Is Your Business GDPR READY?

Understanding the new privacy law and how it affects your business

FLAG Computer Repair

It’s the biggest change to the digital world since the 1990s and it came in with a storm of uncertainty.

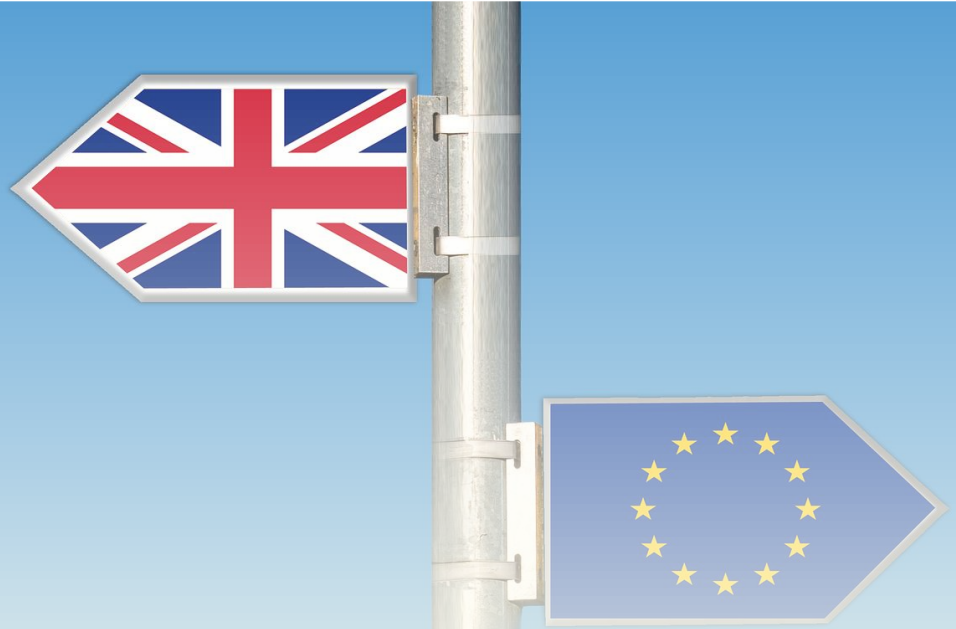
The **General Data Protection Regulation (GDPR)** is a new set of laws designed to control how companies use their personal details, and there’s a strong chance it will affect your business. This ebook explores the GDPR from a global small/medium business perspective, including what you need to do to stay compliant and avoid penalties.

The Bare-bones Version

- GDPR is a set of stronger privacy & data protection laws
- Many think it's only important for those in Europe (false)
- Business across the world must be compliant
- You'll need to review your privacy policy & set of practices
- Hefty penalties apply for breaches
- Came into effect on 25th May 2018

GDPR applies to you if:

1. You have an establishment in the EU, regardless of where you process your data. That could mean your website or email is handled by a US host, but because you/your business is located in the EU, the new laws apply.
2. You do NOT have a business in the EU, but you offer goods and services to people in the EU. These could be physical or digital goods, plus in-person or remote services.
3. You do NOT have a business in the EU, but your database may include details of people from there, or you monitor their website browsing using cookies etc. Even using basic analytics on your website means you may tick this box.
4. So, whether you're a 'one-person band' or Apple you fall within the remit of GDPR.



The ‘Brexit’ Complication

For those businesses in the UK breathing a sigh of relief, be advised the GDPR will continue to apply as it’s already been written into UK law.

You’re not alone. For many countries, the protections offered by GDPR will either supersede or complement state/national/industry policies. Many countries are currently updating their own privacy laws to reflect the GDPR changes, especially regarding breach disclosure and consent.

Laws came into effect 25th May 2018

How this affects businesses like yours

The new laws were designed to pull the US tech giants like Facebook and Google into line, stopping them from cashing in on private data without consent. While most people were more than happy to see individual rights protected, it's had a restrictive effect on small business and sole traders.

We're hearing a lot of concern that becoming and staying compliant will cost unnecessary time and money, particularly as you've historically been doing all the right things. As a small business though, your agility is an advantage. With this ebook, you'll be able to narrow in on the changes you need, skip the ones you don't, and maintain compliance without large investment or inconvenience.

Rather than view the new laws as a negative, consider them as a clear guide to keeping your customer's trust.

Private data has been expanded

You're accustomed to protecting your customer's private data, such as name, address and billing details. Under the GDPR changes, the definition of private data has been expanded to include internet browsing habits collected by website cookies, location data, other online identifiers and genetic data.

Consent must be explicit

Under GDPR, **consent needs to be explicit** - and provable. This means you can't send cold emails to drum up business anymore, nor can you add friends/family to your database or that lead you bumped into while fetching coffee.

Cold email marketing will be a breach

Silence, pre-ticked boxes or inactivity are not considered consent. Simple changes will bring your business into compliance, such as having customers intentionally tick a box to receive newsletters, or using clear form text so individuals know what they're agreeing to.

More specific requirements apply in relation to consent from children under 16.

Cookies and analytics usage will change

Many business websites use cookies and analytics by default. Under GDPR, you'll need to lead with explicit consent. This means asking users to opt-in for cookies (no more 'by using this site you accept cookies' notices), and ensuring any data is pre-emptively stripped of all personal identifiers before being sent to your analytics tool.

Individuals have a right to be forgotten

While the standard ‘unsubscribe’ link has been law for some time now, GDPR expands this to include a right to erasure. Individuals can ask to be completely deleted, not just unsubscribed.

You’re required to confirm and delete their personal data, plus take steps to ensure any copies or backups containing their data are also treated.

Mandatory breach reporting within 72 hours

As a result of all those data leaks we’ve heard about where the company has kept it secret for as long as possible, all breaches must be reported within 72 hours.

You’ll need to advise your relevant supervisory authority unless the breach was so minor that no private data was accessed. If the breach is likely to result in the individual being placed at any amount of risk, you’ll need to notify authorities, plus the individuals in question.

Penalties Are Severe

GDPR takes the protection of Personally Identifiable Information (PII) very seriously. If you're caught being non-compliant, expect a financial penalty of up to 20 million Euros (approx. £ 17.6million), or 4% of annual turnover, whichever is greater.

Whether it's an employee mistake or external hack, the owner of the business is the one who pays. Add in the negative publicity and brand damage, and the costs of non-compliance can be catastrophic.

How You Can Protect Yourself

To help meet GDPR compliance, we recommend a triple action approach.

1. Review your privacy policies, data collection and marketing methods
2. Educate employees, embedding good practice into business culture
3. Engage remote monitoring and management services

Monitoring allows us to provide instant notification of problems or changes in status across workstations, plus remote computers. You'll receive alerts when critical services go down, when your employees and users alter their configurations, or when a possible security breach occurs.

It's Time to Get Prepared

GDPR is here, and its impact is significant for any businesses that handle the data of UK/European citizens. As more countries pick up the stricter controls, these are changes you'll have to make soon, even if you're not directly impacted by GDPR yet.

Businesses need to start getting prepared now — if they haven't already.

By deploying the following effective solutions, you can help ensure that you are compliant with GDPR. At the same time, we can strengthen your defences against the growing array of security threats.

Who is responsible?

The responsibility of protecting PII falls on all the employees in a business so when we refer to you take it to mean all employees.

You are responsible for your customers/clients PII. So, whether you write it down in the pages of your notebook or store it within the deep beyond of the Apple international servers, if there is a breach the regulator will be coming to ask you what you did to protect your customer data. When you use suppliers and they hold PII, it is your responsibility to find out how they protect your customer data. If your supplier has a breach you are still responsible for your customers data.

Be mindful of where your customer PII is stored. Within the premises you conduct business is obvious but don't forget, those employee laptops, tablets, smartphones, USB sticks and Cloud storage. They are designed to make a more mobile workforce, but they create a security nightmare.

So how are you going to protect that data.

We are focusing on the cyber security side of protection but bear in mind the physical protection required for premises and devices.

You are only allowed to hold data for as long as you need it and the data you hold must be kept securely.

Before you go deleting all your customer PII to rid yourself of the problem, remember that there may be legal reasons why you need to hold onto the data. For example, in the UK, HMRC requires us to hold records for 5 years. Medical records can be held for longer. These requirements supersede the GDPR requirement.

Encryption

The first thing you should consider is encryption. This helps the most because if you do suffer a breach the encrypted data is inaccessible.

All modern Apple computers and devices come with encryption installed. Has it been setup yet?

If you have a modern professional version of Windows, then you have encryption installed. Not only does it protect the computer, but it can also protect external hard drives and USB sticks. Has it been setup yet?

If you have a home version of Windows, then you need to upgrade to professional to get encryption. In addition, you also get the added advantage that you can defer windows updates as well.

Remember that if you store your PII data or backups of your PII data on external drives or in the cloud then that must be encrypted as well. It goes without saying that you should be backing up your business data. How would your business cope if you lost all your client and supplier records! Windows backup is not encrypted so unless the drive or cloud storage area your using is encrypted then all your data is in open view of hackers.

Firewall

You should protect your Internet connection with a firewall. This effectively creates a ‘buffer zone’ between your IT network and other, external networks.

In the simplest case, this means between your computer (or computers) and 'the Internet'. Within this buffer zone, incoming traffic can be analysed to find out whether or not it should be allowed onto your network.

You could use a personal firewall on your internet connected laptop (normally included within your Operating System at no extra charge).

Or, if you have a more complicated set up you might require a dedicated boundary firewall, which places a protective buffer around your network as a whole.

Some routers will contain a firewall which could be used in this boundary protection role. But this can't be guaranteed – if you can, ask your internet service provider about your specific model.

Passwords

Your laptops, desktop computers, tablets and smartphones contain your data, but they also store the details of the online accounts that you access, so both

your devices and your accounts should always be password-protected.

Passwords - **when implemented correctly** - are an easy and effective way to prevent unauthorised users accessing your devices. **Passwords should be easy to remember and hard for somebody else to guess**. The default passwords which come with new devices such as 'admin' and 'password' are the easiest of all for attackers to guess.
So you must change all default passwords before devices are distributed and used. The use of PINs or touch-ID can also help secure your device.

For 'important' accounts, such as banking and IT administration, you should use two-factor authentication, also known as 2FA. A common and effective example of this involves a code sent to your smartphone which you must enter in addition to your password.

Control who has access

To minimise the potential damage that could be done if an account is misused or stolen, staff accounts should have just enough access to software, settings, online services and device connectivity functions for them to perform their role. Extra permissions should only be given to those who need them.

Check what privileges your accounts have - accounts with administrative privileges should only be used to perform administrative tasks.

Standard accounts should be used for general work. By ensuring that your staff don't browse the web or check emails from an account with administrative privileges you cut down on the chance that an admin account will be compromised.

This is important because an attacker with unauthorised access to an administrative account can be far more damaging than one accessing a standard

user account.

Another simple and effective way to ensure your devices stay secure and malware-free is to only use software from official sources.

The easiest way to do this is to only allow your users to install software from manufacturer approved stores, which will be screening for malware. For mobile devices, this means sources such as Google Play or the Apple App Store.

Protect yourself from viruses & malware

Malware is short for ‘malicious software’. One specific example is ransomware, which you may have heard mentioned in the news. This form of malware makes data or systems it has infected unusable - until the victim makes a payment.

Viruses are another well-known form of malware. These programs are designed to infect legitimate software, passing unnoticed between machines, whenever they

can.

There are various ways in which malware can find its way onto a computer. A user may open an infected email attachment, browse a malicious website, or use a removable storage drive, such as a USB memory stick, which is carrying malware.

Anti-malware measures should be used on all computers and laptops. Smartphones and tablets should be kept up to date, password protected and where possible, you should turn on the ability to track and erase lost devices. If you can avoid connecting to unknown wi-fi networks, this will help to keep your devices free of malware too.

Whitelisting can also be used to prevent users installing and running applications that may contain malware. The process involves an administrator creating a list of applications allowed on a device. Any application not on this list will be blocked from running. This is a strong protection as it works even if the malware is undetectable to anti-virus software. It also requires

little maintenance.

Sandboxing. Where possible, use versions of the applications that support sandboxing. For instance, most modern web browsers implement some form of sandbox protection. A sandboxed application is run in an isolated environment with very restricted access to the rest of your device and network. In other words, your files and other applications are kept beyond the reach of malware, if possible.

Keep your devices and software up to date

No matter which phones, tablets, laptops, or computers your organisation is using, it's important they are always kept up to date. This is true for both Operating Systems and installed apps or software. Happily, doing so is quick, easy, and free.

Manufacturers and developers release regular updates

which not only add new features, but also fix any security vulnerabilities that have been discovered.

Applying these updates (a process known as patching) is one of the most important things you can do to improve security.

Operating systems, programs, phones, and apps should all be set to 'automatically update' wherever this is an option. This way, you will be protected as soon as the update is released.

However, all IT has a limited lifespan. When the manufacturer no longer supports your hardware or software and new updates cease to appear, you should consider a modern replacement.
Windows 7 became obsolete in January 2020; you should seriously consider changing to a more secure operating system as this is not compliant with GDPR
This guide isn't intended as a replacement for the regulations. They can be found in full at

https://ico.org.uk/

We provide cyber security services to small businesses to keep you compliant with GDPR & the NCSC Cyber Essentials Certification

TALK TO US TODAY
07976 151148

FLAG COMPUTER REPAIR

Phone: **07976 151148**

Email: **gary@flagcomputerrepair.co.uk**

Web: **http://www.flagcomputerrepair.co.uk**

Facebook: **www.facebook.com/flagcomputerrepair**