WardWilliams
chartered accountants

GDPR
Now the realities appear

Are you sure your business is GDPR compliant?

GDPR: Now realities appear

If you are like us, you probably reached GDPR fatigue a long time ago, and who knew that so many businesses were your friends, many you had never even heard of!

GDPR is not the new Millenium Bug - GDPR is here to stay and MUST be taken seriously as it impacts on every business in the United Kingdom.

With fines of £18,000,000 and, under the new Data Protection Act 2018, directors held personally liable to pay those fines, the time to act is definitely now.

Whilst most businesses will not face fines of £18 million, what level of fine would hurt your business? Would it be £50,000, £100,000 or higher than that? Would your directors want to pay that out of their own pockets whatever that fine was?

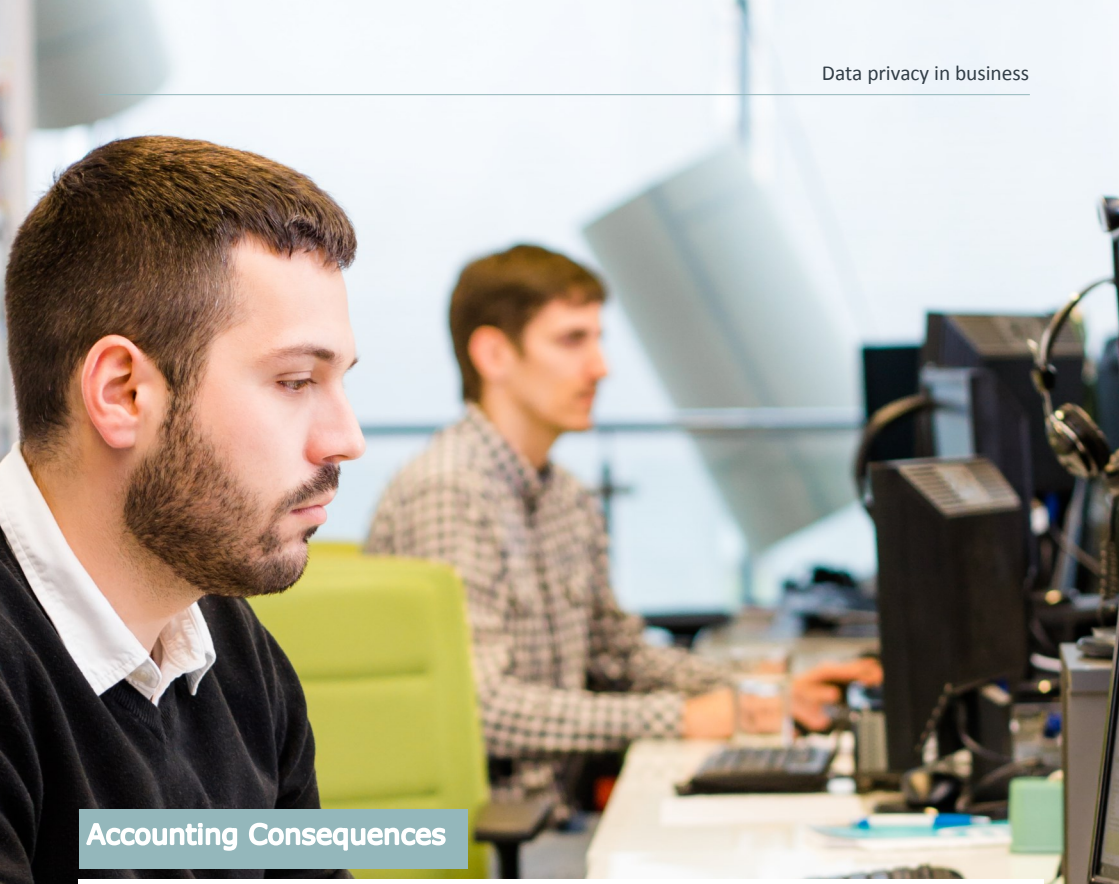
Accounting issues

Many businesses should have registered with the Information Commissioners Office (ICO) to legally have personal data (for example, no matter how small the business, if CCTV was used on business premises that business had to register) but very few did. That means all the personal data was illegally collected.

Separately, if no Privacy Notice was given at each collection point then it was unlawfully collected.

Additionally, we have seen that businesses which "borrowed" someone else's Privacy Notice have ended up being fined, as they did something with personal data that was not in their Privacy Notice. We are not talking about Cambridge Analytica / Facebook, but businesses a lot smaller than that.

Each of these failures means each past and present customer has a claim as of right.



Accounting Consequences

For those businesses that were either:

(a) not registered with the Information Commissioner under the 1998 Data Protection Act but should have been (were you registered?); or,

(b) who did not give a Privacy Notice at every point of collection of personal data (website, form, app, call), (did you?);

Those failures means each past and present customer automatically has a claim, of a minimum of £1,000. Article 82 GDPR enshrines claims for related distress so there is no escape.

Due to the Accounting rules , the existence of potential claims means that accountants will, or should, consider closely during any end of year audit putting provisions in the accounts.

Provisions of even £1,000 per past and present customer will be a lot for any business. It would mean that no dividends could be paid out until those provisions wash through.

Reduction in value

Data is valuable, we all know that. The value of personal data that has not been collected in line with the Privacy Rules is, on the other hand, not only worthless it is a liability and that acts to reduce the price buyers will pay.

We are aware that lawyers have for the last 10 years been negotiating reductions in the sale price of between 20% and 33%. That was when the maximum fines were £500,000, there were no potential privacy claims, no personal liability for directors and no provisions needed to be made.

How much will be deducted now do you think? How much would you deduct to account for these potential risks?

Would anyone want to buy a tainted business with the level of personal risk it would bring to the new directors?

Cashflow: Impacts of the new PPI

Whilst PPI affected a small number of businesses, (the lenders), the above failures apply to most businesses now, and the failure to comply or to protect data will see claims multiply.

It is likely be the new PPI, as PPI lawyers and personal injury lawyers look for new work to plug the gaps as current opportunities diminish.

This affects every business – It is not optional.

Every customer of a non-compliant business is in a position to claim for past failures, and will definitely claim for future failures.
Just think about the impact this will have – what business MUST do is take action to reduce the likelihood of being affected.

Supply chain business

Any business that depends on a supply chain up and down which any personal data moves, like insurance brokers, finance brokers, body shop repairers and so on, will be removed from that chain if they cannot demonstrate that they are GDPR compliant.

It also means they cannot bid for Government work.

If you are a franchisee you need to make sure your Franchisor has provided you with a complete GDPR solution. It is an essential part of any business.

Personal Liability

Accepting that customer data is a valuable asset of the company means under the Companies Act 2006 it has to be stewarded by the directors and its value maintained.

As we have seen, this has not happened in many cases and indeed that reduces the value of the business and exposes it to claims. This could lead to shareholders looking to directors to make good any shortfall on sale where the business has suffered a reduction in price**.**

We have already seen that the new Data Protection Act 2018 s.198 will make directors personally liable for fines under GDPR.

Directors of non-compliant businesses could see lenders refusing to lend to them personally or increasing the cost of borrowing to cover the additional risk.

Some fines are in the £18,000,000 (4% global turnover if higher) **band** such as:

- Not giving accurate privacy notices or not having a privacy notice
- Keeping data too long or losing data
- Not following the main GDPR principles
- Not informing people the data is stored abroad (which applies to many Cloud based services)
- Not enabling data subject rights

It has another range of **fines** of up to £9,000,000 (2% global turnover if more) for things like:

- Failing to do data privacy impact assessments
- Failing to properly obtain a child's consent
- Failing to apply protection by design & default to personal data processes
- Failing to put in place data processor contracts where needed
- Failing to know when to notify a personal data breach
- Failing to have proper data privacy management procedures in place
- Failure to have training programmes in place

eMarketing is next

The ePrivacy Regulations are due out by the end of 2018. The name is not helpful as they actually are about eMarketing.

Any business that has not checked it has clear consents (either Soft Opt in or positive opt in) or other rights will be at risk of claims and indeed fines every time it sends an email marketing message out. Those fines are very likely to occur because every email which is wrongly sent out is effectively a bullet to be fired back along with a fine and a claim.

Competitive Advantage

Now for the good news! Now is the time to roll up the sleeves and dig in, because this can be used to give competitive advantage to those businesses that want to thrive.

Having personal data is a matter of trust. Just look at Facebook and Cambridge Analytica. Even before any regulator had said anything was done wrongly, Facebook lost a third of its value and Cambridge closed its doors.

Its directors may yet be held personally liable to the ICO. The public had tried them and found them wanting – a failure of trust.

Show your customers that you can be trusted with their personal data. Who do potential customers want to do business with – those who can demonstrate they take their obligations seriously, or those who don't care?

Investing the time and effort in getting GDPR compliance sorted is not only good for efficiency, it is good business.

There are marks that can be awarded to show that a business has done the right things and can be trusted with personal data.

These marks will soon be like the https or padlock symbol on a site that wants your credit card details – if you don't see them, you don't do business with them.

Do you think your competitors might see a way to "weaponise" GDPR? To use it for their commercial advantage? Can you?

Did you know?

Section 198 Data Protection Act 2018 is going to make directors personally liable for GDPR fines. Partners and sole traders already are.

DataGuardsman—Setting the standard in GDPR compliance

It is not easy to comply with the requirements of 262 pages of text, 99 rules and 6 Principles. How do you ensure you are doing what is needed to run your business safely? The solution is DataGuardsman.

What is DataGuardsman?

This web based system was designed by legal experts and tested by real businesses to make it as simple to use as possible. Sign up, log in securely and work through bite sized modules at your own pace at a time to suit you.

DataGuardsman asks users to answer simple questions about their business and intuitively produces policies, documents - and where necessary, a task list for you to complete. Updates are also issued as the law changes making sure users remain protected and well informed.

Once all the modules have been completed the DataGuardsman seal will be issued for your business to use on documents and web sites, plus an additional £250,000 of insurance against fines to protect directors and business owners.

Protect your business with GDPR and Cyber Security options

Option 1: Brookland Protect – Raising the standard with training

Making sure that your business is fit to trade is one thing, but if you have staff it is important that they are aware of how to manage data, promote the business safely and avoid potentially costly data breaches, privacy claims or ICO fines.

Providing unlimited access to Cyber Security and GDPR training through on line learning solutions is an efficient, cost effective and easy way to make sure that your team are well informed, also provides you with clear guidance and knowledge as well as complete peace of mind in the complex world of online security.

GDPR Protect includes a DataGuardsman subscription and on line certified courses at Employee, Foundation and Practitioner level covering topics such as ePrivacy, Cyber Security Awareness, Malware and Phishing, Fraud Prevention and Internet, Email and social Media Safety.

Cost £99 + vat per month (minimum 24 month contract).

Option 2: Brookland Protect Ultimate – Security, training, compliance and software solutions

In addition to the GDPR Protect service the very latest software solutions can be added to give practical protection immediately – a privacy and security package including Mobile Device Management, E Mail Encryption, Web Filtering and Multi Factor Authentication for security has been designed to provide security and peace of mind for SME's.

Cost £99 + vat per month PLUS £25 + vat per user (Minimum 24 month contract).

Example: a 5 staff business = £224 + vat per month.

N.B. A one off technical set up charge will be due when the software installation occurs, this will be quoted on a client by client basis subject to system requirements and numbers.

If you would like any further information on any of these options please contact the office on 01932 830664 or email gdpr@wardwilliams.co.uk.

Ward Williams
chartered accountants

www.wardwilliams.co.uk

GDPR@wardwilliams.co.uk

Weybridge:
t: 01932 830664 **f:** 01932 830733
Belgrave House, 39-43 Monument Hill, Weybridge, Surrey, KT13 8RN

Uxbridge:
t: 01895 236335 **f:** 01895 257641
Bay Lodge, 36 Harefield Road, Uxbridge, Middlesex, UB8 1PH

Sunninghill:
t: 01344 624114 **f:** 01344 873197
9 Crossways, London Road, Sunninghill, Ascot, Berkshire, SL5 0PY

Bracknell:
t: 01932 830664 **f:** 01932 830733
Venture House, 2 Arlington Square, Downshire Way, Bracknell, Berkshire, RG12 1WA

London:
t: 020 3858 0127
1 Primrose Street, London, EC2A 2EX