GDPR:
THE TIME TO ACT IS NOW

GDPR: THE TIME TO ACT IS NOW

You probably already know that new GDPR data protection laws are being introduced this month. But did you know that your business could be publicly shamed if you don't comply?

If you're thinking that data legislation is the last thing you want to be thinking about right now, I understand. It's certainly not the most scintillating of subjects.

But before you look away and do something else, **stop!**

This short educational guide has been created to help you get your head around GDPR and get it right, early and quickly.

Because honestly, this is something you really can't afford to ignore.

The penalties for getting it wrong are enormous, for all size businesses. Including yours.

And we're not just talking about the financial implications.

One of the biggest problems you'll have to face if you do get it wrong is having your company's data protection mistake made public to the rest of the world.

A BRIEF RECAP:
WHAT IS GDPR?
WHAT DO YOU HAVE TO DO?
AND WHAT ARE THE POTENTIAL PENALTIES?

1>

WHAT EXACTLY IS THE GDPR?

The European General Data Protection Regulation (GDPR) is the new, improved version of the Data Protection Act. It comes into force on 25th May 2018, and it will change the way organisations collect and manage the information they collect about customers.

The regulation is the new framework for data protection across the whole of Europe. According to the governing bodies behind it, GDPR has been designed to harmonise data privacy laws and protect the rights of individuals.

2>

WE ALREADY HAVE DATA PROTECTION LAWS. WHY DO WE NEED MORE?

Yes we do, but things have changed a lot since the last laws were passed. It's hard to imagine now, but back 1998 there was no such thing as smartphones and Facebook. Let's face it, the world is a very different place now and the change is long overdue. We're creating and collecting huge amounts of digital information every second, and the laws created twenty years ago just don't cut it any more.

3>

IS MY BUSINESS GOING TO BE AFFECTED?

Yes. All organisations that collect data – even just a name and number – will have to comply with the GDPR. There are more hefty requirements for businesses employing 250 staff or more, but all organisations that collect any kind of personal data are going to be affected.

You will also have an obligation to erase the data of any individual who exercises their "right to be forgotten". At any time, your customers can withdraw their consent to your storing or using their personal data and insist that you delete it.

4>

WHAT'S THE SCARIEST PART OF GDPR?

Critically, you must also ensure that your data cannot be lost or stolen. If it is, you must tell the Information Commissioner's Office within 72 hours. And you must also tell the people whose data has been breached.

In our view, that's the scariest part of GDPR. Especially in the world of hacking and data theft we live in today…

SO DATA BREACHES ARE THE THING TO FEAR. PROBLEM IS, YOUR STAFF CAN INADVERTENTLY BE YOUR GREATEST HEADACHE

The vast majority of data breaches are caused by human error. Let's take a look at a common scenario.

Office manager Nicole has had a tough day. The IT system has been playing up, people have been shouting at her to fix it, and the phone hasn't stopped ringing. She hasn't had a proper lunch break and she's tired and hangry.

At 4.30pm things have started to get better and she can finally see the light at the end of the tunnel.

The chief executive Mark left for an important meeting at 2pm, specifically asking only to be contacted in an absolute emergency. So when she receives an email from him reminding her she needs to transfer some money into a supplier's bank account, she thinks she must have forgotten something important and does it.

There's already been a bit of tension in the office and everyone knows not to argue with Mark when he's having a bad day. With her appraisal coming up, the last thing she wants to do is annoy him.

Besides, the email looks legit. All the headings are there, the names are right, the message is signed off with "sent from my iPhone". It's getting late, she wants to get home, what could possibly go wrong?

Unfortunately, Nicole's day has just got a whole lot worse and she doesn't even know it yet.

Turns out that what looked like a totally innocent and genuine request was a phishing email, carefully crafted by an expert cyber-criminal. The perpetrator registered a domain that looks almost exactly like the real thing, complete with all the right colours, fonts and names.

All it took was a little bit of Googling to obtain all the information they needed to create a horribly realistic scam, and now not only has poor old Nicole just wired some money across to the criminal's bank account, she's also unwittingly given them access to the company's business critical data.

Today she'll go home thinking it's been a headache but relieved it's all over. Little does she know that her day from hell hasn't even started yet, and soon the details of the cyber breach will be out there in the public realm for all to see.

That means loss of face, an astronomical fine, potential court case and Mark's wrath. Now that's what you really call a bad day at the office.

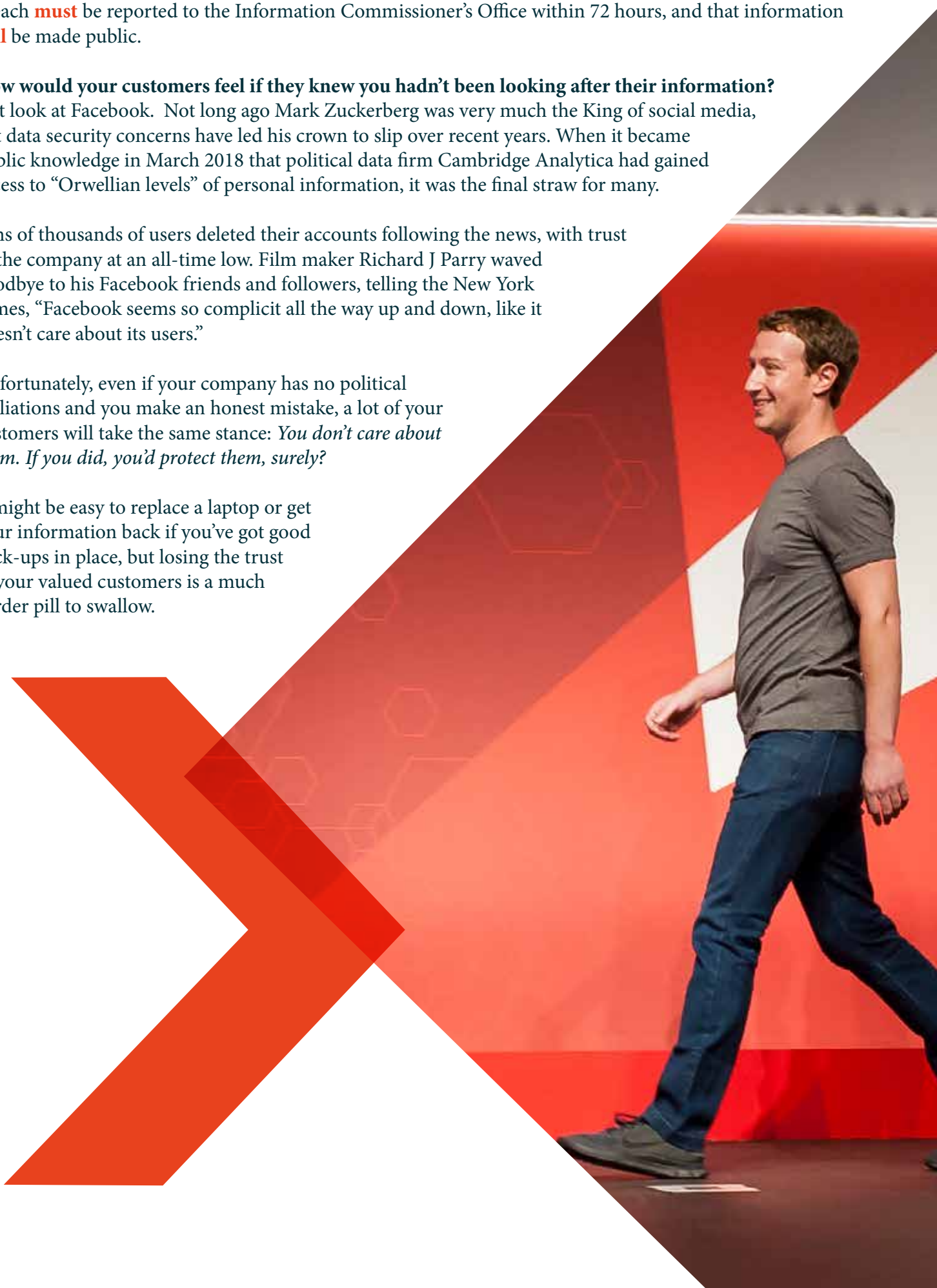
GDPR means that data breaches like this have the potential to totally destroy businesses.
That's because you can no longer sweep them under the carpet and hope nobody finds out. Now, every single breach **must** be reported to the Information Commissioner's Office within 72 hours, and that information **will** be made public.

How would your customers feel if they knew you hadn't been looking after their information?
Just look at Facebook. Not long ago Mark Zuckerberg was very much the King of social media, but data security concerns have led his crown to slip over recent years. When it became public knowledge in March 2018 that political data firm Cambridge Analytica had gained access to "Orwellian levels" of personal information, it was the final straw for many.

Tens of thousands of users deleted their accounts following the news, with trust in the company at an all-time low. Film maker Richard J Parry waved goodbye to his Facebook friends and followers, telling the New York Times, "Facebook seems so complicit all the way up and down, like it doesn't care about its users."

Unfortunately, even if your company has no political affiliations and you make an honest mistake, a lot of your customers will take the same stance: *You don't care about them. If you did, you'd protect them, surely?*

It might be easy to replace a laptop or get your information back if you've got good back-ups in place, but losing the trust of your valued customers is a much harder pill to swallow.



LET'S DIG A LITTLE DEEPER INTO WHAT GDPR MEANS FOR YOUR BUSINESS

You are required by law to report personal data breaches within three days. If the breach is likely to affect any individual's rights and freedom, you must tell them.

You must be able to demonstrate that you have adequate breach detection, investigation and reporting procedures in place.

You must keep a record of any personal data breaches, whether you have to notify the people involved or not.

The fines are massive. We're talking big figures here, up to €10 million or 2% of your global turnover (whichever is greater) for relatively small misdemeanors or €20 million or 4% of global turnover for big ones.

If the breach has a detrimental effect on an individual or group, it's really bad news.

You don't have to necessarily suffer a breach to be fined. You will still have to pay out if you fail to process someone's data correctly, fail to provide an individual with their data when requested or don't employ a data protection officer if required.

BREXIT IS IRRELEVANT

No matter how much people like us bang on about it, some companies are still of the opinion that they won't have to worry because Britain is leaving the EU. Nope.

Any company with employees located in the EU is obligated to comply. Brexit or not. Sorry about that.

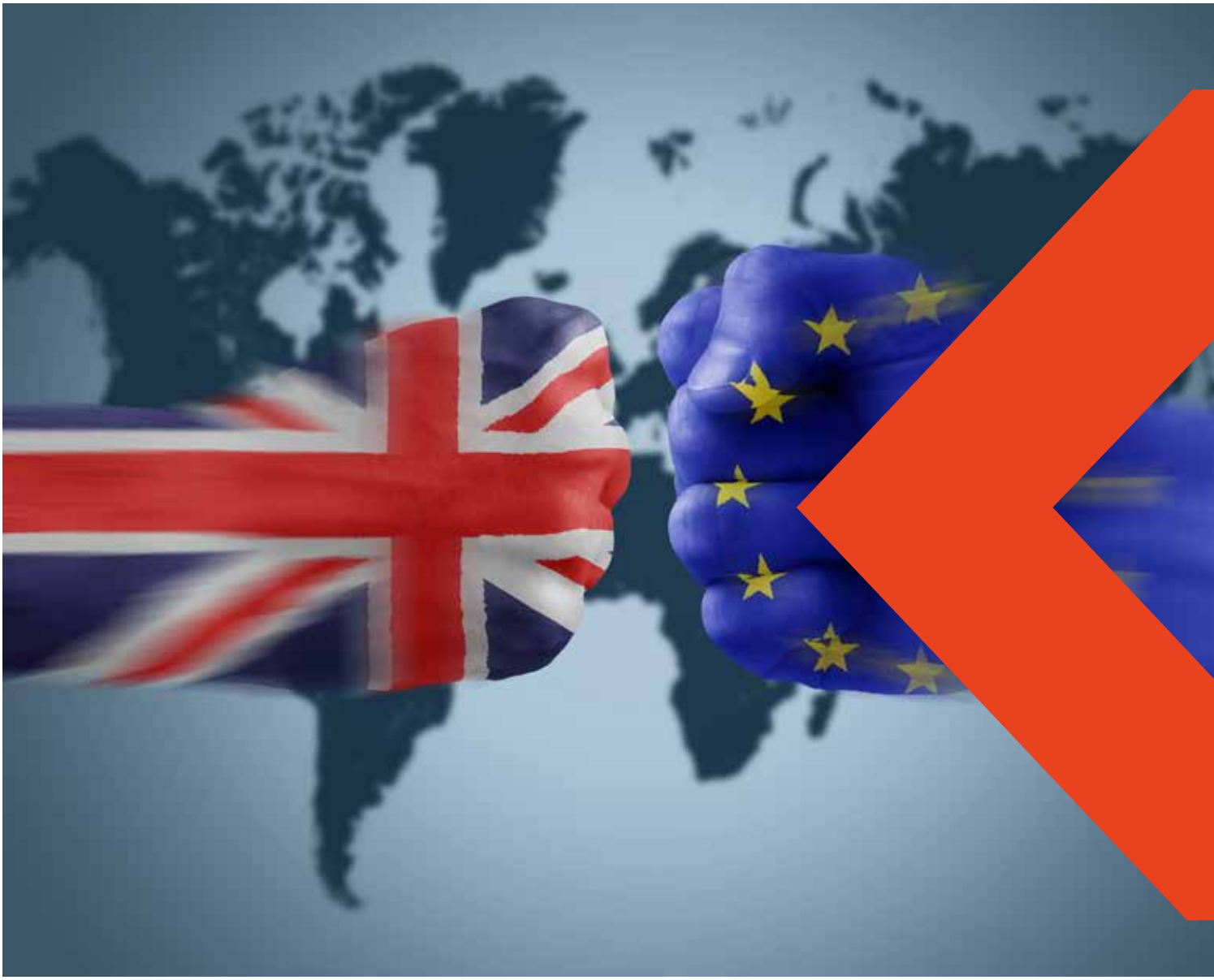
If you don't comply – either deliberately or by failing to plan – it can have catastrophic effects. Not to mention all the time and money you'll waste gathering all the information and dealing with the PR nightmare you'll be pulled into.

During the three days following a breach, you'll be faced with a barrage of questions and concerns. Your employees will panic. Morale will be at an all-time low.

You'll be frantically gathering information, trying to work out what went wrong and how you could have avoided this disaster. You'll need to get legal advice, check out your insurance, dig deep into the company funds and face the embarrassment of having your customers and your competitors find out what's happened.

Unless you're superhuman, that's going to have a knock on effect on your sleep, your health and your home life.

Is it worth it?



HERE'S THE GOOD NEWS.
IT DOESN'T HAVE TO BE THIS WAY.

The best way to stop data breaches like this happening is to take a proactive approach. Prevention is always, always better than cure. That means having robust security protocols in place and doing everything you can to keep your customers' details safe and sound.

How?

By outsourcing your data security to a crack team of experts who know their way around the GDPR.

Let's face it, you're already busy enough, so attempting to handle something as big as this yourself is asking for trouble.

The EU legislation is unwieldy. There are 99 articles, and they don't make light reading. My team and I understand the data security aspects of this legislation.

We'll ensure you have all the right levels of protection for your network and all your devices.

And we'll help you sleep better at night.

Please, please don't let complacency destroy the reputation you've worked so hard to build.

Don't take your eye off the ball, and don't become a GDPR statistic.

Let us help you.