GDPR OVERVIEW

A Midland Tech Guide to GDPR and Data Security

PURPOSE OF THIS GUIDE

With the May 25th deadline fast approaching, many businesses still aren't ready for it. This guide aims to help you prepare for the introduction of GDPR, and in particular looks at the technical measures you should be taking to protect your data.

In addition to GDPR, the recent explosion in cybersecurity threats such as ransomware and phishing scams mean that **businesses need to be taking data protection more seriously than ever before**.

It is important to point out that the May 25th date for the introduction of GDPR doesn't mean that you have to be completely ready for it by then, what is important is that **you have acknowledged the requirements and that you are committed to an ongoing plan** to implement technical and procedural improvements. In short, you need to demonstrate that you are at least making progress by that date.

WHAT IS GDPR?

The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union. It replaces the current 1998 Data Protection Act, and will still be a requirement even when the UK has left the EU.

Any organisation holding personal data on EU subjects will fall under the regulation, and some examples of personal data are:

- Personal information like names, birthdates, and physical addresses
- Digital identifiers like email addresses, IP addresses, MAC addresses, and passwords
- Financial information like bank accounts and card details
- Location information such as GPS locations or social media check-ins
- Medical records like doctor visits, medication lists, and medical histories
- Legal or Government records

Basically, if a piece of information can be used to identify an individual, you must secure that data under the new law.

OVERVIEW OF GDPR

The main principles of GDPR require that personal data shall be:

- **Processed lawfully**, fairly, and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Accurate and kept up to date
- Kept for no longer than is necessary
- Processed in a manner that ensures appropriate security of the personal data, using **appropriate technical or organisational measures**

A **Data Controller** determines the purposes and means of processing personal data.

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

Additionally some organisations also need a **Data Protection Officer**, an expert in data privacy, though this rarely occurs in small businesses.

LAWFUL BASIS FOR PROCESSING

You must have a valid lawful basis in order to process personal data. There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual. The six bases are:

- **Consent.** Consent requires a positive opt-in, don't use pre-ticked boxes or any other method of default consent. Consent can be difficult to obtain, and easily withdrawn, so shouldn't be relied upon as the primary basis for processing.
- **Contract.** You can rely on contractual basis if you need to process their data in order to fulfil your contractual obligations to them (e.g. customer or supplier), or because they have asked you to do something before entering into a contract (e.g. provide a quote).
- **Legal Obligation.** You can rely on this lawful basis if you need to process the personal data to comply with a common law or statutory obligation (e.g. An employer needs to process personal data to comply with its legal obligation to disclose employee salary details to HMRC).
- **Vital Interests.** You are likely to be able to rely on vital interests as your lawful basis if you need to process the personal data to protect someone's life.
- **Public Task.** This is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest.
- **Legitimate Interests.** This is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate. It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact.

RIGHTS OF THE INDIVIDUAL

The individual for whom you hold personal data has a number of rights, as follows:

- **Right to be informed.** You must provide individuals with information including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with.
- **Right of access.** Individuals have the right to access their personal data and supplementary information.
- **Right to rectification.** This is the right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.
- **Right to erasure.** Also known as 'the right to be forgotten', individuals can request to have their personal data erased. However, this right is not absolute and only applies in certain circumstances (e.g. the right does not apply if processing is required to comply with a legal or statutory obligation).
- **Right to restrict processing.** Individuals have the right to request the restriction or suppression of their personal data. Again, this is not an absolute right and only applies in certain circumstances.
- **Right to data portability.** This allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- **Right to object.** Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority; direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.

DATA SECURITY AND TECHNICAL MEASURES

A key principle of the GDPR is that you process personal data securely by means of 'appropriate technical and organisational measures'. The exact measures required will vary from one organisation to another, and costs of implementation must be assessed against risk when deciding which measures are appropriate for your organisation.

However, we believe **there are basic measures which every organisation should either have or plan to introduce**, as set out on the following pages.

Locate All Personal Data

Personal data is likely to be spread across the organisation, hidden in databases, spreadsheets, legacy systems, and old devices for example.

The first step is to **identify and document all personal data**, where it is stored, on what basis it is being processed, and how it is secured. This goes beyond security, you can't comply with data access or erasure requests if you're unaware of all data that exists on your systems for a data subject.

Document Everything

You need to **make sure you have an audit trail**, after a data breach (which must be reported within 72 hours of discovery) the authorities will look for evidence that the organisation made good faith efforts to protect personal data. This includes documentation of the data itself, what steps you have taken (or plan to take) to protect the data, security and privacy policies, access rights, how long you propose to keep the data for, and evidence that you have provided data privacy and security training to employees.

User Security Training

Data breaches often start with employees making mistakes such as downloading malicious software or being caught by a phishing email. Your IT or training provider should be able to provide **ongoing training and awareness programs for your staff**.

Layered Security Strategy

These days, cybercriminals have many ways to compromise a company's security and breach their data. Whether it's exploit kits, denial of service attacks, ransomware, phishing, or social engineering, the bad guys have a slew of weapons to choose from to cause mayhem. You shouldn't rely on any one technology to protect your data, but rather a multi-layered approach including the following:

- **Encrypt** all mobile devices, including laptops, tablets and phones.
- Lock down **user permissions** and admin access.
- Track mobile devices and **remotely lock or wipe** any stolen or lost devices.
- Ensure all **anti-virus and anti-malware software** is running and up to date.
- **Patch and update all software systems**, including Microsoft Windows.
- **Backup data** on a regular basis, and test those backups for effectiveness.
- Introduce **email security** to help prevent viruses, spam and phishing attempts.
- Consider a dedicated firewall with security services, to **protect your network**.
- Write and follow an **IT Security Policy**.
- Get a Government-backed certificate such as **Cyber Essentials**.

WHERE TO GO FROM HERE

As mentioned previously, by May 25th you should have a plan to implement technical and organisational measures. You will need to do the following:

- Awareness. Decision makers and key people should be made aware of GDPR and the likely impact in your organisation.
- Information Held. You should document what personal data you hold, where it came from, and who you share it with.
- Communication. You should review your current privacy notices and put a plan in place to update these.
- Individuals' Rights. You need procedures to cover the rights of individuals, including how you would delete data.
- Lawful Basis. The lawful basis for processing all data should be identified, documented and included in your privacy notice.
- Data Breaches. You should make sure you have the right procedures in place to detect, report and investigate a data breach.
- Technical Measures. You should review and implement 'appropriate' technical measures in conjunction with your IT Service Provider.

WHAT MIDLAND TECH CAN PROVIDE

Although we have put together this general guide, our strength lies in the technical measures required to protect your organisation from cybercrime. We provide all of the multiple layers of security mentioned above, as well as ongoing user training centred around phishing emails.

All of our services are fully managed, leaving you free to concentrate on your business. For a full assessment of your current and future cybersecurity requirements, get in touch with us today.