THE EUROPEAN UNION IS WATCHING YOU

The General Data Protection Regulation (GDPR) is the biggest piece of data protection legislation ever passed in the history of the European Union. When it comes into law in May 2018, it will have a profound effect – including the potential for multi-million euro fines – on the way organisations manage personal data, according to investigations by Richard Fitzpatrick

Next year the first EU regulation dealing with personal data will come into force. Entitled GDPR for shorthand, it will be ushered in by the European Union on 25 May 2018. It'll change all the rules about how organisations handle personal data, forcing them to take seriously data privacy for the first time after years of cavalier marketing and data harvesting.

Gary White, EMEA Sales Manager, Waterford Technologies, paints a provocative picture to illustrate what spurred the legislation into place: "GDPR was created because of the Internet of Things (IoT), the explosion of technology companies and the capturing and processing of citizens' data. Fifteen years ago, companies like Facebook and Snapchat didn't exist. Google was only a few years old.

Gary Whyte from Waterford Technologies

"Can you imagine if you explained to someone 15 years ago, that you would casually tell a company (that you had no relationship with) intimate details like your name, your address, your holiday destinations, your shopping preferences, your bank details, your likes, your dislikes, your friends, your girlfriends, where you like to eat, where you like to drink, whether you like pets, your political beliefs, your religious beliefs, your sexual orientation, your marital status? You'd be laughed at, and told that was something the Stasi did in East Germany a generation ago; nobody is that stupid.

"All of these companies are using huge amounts of data from EU citizens – and people around the world – for multiple reasons, but mainly to target you and me for advertisements, for political, banking and financial reasons.

"Data is today's currency the way salt was during the Roman Empire. If you imagine, and go back 15 years ago, that you had a lot of money and you went to your local bank and you gave them your money, there would be a reasonable expectation on your behalf that money was protected – that it would be put in nice, big vault. The vault had an alarm as well as a security guard.

"If we take the current situation, data is invaluable because you can identify so much about a person with the data points they cough up to companies. Your data should be protected like your money is, but it's not – it's been stored in unprotected, poorly resourced systems. Companies are also taking your data and selling it to other companies. An example would be Facebook. It's one of the largest purchasers of data in the world, as well as clawing data from their 1.2 billion users. They're buying this data to send targeted advertisements, to sell to you."

The GDPR is the most significant piece of data protection legislation to be passed in the history of the European Union. Paul Jordan, Managing Director, International Association of Privacy Professionals, has consulted with governments and data protection authorities across Europe over the last couple of years while the legislation has been put in place. He's been struck by its scale and ambition.

"Getting 28 EU member states to agree final text after six years of long, protracted negotiations is quite something. We have a very diverse culture in Europe. We have different ways of looking at data protection and privacy within the EU. Ireland and the UK, for example, are probably a bit more liberal in their approach and how they deal with businesses where-

as on the continent they are much more prescriptive.
"With an expanding EU, coming to a meaningful consensus on any piece of legislation is a remarkable feat. The GDPR has probably been the most lobbied piece of legislation in recent times in Europe. There were 6,000-7,000 tabled amendments on it. These weren't only from European companies – they came from companies from the United States and beyond, too. It's a very influential piece of legislation."

The fact that it will reach beyond the EU is one of its striking aspects. A global standard for data protection will be driven by GDPR. Corporations from outside its borders who trade with the EU, which is a top trading partner for approximately 80 countries, will have to abide by its stipulations. And the legislation has teeth to ensure compliance.

"What's really catching the headlines is the new top-end fine," says Bryan McCarthy, Partner and Head of Cyber and Data Protection with solicitors Ronan Daly Jermyn. "To give an example, the higher-tier provision will result in a maximum fine of up to 4% of a company's

Bryan Mccarthy from Ronan Daly Jermyn solicitors

preceding year's global, worldwide turnover or €20 million, whichever is greater. Compare that to the existing law where the maximum penalty applicable to most companies is €100,000.

"Take the example of Yahoo! In 2013, Yahoo! was hacked, which it disclosed in 2016. If we were to apply the newer higher-level administrative fine – in 2016, Yahoo!'s annual revenue was just north of $5 billion so it would be in line for a fine of $240 million. When I'm advising clients, though, I stress also the reputational harm that can be caused to a company by security breaches or, for example, if there is a data access request that hasn't been complied with correctly. Consumer groups have been closely monitoring the development of data subject rights and I know they will assist individuals to pursue fully their rights under GDPR."

The prevalence of data breaches and cyber attacks is widespread. According to a recent study by management consultants EY, three-quarters of Irish firms it analysed have come under siege in the last two years, and alarmingly, 55% of business leaders it polled said their organisations were unlikely to detect a serious cyber attack.

Under GDPR, citizens will have several rights, including the right to transfer any online data a company or, say, a public sector body like a county council has gathered on them and critically "the right to be forgotten", which means that any information stored on them will have to be erased from the company's corporate memory. It will ensure safeguards for citizens, but it will mean administrative and IT costs for organisations, which will have to deliver on these citizenry data requests free of charge.

"There is no company out there that can provide a 'one stop shop' to protect you from the 99 articles contained within GDPR," says White. "It came out 12 months ago. There is no way technology has advanced where it could protect against international data transfers, data breaches, email data leak prevention, BACCs content and so on. There is so much.

"A lot of money will be spent on consultancy fees advising companies on how to prevent getting a €20 million fine. A company like Waterford Technologies are GDPR experts, with certified data protection professionals. We solve the major problem of email, which is the biggest form of communication for a company."

According to the International Association of Privacy Professionals, as many as 11,800 mandated data protection officers (DPOs) will have to be employed in Europe alone over the next two years, and as many as 75,000 positions globally. Jordan stresses, though, that the legislation will bring in opportunity as well as headaches for companies grappling with GDPR.

"It's enshrining the fundamental rights to privacy in Europe. As consumers, we'll have enhanced consent rights, the right to access information, the right to be forgotten, data portability, which will create a lot of change for organisations and companies. There will have to be an overhaul in organisations. It's going to drive organisational and behavioural change, and will spur IT innovation and data protection tools, as we move forward into a new digital reality for consumers."