others.

Take action

- Special consideration should be given to any data not directly stored on your own local network.
- Check the network security systems and processes of any third parties who hold your data to ensure GDPR compliance.

Can you prove consent?

Your firm will need to have an audit trail to be able to prove that consent was given by the individual for the processing of data, for example, when using their email address for marketing purposes. Because GDPR rules state that consent must be 'unambiguous' when given, it's important to distinguish that individuals will need to actively give their consent – it's no longer sufficient to have a pre-ticked box. Consent must also be presented separately so that it doesn't get 'hidden' with other statements or documentation, or small print on your contracts or website.

Take action

- Check your consent practices and ensure they meet GDPR standards. You must have a positive opt-in and be specific so that you get separate consent for separate things.
- Review historical records and request consent where necessary. Make sure you keep evidence of consent.
- Make it easy for people to withdraw consent.

Build data protection into business as usual

You need to ensure your business is compliant now and into the future, so it will save time and effort, and reduce your risk, if GDPR-compliant data collection and storage practices become business as usual.

Businesses will need to document what personal data they hold and be clear on where the information came from, where it is held and who has access to it.

Take action

- Ensure you have the right IT systems in place to allow you to maintain customer records without the task becoming too onerous for your teams.
- Ensure you can retrieve information easily and ensure only appropriate employees have access to relevant data.
- Create an audit trail to show when records are added, altered or removed.

Under the rights to rectification and erasure, also known as the right to be forgotten, data subjects can demand data is corrected or removed, which means organisations must know the locations of all instances of personal data. While the right to erasure is not absolute, organisations must know when and to what extent data should be erased.

IT teams, therefore, find themselves at the sharp end of facilitating compliance with some of the most technically challenging aspects of GDPR.

Prepare for data security breaches

Part of your overall business readiness should involve preparing for data security breaches. It's imperative that your employees understand what constitutes a breach and that you have an effective procedure for reporting and rectification.

Take action

- Provide adequate training and refresher training for all employees.
- Put together a plan for managing a security breach.
- Ensure employees feel able to report security breaches which have arisen from mistakes.

> It could be very easy for an employee to make a note of a customer name and address in a Word document and save it to their local network, not considering that this data falls under GDPR. The data controller would have no way of knowing this data exists so could not appropriately action a request to be forgotten or changed. Managing the location of all this data must be clearly defined to all staff and ensuring full awareness of the requirements of GDPR to employees is vital.
>
> **Trevor Scanlon**
> Operations Director
> Ten Ten Systems Limited

Put GDPR at the forefront of decision-making

Organisations must implement 'appropriate technical and organisational measures' that support data protection principles. Importantly, this includes 'at the time of the determination of the means for processing' – in other words, data protection must be considered at process conception.

This is the principle of data protection by design and by default. In addition, companies are obligated to 'take into account state-of-the-art' in designing and executing their data protection responsibilities, which raises the questions: what is state-of-the-art? Who decides? And how often should organisations review their position?

Take action

- Ensure someone within your organisation is tasked with maintaining ongoing awareness and knowledge of IT technology and how it may be used within your company to support GDPR compliance, or work with us to protect your business.
- Rectify any ageing and/or undocumented IT systems, especially in combination with the requirements of data protection by design and by default.

No two businesses are the same so it's important to conduct a thorough audit at the outset to identify any gaps and to put together a detailed action plan to ensure you are prepared. You may also need to appoint a member of staff to specifically look at this issue.

Review your IT security

Whilst the specific areas of GDPR will vary slightly from company to company, almost all firms will need to look closely at compliance in the following IT-related areas:

- **Perimeter** – the first point of contact your network has with the outside world, usually a robust firewall. Check that your firewall provision is adequate.
- **End point** – it's imperative to have adequate End Point protection on computers to detect viruses, malware and other threats. Many methods of stealing data are triggered by viruses infecting computers, so preventing this should be a high priority.
- **Encryption** – data encryption is hugely beneficial to ensuring that data cannot be accessed should a security breach occur. Methods can be implemented to ensure only devices with the permissions to open the file will ever view its contents.
- **Email security** – when you consider that over half the email received globally is spam, it's little wonder that email security is an issue. Email security and other methods of spam prevention such as SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) should be explored.
- **Secure Remote Access** – if you have remote workers you need to ensure their connection to your network is secure.
- **Disaster recovery/backups** – hopefully this issue has already been addressed but you now need to look at how that data is stored when you have backed it up. If it's offsite, then what security measures are in place at the data centre? If you backup to tape, where do you store that tape for GDPR compliance?

1010 ten ten systems

Providing IT with intelligence

Let us help you protect your business

Your IT systems are central to GDPR compliance and our expert team can help you to be prepared.

For more information please contact us either by phone or email using the details below.

Further information

We will provide regular updates on GDPR via our website and email newsletter. Visit our blog or sign up to receive our monthly email newsletter.

The Information Commissioner’s Office also provides comprehensive information on all aspects of GDPR.

Ten Ten Systems Ltd
4 Abbey Square, Chester, CH1 2HU

t +44 (0)1244 408990
e info@1010systems.co.uk

www.1010systems.co.uk

HIKVISION

Microsoft Partner
Gold Midmarket Solution Provider
Gold Devices and Deployment

DELL

SONICWALL