GDPR DATA LAWS

May 25th 2018

HARDSOFT™ COMPUTERS

Issue 3

In this issue we look to help you and your business with specific TO DO's and also expose some myths we have come across.

GDPR Myths

- You don't need an appointed person or Data Officer. It's a good idea to have someone responsible for your company's data but it's not a role you need to assign to someone.
- There is no such thing as a GDPR Policy - you need to be producing a Privacy Policy
- You do NOT need Pre ticks for consent on everything if it stops your business dealing with that client.

We are not GDPR or data privacy professionals so this advice should be used only as a guide. The ICO, who will be policing Data Privacy, are looking from SME's to prove they have looked at and thought about how you deal with data that you handle. More importantly; customers or potential customers that you may market to now have the right to find out where you hold that data, what data you hold and that data to be removed if you have no reason to hold it.

Although we don't anticipate that the ICO will be knocking on your door, you should anticipate a number of enquiries from prospects who may wish to be removed.

We hope this guide helps you and offers sensible advice, we also have external Data Privacy Partners we can recommend who can come to you and offer advice or create your own Privacy by Design, with a unique Data Privacy Policy.

HARDSOFT™ COMPUTERS

We can't help with many of the points mentioned previously like updating Privacy Policies on your website BUT we can update you on the current scenario in regard to the Server equipment supplied by HardSoft...

External Back Ups on the Server will now need to be secured and encrypted. Call for details.

Our Cloud- Back Up offers Bank-level Security. Livedrive stores your customer's files in UK data centres.

Additionally you maybe **backing up data onto Memory Sticks**. These now need to be secured with PIN enabled devices.

Anti –Virus and in particular the Ransomware/ CryptoVirus. This threat is a direct attack on data on a Server and loss of data could mean reporting it to the Commissioner and possible fine. Many of our Server customers have added an extra layer of security which is Sophos Intercept X protection. This is recommended to tighten up leaks.

Software Updates - Don't ignore those annoying Windows reminders and pro-actively look for updates on other software such as Sage.

Office 365 emails - Your emails are stored by Microsoft. Microsoft are fully GDPR compliant as you would expect BUT only since August 2016 have they had your data stored in the UK. If you are in an industry sector like Legal then you may have had requests as to where your data is held. You may want to have your Data relocated to the UK by Microsoft. We can do this for you, but note, there will be a downtime as Microsoft transfers your Data between countries.

Right to Forget - If a customer invokes this you will need to not only remove their details from your system but also from any Cloud and External Drive backs ups.

Passwords need to be secure and changed regularly. Building Data Security into the heart of the business - staff need to understand the dangers of passing data around and even sharing personal data.

To Do List

Data Privacy is the basis of GDPR Regulation and will be an ongoing narrative for your business both internal, how you handle data, and external with clients and prospects. So it's likely you will be ready for May 25th and then never want to look at it again, you will need to review procedures on a timely basis. However there are things we recommend you do before May 25th:

- Register with the ICO - go to **www.ico.org.uk/registration/new** and register your company. This is currently only £35 + VAT, after 25th May if you are not registered you could get a £2000 fine. If you do nothing else DO THIS.

- Data Processing - you need to think about two types of Data, internal, such as staff DOB, Payroll info, next of Kin; and client which may be name, address, bank details, DOB, email. You need to be able to show the ICO, your procedures concerning the following:

- What Data is held?

- Where is it held- such as Cloud / Server / Encrypted / USB stick / Paper in a filing cabinet?

- How long will it be held for? You can only hold it only for as long as is necessary, this may mean 7 years for payroll as HMRC advise, but for a one off purchase maybe only 2 years to cover 2 accounting periods.

- Staff Guidelines- chat with staff, discuss the GDPR elephant in the room. Give advice how they deal with an enquiry. No one needs panic, but set a time line to deal with any queries. Then write an easy to follow procedure to help regulate staff responses.

With the above information you should be looking to produce a comprehensive Privacy Policy – the foundation of being GDPR compliant.

HARDSOFT™ COMPUTERS