Don't bury your over changes to

Mark Thomas picks his way through the latest legislation and how it will affect business across region

FROM April Fool's Day, we will have just 37 business days left to prepare for the biggest revolution in data protection and privacy laws to hit Europe in 20 years.

It affects ALL businesses that handle personal data, large and small. And if your business has not already made significant inroads by now in preparing for the launch of the General Data Protection Regulation on May 25, then the fool may very well be you.

For those clutching at straws, Brexit will offer no escape, with the UK government having decided to adopt the GDPR in full, no matter the outcome of our European negotiations.

Most business people will have heard of GDPR by now, but any who have not yet looked into the processes involved in becoming fully compliant may be in for a shock.

The new legislation will give people the right to demand to know what data you hold on them, what you use it for and how long you propose to keep it for. And it gives them the power to demand to see what information you hold on them, and have it removed from your database.

You need to proactively obtain permission to hold or share people's data, and only for the uses and the length of time they agree to you holding it for. It does not just affect digital information, but paper records too.

There is no quick fix here. The GDPR is going to be a complex, time-consuming and potentially expensive process for EVERY organisation that holds data on customers, from the biggest corporations to the smallest one-person business.

And burying your head in the sand and hoping this will go away is dangerous, with the Information Commissioner's Office (ICO) ready to take a firm line on those who are not ready by the looming May 25 deadline.

ICO Head of International Strategy and Intelligence Steve Wood, said last year: "Will there be a grace period? No. You will not hear talk of grace periods from people at the ICO. That's not part of our regulatory strategy. What you will see is a common-sense, pragmatic approach to regulatory principles."

Quite how that manifests itself remains to be seen, but it is clear that organisations that have not taken significant action to attempt to make themselves GDPR compliant could be in major hot water, with fines of up to 20 million euros or 4% of a company's global turnover, whichever figure is greater. The complexities go well beyond IT issues, opening up some complex legal questions around areas such as contracts between businesses who share customer data with each other. Under the new regime no business should share data with another without satisfying itself that that business is also GDPR compliant.

So why are businesses being forced into this expensive and time-consuming bureaucratic minefield?

Kevin Lovelady, whose Kirkdale-based company Tallguy Digital is setting up workshops to provide information and guidance on the GDPR, says: "It is in the same ballpark as Health and Safety legislation. It does seem like a real pain for business people, but you can't think of it purely as an inconvenience.

"You have to look at it from the point of view of you as a punter first rather than you as a business owner. How would you feel if your own data was compromised?

"The big change is that it is trying to give a little bit of control back to the punter. It is about being honest and saying if I am serious about looking after my customers this is going to be a big part of that now.

"One of the reasons the GDPR has been brought in is because things have changed so much since the Data Protection Act in 1998. Just think back to what we were doing in 1998 with data compared with what we are now all doing with social media, with fingerprint recognition and facial recognition, all that biometric stuff, and even CCTV.

"You think of all the interactions that now go on with data, and that's why this is coming in, because of the massive changes that have happened in our lives."

Kevin says the state of preparedness

WHAT THE GDPR IS NOT

- It is NOT just an IT issue
- It does NOT affect just electronic records
- It does NOT just affect your customers
- Your staff/employees are NOT exempt
- It is NOT a one-off exercise
- It is NOT going to go away or be delayed!

DATA SUBJECTS' RIGHTS

DATA subjects will be entitled to:

- Access their own personal data.
- Rectify inaccurate personal data
- Challenge automated decision making
- Object to direct marketing
- Right "to be forgotten"
- Right to data portability

head in sand data protection

for GDPR amongst a lot of small businesses he comes into contact with is "appalling".

"There is a lot of work to do and potentially it could be a bit costly. A lot of businesses may decide they haven't got the resources to deal with a lot of it, and will 'take the risk' - until we get a high-profile case where a small business gets a big fine and goes under."

Organisations will need to appoint part or full-time Data Protection Officers to supervise how they handle people's information, and every employee needs to understand their responsibility to protect customer data and handle it correctly in keeping with the new legislation.

Kevin says a lot of businesses will be writing to all the customers in their databases to obtain fresh permission to hold their information under the terms of the GDPR, deleting anyone who does not give full consent from their files.

"One positive about this is that once you have done that, your database should be a lot cleaner and stronger and you will have much more engaged customers," says Kevin. "And once you are compliant that could be a marketing opportunity. You can claim: 'We are GDPR compliant, your data is safe with us.'"

A good starting point towards GDPR compliance is to check out the advice on the ICO's own website. If nothing else, this will open your eyes to just how complex a task businesses face.

● Kevin Lovelady

You may well then need to call in the advice of expert consultants like Kevin on the digital side, and may also need to seek legal advice, though the services of experts in both areas are likely to be at a premium as pressure mounts in the final countdown to May 25.

ICO'S 12-STEP PLAN TO PREPARE FOR GDPR

AWARENESS
Make sure that decision makers and key people in your organisation know about the GDPR and appreciate its likely impact.

INFORMATION YOU HOLD
Document the personal data you hold, where it came from and who you share it with. You may need to conduct an information audit.

COMMUNICATING PRIVACY INFORMATION
Review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

INDIVIDUALS' RIGHTS
Check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

SUBJECT ACCESS REQUESTS
Update your procedures and plan how to handle requests within the new timescales and provide any additional information.

LAWFUL BASIS FOR PROCESSING PERSONAL DATA
Identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

CONSENT
Review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

CHILDREN
Do you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity?

DATA BREACHES
Make sure you have the right procedures in place to detect, report and investigate a personal data breach.

DATA PROTECTION BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS
Familiarise yourself with the ICO code of practice on Privacy Impact Assessments and work out how and when to implement them.

DATA PROTECTION OFFICERS
Designate someone to take responsibility for data protection compliance. Consider whether you are required to formally designate a Data Protection Officer

INTERNATIONAL
If you carry out cross-border processing in the EU, determine your lead data protection supervisory authority.