The EU General Data protection Regulation (GDPR)

"Are you ready?"

From 25th May 2018 Companies may face "Fines of up to 4% of their annual global turnover or €20 million whichever is greater. This is a significant development in the current ruling and clearly moves the responsibility for the protection of data away from the IT department and places it squarely in the territory of the board of directors.

A move of this magnitude, one that can cause even the largest companies considerable financial pain, needs to be raised to a high priority and actions taken to prevent prosecution. The recent fine placed on Talk-Talk for their data breach was £400,000, if they commit the same offence after May 2018 this fine could be £31.4 million; the message is clear.

2016 saw some of the most ambitious cyber-attacks which ranged from multi-million dollar virtual bank heists, state sponsored interference with elections to disk-wiping attacks in the Ukraine which caused multiple power outages. In the UK GCHQ blocked more than thirty four thousand attacks principally from Russia and China, while 50% of British businesses suffered cyber-attacks, double the 2015 level.

The World also saw one of the furthest reaching malware attack to date when the WannaCry ransomware hit more than 300,000 computers in over 150 countries, an attack that could have been avoided by the most basic attention to software updates and an indication that the next hit will be stronger and more refined.

Big business needs to be alert as the cyber criminals are shifting the goal posts, for example, there is a move away from stealing from individual accounts to stealing from the banks, one group managed to steal US$81 million from Bangladesh's Central Bank. While at home there were 188 high-level attacks aimed to steal defence and foreign policy secrets, businesses, governments and all organisations have become the victims of the latest most supplicated hackers.

Core Elements

The GDPR runs to over 260 pages of difficult reading and contains a number of potential contradictions. Organisations could benefit with professional and legal advice to demonstrate adherence to the regulation.

Article 32

> *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the*

*processor shall implement appropriate technical and organisational measures **to ensure a level of security appropriate to the risk**, including inter alia as appropriate:*

(a) the pseudonymisation and encryption of personal data;

(b) *the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*

(c) *the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*

(d) *a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*

In essence this article requires organisations to implement the appropriate security measures to protect personal data held by them. This article makes specific reference to the encryption of personal data as one of the elements in achieving this objective.

To whom does GDPR apply

Some small and medium sized companies may be thinking that GDPR only applies to large companies and organisations like the NHS and banks. Not so, any organisation that processes personal data comes under the rules set down within GDPR, this includes both the public, customers, clients and employees.

The regulations also impose restrictions on the transfer of personal data outside the European Union and the control of personal data held by European subsidiaries or offices of foreign entities.

Companies will invariably appoint a member of senior staff to take responsibility for ensuring that there is conformity and for organisations with around 5000 personal records or more a specialist Data Protection Officer (DPO) will need to be employed.

Safeguarding your systems

There are four major areas that need to be addressed to create a secure system and thereby avoid falling foul of GDPR. First there is the issue of out of date software and operating systems, then there are user bad habits, main server weaknesses and network security.

Software

It is important to ensure that all software and operating systems are kept up to date, this includes anti-virus, firewalls, anti DOS (Denial of Service Attack) and other software elements contained within hardware. While some updates are there to improve or correct errors in a system the majority are there to fill gaps vulnerable to attacks or security updates; therefore these should not be ignored.

Had users kept systems up to date with the patches from Microsoft the recent WannaCry ransomware attack would have been avoided as the fix for this known malware was included in updates supplied some months ago.

Users

We then come to the Users, a frequent cause of malware attacks. Perhaps the biggest problem is caused by extraneous emails frequently carrying attachments. One should note that 57% of data breaches are due to hackers or malware and 23% of data breaches are caused by unintended disclosure (the User). Email attachments are notorious as the delivery vehicle for nasty pieces of software. There is also the issue of obedience of very basic security principles, how often does one see post-it notes on or around the PC with the user's password written on it.

Employers need to establish procedures to ensure that employees do not contravene the GDPR guidelines and cause a possible data security breach. Employees should also be made aware of what to do in the event of discovering a data breach.

PC's and Servers

Moving onto the Servers installed these and their associated protection hardware need to be maintained with the most recent updates and in addition need close attention to how they are connected to the outside World. When hackers attack data centres they invariably find their way in via a poorly protected open port, how else do teenagers in their bedrooms find their way into NASA? We know that some ports must be open to allow access for legitimate users and access to the internet, but they do need to be configured to maintain a secure system. IT managers should also review ageing equipment. Hardware over five years old may no longer meet the current high standards required to maintain a secure system. Companies must take the bitter pill of high expenditure but remember the cost of replacement and additional equipment is likely to be far less that the penalty posed by the Information Commissioner's Office (www.ico.org.uk) who will enforce the GDPR. For some companies the inclusion of the '**Data-at-Rest Protection**' system (available from MPWA Limited) may be the answer for a truly secure system. DRP is a state of the art encryption system whereby all of the data held on a company's servers is encrypted. Data is only decrypted when a user opens a data set for access and update, and is then re-encrypted with a new PKI (Public Key Infrastructure) private key when the user closes the session.

Networks

Finally we come to the Network connection, the speciality of MPWA Ltd. There are two vital elements to consider, first there is the problem of making sure that the User is indeed a legitimate user; second that every data packet transmitted between user and server is encrypted. To guarantee the legitimacy of the user there should be three factor

authentication, something the user owns, something the user is (a biometric) and something the user knows (a compound password). To meet the stringent demands for a secure network connection only the **NiCE-Security System** scores in both departments. Using NiCE the three factor authentication is supported by virtue of the user possessing the NiCE_Key, registering their fingerprint and knowing their composite password. Meanwhile the highly secure VPN (Virtual Private Network) connection is encrypted with a compound code word made up of an SSL (Secure Socket Layer) certificate coupled with an addition one time random token. ONLY NiCE offers this level of security as other Software VPN Systems, (including such market leaders as Cisco and Citrix) can support a maximum of two factor authentication and have to exchange unencrypted data packets in order to set up the encryption code word.

It has been commented by a very senior IT Security Specialist that the combination of the 'NiCE Security System' and 'Data-at-Rest Protection' makes for the most secure networked system possible.

What if there is a Data Breach

There are a myriad of procedures available by searching the internet and companies should seek professional help to tailor a response sequence that is appropriate. The important thing to remember is DON'T ignore a data breach.

Under the GDPR paragraph (85):

> "*the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay".*

Also be aware that some data breaches may have happened in the past and just been discovered. The following is a sample showing the level of response appropriate.

First 48 Hours – Your Incident Response Checklist
When organizations adopt an "assume breach" philosophy and take steps to prepare for an incident, they're less likely to panic and make damaging mistakes when a breach occurs. Keep the following items in mind as you go through the first 48 hours after discovering a data breach.

Document in detail the date/time and how the data breach was discovered, who discovered it, and when the incident response procedure began.
Immediately notify all members of the crisis communication and forensics team, third-party vendors as well as executives.

Preserve all physical evidence surrounding the location of the breach.
Protect unaffected systems from further data loss by disconnecting them from affected systems while bringing affected systems offline.
Perform a thorough forensic investigation of all unaffected systems to ensure they are not breached.
Protect yourself from further liability; document everything, including the circumstances under which the breach was discovered, types of data lost, affected parties, etc.
Employ an independent third-party vendor to interview internal employees who discovered and initially responded to the data breach.
Dispatch the forensics teams (both internal and external) to begin investigating the breach and document their findings. Fix the issue that caused the breach.
Begin the notification process after consulting with the legal team to determine the notification process and priorities.
Contact law enforcement agencies and begin temporarily expanding the customer support team and setup the incident response hotline.

Remember that your lawyer is there to guide you through the procedures necessary to minimise your exposure.

Start planning now

These new directives are barely a year away and to use the old Boy Scout adage its best to 'BE PREPARED'. Forward looking Law Firms both sides of the pond are now helping their clients to put into place plans and procedures to not only prevent breaches but to minimise the consequences if one occurs. These Law Firms will be working with IT Security Specialists to ensure that companies are adequately prepared.

By using the right Law Firm companies will not only be best placed to follow the guide lines but will also benefit in the event of a data breach by being able to mitigate any penalty by being able to demonstrating their effort to comply.

Contact Details:

MPWA Limited

Mob: +44(0)7774 232898

Email mw@mpwa.co.uk

Website www.mpwa.co.uk