



GDPR Support For You

What Are The Hidden Dangers Of Non GDPR Compliance?

What Does GDPR Compliance Involve?

Is This Something You Feel Comfortable Doing Yourself?

Get Professional Help and Remove The Headache!

Compliance Checklist GDPR & Data Protection Act 2018

'Ignorance of the law excuses no one'

Correct - Protect - Secure - Safeguard



Are There Dangers For You In Not Being GDPR Compliant?

What Is Required To Have GDPR Completed For You?

See an outline below of the points showing you how to become GDPR compliant

Checklist follows below this introduction – be sure to read the end pages final concluding section

GDPR compliance became compulsory on the 25th May 2018. This is a potentially severe piece of regulation imposing a multitude of new liabilities and duties on business owners and other organisations that process personal data.

Most Businesses & Organisations Process Some Type of Personal Data

You may think you do not process personal data. If you are in business or indeed any type of organisation, there is a very strong chance that you do, in some way, process personal data. That means this law applies to you. The definition of 'processing personal data' is cast very widely.

Personal data is anything that can identify a 'natural person' and can include information such as a name, a photo, an **email address** (including work **email address**), bank details, posts on social networking websites, medical information or even an IP **address**.



You Are Legally Obligated to Keep Business Accounts & Now Privacy Records

In the same way that your business or organisation is obliged to keep accurate accounting records, you must now legally keep accurate privacy records, across various areas of your business.

The legislation was drafted with the aim of changing the 'culture' toward privacy and data protection in general. In this respect, it adds various obligations and duties that are backed up with penalties and enforcement provisions. The bar has been raised and the standards expected from business owners and organisations have risen considerably.

Ignorance of The Law

Most people are familiar with the legal principle that 'ignorance of the law is no excuse'. This age-old rule prevents individuals from avoiding prosecution by claiming that they did not know their conduct was illegal. Many business owners have tried to dismiss the new regulations as not applying to them. Do not make this mistake.

There are other potentially damaging blows that business owners face and no one is speaking about them yet. These implications are very real and potentially detrimental to business owners and organisations that are not aware of them.

Numerous business owners find themselves overlooking these new liabilities and how they genuinely and strictly affect their business over the immediate to long term.

While at first sight these regulations appear to be onerous, there can be advantages and benefits waiting to be gained. Weather by design or simply by default, GDPR in parts reflects a basic law of business and of nature.

Much has changed in the business landscape in recent years, especially with the way IT is now a central and crucial part of any business.

Ancillary To Data Privacy Are Your Own Business & Organisations Assets

Think about the most valuable asset in your business. Your business information and data, suppliers, customer records and many other details.

If this data was maliciously destroyed or criminally encrypted, so you could no longer use it, could your business or organisation still function?

Large scale cyber-attacks are not something that just large business needs to worry about. Hackers are on a daily mission, constantly probing websites, business networks and even computers in your home, looking for vulnerabilities.

The concern about this is very real. The news is full of Russian and other rogue states deliberately attacking installations, organisations and businesses vital to society. Attacks on small business and small business websites are just as prolific. According to Yell Business, some 30,000 websites are hacked every single day.

Double Purpose Protection

By examining the whole issue of data privacy, as proposed by the 'data privacy by design' principle in the GDPR, you will do yourself a massive favour by examining your overall business operations and your IT security. All businesses and organisations of every size can benefit from this.

Security that protects and secures not only an individual's data but also the general data held by your business. The data that is essential and necessary for your business or organisation to function correctly.

Security

If you are serious about data protection and security in your business or organisation, endpoint device encryption is one of the things that is highly recommended. It will provide a layer of security and will help you comply with privacy laws for all devices that hold any personal data – computers, laptops, tablets, mobile phones and removable storage devices.

Business Expenses Tax Deductible

Many business owners and organisations worry about the extra cost of legal compliance that GDPR will mean. The cost of securing your data is not an expense when you consider it. It is a 'business essential' and required if you wish to conduct business. In any event most business and organisations should find that the costs of compliance are a tax deductible business expense. Please confirm the position with your own accountant.

Do GDPR Yourself?

You can always use the checkpoints provided here to try and comply with GDPR & the Data Protection Act 2018 yourself. This is not impossible but let me say it can be complex.

The GDPR regulations are not entirely clear cut in all areas. It will to some extent depend upon the complexity of your business or organisation. What it will also do is add a layer of stress to your life that you can probably do without.

Creating the correct agreements, recording the correct things and understanding things like mandatory and required legal clauses, can mean your experience will feel much like taking time out to give yourself a full on legal training.

Interpreting how much of the regulations may apply to you and how to decide this are other factors that add to the headache.

Whichever route you chose, GDPR is a requirement that is here to stay.

*** Please read the following assessment GDPR checklist and the concluding statement at the end of the assessment.*

Are You Processing Personal Data		Yes	No
Understanding whether you are processing personal data is critical to understanding whether the GDPR applies to your activities.			
Personal data is information that relates to an identified or identifiable individual Does your business know what identifies an individual as defined under the terms of GDPR?		<input type="checkbox"/> <input type="checkbox"/>	
GDPR Applies To 'Controllers' And 'Processors'			
Does your business understand who has responsibilities under GDPR?		<input type="checkbox"/> <input type="checkbox"/>	
GDPR Defines Processing of Data			
Does your business understand what 'processing' of data is under GDPR?		<input type="checkbox"/> <input type="checkbox"/>	
Accountability Under GDPR			
Accountability is one of the data protection principles. You are responsible for complying with the GDPR. There are two key elements. First, the accountability principle makes it clear that you are responsible for complying with the GDPR. Second, you must be able to demonstrate your compliance. (See below)			
Enforcement Under GDPR & Data Protection Act 2018			
Action can be taken to change the behaviour of organisations and individuals that collect, use and keep personal information. This includes criminal prosecution, non-criminal enforcement, audit and potentially substantial fines.			

GDPR PRINCIPLES		Yes?	No?
Compliance with the spirit of these key principles is a fundamental building block under GDPR			
1. Lawfulness, Fairness and Transparency Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals. ('lawfulness, fairness and transparency')		<input type="checkbox"/>	<input type="checkbox"/>
2. Purpose Limitation Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. ('purpose limitation')		<input type="checkbox"/>	<input type="checkbox"/>
3. Data Minimisation Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. ('data minimisation')		<input type="checkbox"/>	<input type="checkbox"/>
4. Accuracy Personal data shall be accurate and, where necessary, kept up to date. ('accuracy')		<input type="checkbox"/>	<input type="checkbox"/>
5. Storage Limitation Personal data shall be 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. ('storage limitation')		<input type="checkbox"/>	<input type="checkbox"/>
6. Integrity and Confidentiality (security) Personal data shall be 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. ('integrity and confidentiality')		<input type="checkbox"/>	<input type="checkbox"/>
7. Accountability The controller shall be responsible for, and be able to demonstrate, compliance with the GDPR. ('accountability')		<input type="checkbox"/>	<input type="checkbox"/>
1. LAWFUL BASIS FOR PROCESSING (Non-Sensitive Data) - Does Your Business Know The Legal Basis And Grounds Upon Which It Processes This Type of Data? (Article 6)			
The following grounds allow for lawful processing:-			
1. Consent: the individual has given clear consent for you to process their personal data for a specific purpose		<input type="checkbox"/>	<input type="checkbox"/>
2 Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.		<input type="checkbox"/>	<input type="checkbox"/>
3. Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).		<input type="checkbox"/>	<input type="checkbox"/>
4. Vital interests: the processing is necessary to protect someone's life.		<input type="checkbox"/>	<input type="checkbox"/>



5. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.	<input type="checkbox"/> <input type="checkbox"/>
6 Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.	<input type="checkbox"/> <input type="checkbox"/>
<p>What are the conditions for processing special category data?</p> <p>Does Your Business Know The Legal Basis and Grounds Upon Which It Processes (Special Category or Sensitive) Personal Data. (Article 9). In order to lawfully process special category data, you must identify both a lawful basis as detailed above and a separate condition for processing special category data</p>	
<p>The following legal grounds apply :-</p> <p>1. The data subject has given explicit consent</p>	<input type="checkbox"/> <input type="checkbox"/>
2. Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law	<input type="checkbox"/> <input type="checkbox"/>
3. Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent	<input type="checkbox"/> <input type="checkbox"/>
4. Processing relates to personal data which is manifestly made public by the data subject	<input type="checkbox"/> <input type="checkbox"/>
5. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity	<input type="checkbox"/> <input type="checkbox"/>
6. Processing is necessary for reasons of substantial public interest	<input type="checkbox"/> <input type="checkbox"/>
7. Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services	<input type="checkbox"/> <input type="checkbox"/>
8. Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care	<input type="checkbox"/> <input type="checkbox"/>
9. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes'	<input type="checkbox"/> <input type="checkbox"/>




Where The Grounds For Processing Is Consent (Article 7)		Yes?	No?
1. Was the consent freely given?		<input type="checkbox"/>	<input type="checkbox"/>
2. Is the consent presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language?		<input type="checkbox"/>	<input type="checkbox"/>
3. Can your business demonstrate that the individual gave their consent?		<input type="checkbox"/>	<input type="checkbox"/>
4. Does the individual have the ability to withdraw their consent?		<input type="checkbox"/>	<input type="checkbox"/>
Profiling (Article 22)			
1. Does your business carry out profiling on employees or customers?		<input type="checkbox"/>	<input type="checkbox"/>
2. If so, does this profiling result in making a decision about the individual which would have a significant legal effect or similar on that individual e.g. refusal of credit or refused for an interview?		<input type="checkbox"/>	<input type="checkbox"/>
3. If the answer to point 2 is yes, has your business received the consent of the individuals to this profiling?		<input type="checkbox"/>	<input type="checkbox"/>
Children (Article 8)			
Does your business process personal data of children? If so, consider language of privacy notices and how to obtain a valid consent		<input type="checkbox"/>	<input type="checkbox"/>
2. INDIVIDUAL RIGHTS GDPR provides rights for individuals (Article 15)		Yes	No
1 Does your business or organisation enable employees and customers to request their personal data held and processed by your business or organisation?		<input type="checkbox"/>	<input type="checkbox"/>
2 Are there personnel trained to respond to requests within the 1-month timeframe?		<input type="checkbox"/>	<input type="checkbox"/>
Does Your Business Have The Processes Or Technology To Enable Data Subjects To Exercise Their Rights? (Articles 16–21)			
Summary of data subject rights:		<input type="checkbox"/>	<input type="checkbox"/>
1. Right to rectification of inaccurate data		<input type="checkbox"/>	<input type="checkbox"/>
2. Right to erasure where the data is no longer necessary in relation to the purpose for which it was collected:			
• The data subject withdraws consent			

<ul style="list-style-type: none"> • The data subject objects to the processing • Data has been processed unlawfully • For compliance with a law • The data concerns a child and was processed by a website 	<input type="checkbox"/> <input type="checkbox"/>
Your business needs to be able to identify other data controllers to whom it has disclosed data to advise them that the individual wants to be forgotten (subject to cost and available technology)	<input type="checkbox"/> <input type="checkbox"/>
3. Right to restriction of processing to verify accuracy of data, where processing is unlawful but the individual does not want erasure, the controller no longer needs the data but the individual requires the controller to keep the data for defence of legal claims or pending verification of whether the legitimate interests of the controller in processing override those of the individual	<input type="checkbox"/> <input type="checkbox"/>
4. Right to data portability – controllers have to give data subjects their data in a format which the individual can take to another controller	<input type="checkbox"/> <input type="checkbox"/>
5. Right to object, where processing is based on public interests or legitimate interests or for direct marketing	<input type="checkbox"/> <input type="checkbox"/>
6. Does your website have a mechanism for individuals to exercise the rights referred to above	<input type="checkbox"/> <input type="checkbox"/>

3 RECORD KEEPING UNDER GDPR		Yes?	No?
Personal Data Record Keeping – Data Controller (Article 30) Most organisations are required to maintain a record of their processing activities, covering areas such as processing purposes, data sharing and retention			
Controllers must maintain documented records of the processing of personal data:			
1. The name and contact details of the controller and the data protection officer (if one is appointed)		<input type="checkbox"/>	<input type="checkbox"/>
2. The purposes of the processing		<input type="checkbox"/>	<input type="checkbox"/>
3. A description of the categories of data subjects and of the categories of personal data		<input type="checkbox"/>	<input type="checkbox"/>
4. Categories of recipients to whom the personal data has been or will be disclosed (including recipients in third countries, international organisations)		<input type="checkbox"/>	<input type="checkbox"/>
5. Transfers of personal data to a third country or an international organisation, including the name of the country or international organisation and, the documentation of the safeguards for the transfer (<i>i.e. based on consent, necessary to perform a contract, public interest</i>)		<input type="checkbox"/>	<input type="checkbox"/>
6. The envisaged time limits for erasure of the different categories of data		<input type="checkbox"/>	<input type="checkbox"/>

7. General description of the technical and organisational security measures	<input type="checkbox"/> <input type="checkbox"/>
Personal Data Record Keeping – Data Processor (Article 30)	
1. Name and contact details of the joint controllers, the representative(s) and the Data Protection Officer(s)	<input type="checkbox"/> <input type="checkbox"/>
2. Categories of the processing	<input type="checkbox"/> <input type="checkbox"/>
3. Transfers of personal data to a third country/international organisation and documentation of suitable safeguards	<input type="checkbox"/> <input type="checkbox"/>
4. General description of the technical and organisational security measures	<input type="checkbox"/> <input type="checkbox"/>
Data Protection Officer (DPO) (Article 37)	
Establish whether your business is required to have a DPO. Does one of the following apply:	<input type="checkbox"/> <input type="checkbox"/>
1. Processing is carried out by a public body, except for courts	<input type="checkbox"/> <input type="checkbox"/>
2. Your core activities consist of monitoring operations which, by virtue of their nature, scope or purposes, require regular and systematic monitoring of data subjects on a large scale; or	<input type="checkbox"/> <input type="checkbox"/>
3. Your core activities consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences	<input type="checkbox"/> <input type="checkbox"/>
If your business is not required to have a DPO, you may appoint a voluntary Head of Data Protection. Your DPO contact details must be notified to the regulatory authority and published to the public	<input type="checkbox"/> <input type="checkbox"/>
	Yes? No?
Data Retention (Article 5)	
Data can only be retained for as long as necessary for the purpose for which it was obtained	<input type="checkbox"/> <input type="checkbox"/>
Your business or organisation needs to determine how long data can be kept. After this time it is either completely deleted or anonymised	<input type="checkbox"/> <input type="checkbox"/>
Data Privacy Impact Assessments (DPIA) (Article 35)	
Where your business or organisation implements new technologies, which will or could result in a high risk to the rights and freedoms of individuals, your business is obliged to carry out a DPIA	<input type="checkbox"/> <input type="checkbox"/>
This is to determine what impact the technology and processing will have on an individual's personal data rights. The aim is to ensure that this adheres to all elements of GDPR provisions.	<input type="checkbox"/> <input type="checkbox"/>
Employee Training (Article 5)	Yes? No?

<p>Employees who handle personal data of other employees or data subjects must receive data protection training in order to ensure that they handle personal/special data in accordance with GDPR.</p> <p>Your business or organisation should keep a record of all training and provide update and refresher training at least annually. If changes occur in data protection legislation, your business must put in place suitable updated training.</p>	
Policies and Procedures (Article 5)	
<p>You must ensure that your business or organisation has considered its privacy obligations. It must also implement the 7 GDPR data protection principles (see above).</p> <p>Your business or organisation must have and also have implemented, clear and concise data protection policies. The exact list of policies that will be appropriate for each business will depend on what data it processes and why. There is no set format to these for these policies. A list of common policies follows:-</p> <ul style="list-style-type: none"> • General Data Protection Policy • Employee Privacy Policy and Notice • Data Breach Escalation and Checklist • Data Subject Access Rights Procedure • Data Retention Policy • Processing Customer Data Policy • Guidance on Privacy Notices 	

4. PRIVACY BY DESIGN AND PRIVACY BY DEFAULT (ARTICLE 25)	
<p>Under the principle of ‘data protection by design and by default’, the GDPR legally requires you to take this approach.</p> <p>Privacy by Design</p>	
<p>The data controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures in an effective manner.</p>	
<p>The data controller shall also integrate the necessary safeguards into the processing of the data in order to meet the requirements of the regulation and protect the rights of individuals.</p>	
Privacy by Default	
<p>The data controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed.</p> <p>That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and general accessibility.</p>	

5. PRIVACY NOTICES (ARTICLES 12–14)		
Are Privacy Notices Given At The Correct Time To Data Subjects?	Yes?	No?
Notices must be given at the time that the data is obtained from the individual, or if the data was received from a third party, within a reasonable period after obtaining the data but at the latest within 1 month.	<input type="checkbox"/>	<input type="checkbox"/>
Do Your Privacy Notices Contain All of the Required Information?		

Details required:-	
1. The identity and the contact details of the controller and data protection officer, where applicable	<input type="checkbox"/> <input type="checkbox"/>
2. The purposes of the processing for which the personal data is collected, together with the legal basis for the processing, including the legitimate interests relied upon by the controller	<input type="checkbox"/> <input type="checkbox"/>
3. The recipients or categories of recipients of the personal data	<input type="checkbox"/> <input type="checkbox"/>
4. Where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and how the transfer ensures adequacy of protection (mechanisms set out in GDPR for protection when data is transferred in this way and which mechanism will be used)	<input type="checkbox"/> <input type="checkbox"/>
5. The period for which the personal data will be stored. Alternatively the criteria used to determine that period.	<input type="checkbox"/> <input type="checkbox"/>
6. The right to request from the controller regarding an individual's data:- a) access to and rectification b) erasure of personal data c) restriction of processing d) to object to processing e) the right to data portability	<input type="checkbox"/> <input type="checkbox"/>
7. Where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing, based on consent, before its withdrawal	<input type="checkbox"/> <input type="checkbox"/>
8. The right to lodge a complaint with the ICO	<input type="checkbox"/> <input type="checkbox"/>
9. Where the provision of personal data is: • statutory • a contractual requirement • a requirement necessary to enter into a contract Is the individual obliged to provide personal data and the possible consequences of the individual's failure to provide such data?	<input type="checkbox"/> <input type="checkbox"/>
10. The existence of automated decision making, including • profiling • meaningful information about the logic involved together with the significance and the envisaged consequences of such processing for the individual data subject.	<input type="checkbox"/> <input type="checkbox"/>
Privacy Notices Language	
Is the language concise, transparent, intelligible, in an easily accessible form, using clear and plain language?	<input type="checkbox"/> <input type="checkbox"/>
Do you pay extra attention to your notice if the information is addressed to a child?	<input type="checkbox"/> <input type="checkbox"/>
You need to consider whether the notice is delivered in a format that is user-friendly. In addition, consider the manner of delivery.	<input type="checkbox"/> <input type="checkbox"/>

6. DATA SECURITY		Yes?	No?
Are Your Security Measures Appropriate for the Personal Data? (Article 32)			
<p>Security has to be appropriate to the likely risks to individuals if data was lost, stolen or disclosed to unauthorised people. Security covers organisational matters such as people involved and the type of process used and technical the measures you have taken.</p> <p>Consider the following:-</p> <ul style="list-style-type: none"> • Pseudonymisation • Encryption • Ensuring ongoing integrity, confidentiality, availability and resiliency • The ability to restore data in a timely manner • Processes for testing security 			

7 DATA PROCESSORS AND INTERNATIONAL PERSONAL DATA TRANSFERS		Yes?	No?
Does Your Business or Organisation Use Third-party Data Processors or Group Companies to Process Data on its Behalf? (Article 28)			
<p>If so, there must be a written contract with each data processor which must include the minimum requirements contained within Article 28.</p> <p>Your business must also ensure that it has received 'sufficient guarantees' from its data processors so that they can implement measures (technical and organisational) to meet the requirements of the GDPR.</p> <p>Your business will need to carry out its own due diligence and perform its own assessment about whether its processors are complying with GDPR. This could be achieved by carrying out an audit.</p>			
Does Your Business/Organisation or Does Your Businesses Processors, Transfer Data Out of the EU? (Articles 44–49)			
<p>If data is transferred outside of the EU, which of the approved transfer mechanisms are used?</p> <p>Consider the approved transfer mechanisms which follow:-</p>			
1. A country which has a finding of adequacy from the European Commission			
2. If it is within your business or company group, are binding corporate rules in place?			
3. Standard contractual clauses as approved by the European Commission			
4. If the transfer is to the US, on the basis of the EU/US Privacy Shield programme			

5. With the consent of the data subject	<input type="checkbox"/> <input type="checkbox"/>
6. The transfer is necessary to carry out a contract with the data subject	<input type="checkbox"/> <input type="checkbox"/>
7. The transfer is in the public interest (Press or Law Enforcement)	<input type="checkbox"/> <input type="checkbox"/>
8. The transfer is necessary to establish, exercise or defend legal rights	<input type="checkbox"/> <input type="checkbox"/>
9. The transfer is necessary to protect the vital interests of a person where the data subject is physically or legally incapable of giving consent	<input type="checkbox"/> <input type="checkbox"/>

8. DATA BREACH NOTIFICATION	Yes?	No?
Mandatory Notification (Article 33)		
Does your business or organisation have procedures in place to enable it to report a data breach to the ICO within 72 hours of becoming aware of it?	<input type="checkbox"/>	<input type="checkbox"/>
The breach must be investigated and details provided to the ICO about the nature of the breach, the likely consequences and mitigations being taken to address it. This investigation may require processors to assist, so operational processes should make provision for this		
Notification to Individuals Affected (Article 34)		
If the breach is likely to result in a high risk to the rights and freedoms of individuals, your business will need to notify the individuals affected.	<input type="checkbox"/>	<input type="checkbox"/>
If data is encrypted or otherwise unintelligible, then individuals will not need to be notified.	<input type="checkbox"/>	<input type="checkbox"/>

Concluding Statement

Do not feel overwhelmed with the scope of what is required from the GDPR regulations. This outline is a summary of the pathway toward compliance.

There is an old saying, *“a journey of 100 miles begins with the first footstep”*

So Where Do You Begin?

Full compliance can take some time to achieve. The scope of your compliance requirements can depend upon the size and nature of your business, as well as the type and nature of data processing that you carry out. The best course of action here may well be to get professional advice.

It is advantageous to begin taking at least some action toward compliance and to do so as soon as possible. In the event of a complaint or breach, the enforcement body, the ICO, (the governing body for the UK), will look at what steps you have taken to comply with the regulations. If you have completely ignored the law and made no attempt to begin complying with the regulations, this will probably be viewed unfavourably when the ICO decide what sanctions to enforce against you.

DPIA

Some people will say the first thing you need to do is conduct a DPIA (Data Protection Impact Assessment)

This is generally a good idea. For new projects, DPIAs are a vital part of data protection by design. They build in data protection compliance at an early stage, when there is most scope for influencing how your business will work and how a project or proposal is developed and implemented.

A DPIA is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of your accountability obligations under the GDPR, and when done properly helps you assess and demonstrate how you comply with all of your data protection obligations.

It does not necessarily need to be complex or time consuming and much will depend upon your individual business.

IT and Security Review – Consider Device Encryption

Other areas that can bring immediate results and which will require consideration at some stage of your compliance journey, is an IT and security audit review. Computers, laptops and mobile devices can all benefit from the security that ‘Endpoint Protection’ and ‘Encryption’ can provide. Many data breaches occur because of accidental loss or theft. We hear of people losing their phones every day. Encrypting devices, including mobile devices, makes the data unreadable.

Your Reporting Obligations

While there is a legal obligation to report data breaches to the governing body for the UK, (the ICO), encrypted devices do not need to be reported in this way. If a phone or other mobile device is lost or stolen and it contains personal data, if it is encrypted, you have protection in place.

This decreases your potential liabilities and reporting obligations under the regulations. At the same time, it gives added peace of mind, knowing your devices are secure and that business data cannot be used maliciously by unauthorised persons.

Website Privacy Centre

Your website is an obvious reflection of your business activity. A privacy centre for users of your web site is a great way to show that you take user privacy seriously. At the same time it is also providing a way for you to comply with users privacy requests made through your website under GDPR provisions.

A website without a user privacy centre is a dead giveaway that your business has taken few, if any steps, to become compliant under the GDPR regulations.

Business & Organisations – Are You Aware & Alert To Potential Compensation Claims?

This is probably the biggest problem that the new regulations will bring. Fines under GDPR have been well publicised. Compensation claims for breaches of GDPR are an additional liability.

There have already been examples of 'No-Win – No Fee' claims firms entering the GDPR compensation claims arena. Changes to the way in which claimants can make a claim, together with changes in the law that make 'distress' a valid ground upon which to claim means that business owners and organisations that are not prepared are open to potentially huge compensation claims.

Imagine for a moment that 100 records were breached and a claim for all of them was submitted. Some claims firms have been suggesting that a claim of up to £5000 may be appropriate. Even if a court decided that £1000 was a more appropriate figure, (depending on the nature of the breach), that would work out at £100,000.

Consider the recent case of British Airways. As the Telegraph newspaper reported

'Nearly 400,000 passengers have been caught up in yet another PR disaster for British Airways, with the airline the victim of a "sophisticated and malicious" security hack.'

As a result, BA has been threatened with a £500 million class-action lawsuit in a UK court by law firm SPG Law. It alleges BA is liable to compensate for 'non-material damage' under the Data Protection Act 2018, the UK's implementation of GDPR.

As the effect of such claims filters down, claims firms will become more aggressive, (think of PPI directed at business owners and organisations).

Even smaller business owners and organisations will feel the impact, if they are not prepared. Claims firms have already begun targeting smaller businesses and organisations, when they can see from a quick assessment that the business or organisation is not GDPR compliant.

Add in legal fees for defending such a claim together with potential legal fees and costs of the claimants.

Most people begin to appreciate that this is one of the most serious implications of the GDPR regulations. It has the potential to close a business or organisation down or at the least cause substantial problems.

Other Steps To Take

There are other immediate steps that you may or may not already have in place. These steps will also help in making your business or organisation compliant and can often be quickly determined with a business assessment.

Additional Benefits For Clients

Some of the more far reaching effects of GDPR have not yet filtered through to business owners and very few people are talking them. There will be at least one crucial outcome that every business owner will want to bear in mind. Being prepared and aware of these likely effects will protect and secure your position over the longer term.

Your Next Step

Arrange for a consultation now. It will help you decide the best way to move forward and begin your process of achieving GDPR compliance. It will also help you feel much better. If you have not made any progress in this area to date, knowing you have finally made a decision to become compliant can be a major relief.

Stephen Wilk

Information Provided By 'GDPR Support For You'

28a Hulton District Centre

Manchester

M28 0AX

Stephen Wilk – BA (Hons - Law) - MCSE

T: 0844 4141 326

Email: Stephen@gdprsupportforyou.co.uk

© Copyright 2018 ‘GDPR Support For You’ - Stephen Wilk. Please note that the materials provided in this guide are believed to be accurate and correct. Do not construe this as legal advice. ‘GDPR Support For You’ & Stephen Wilk is a support service assisting and helping you become GDPR compliant. ‘GDPR Support For You’ & Stephen Wilk cannot accept responsibility for any loss or damage resulting out of the use of this information. If in doubt please confirm the validity of all information before relying upon it. Please do not copy or use this material without consent. This is against the terms and conditions upon which this material is supplied.
