GDPR | GENERAL DATA PROTECTION REGULATION

GDPR six months on

why burying your head in the sand is a terrible idea.

A special Q&A guide

GDPR | GENERAL DATA PROTECTION REGULATION

GDPR six months on – why burying your head in the sand is a terrible idea.

The following few paragraphs are to be read in the voice of David Attenborough:

"All around the United Kingdom, flightless birds are afraid. These impressive, yet nervous creatures try to go about their daily lives as if nothing is wrong, but the threat of a vicious predator casts a dark shadow over everything they do.

Painfully aware that the predator may strike at any minute, but too weighed down by other important tasks like feathering their nests, the ostriches choose to bury their heads in the sand.

Desperately hoping that if the enemy can't see them it won't attack, they adopt this graceless pose for days, weeks… even months.

Sadly, their efforts to remain unnoticed are futile. Hunters are well aware of this avoidance tactic, and slowly but surely they make their way through the terrified ostriches, leaving nothing but devastation and empty nests in their wake."

The ostrich effect is common among humans. We bury our heads in the sand to avoid unpleasant information and pretend that everything is ok, even if the world is falling apart around us. While the "out of sight, out of mind" approach can seem attractive in the short term, the bottom line is that problems continue to exist – and get bigger – the longer we ignore them.

Six months on from the implementation of the General Data Protection Regulation (GDPR), there's an alarming amount of ostrich activity going on. Recent research has shown that 70% of companies are still not fully compliant and are yet to get their heads around what's expected of them.

A new study by office equipment company Fellowes found that 17% of employees still haven't been provided with new data protection guidance, and one in ten don't know who in their organisation is responsible for the GDPR. A further 33% admitted to regularly leaving confidential data unattended.

The reasons for this slow uptake vary. In some organisations, it comes down to a genuine lack of understanding about the

new laws. In others, it's about being overwhelmed and seeing the development of new policies as just another onerous task on the to-do list that they'll get around to when they have the time.

Other managers just think it's a lot of fuss over nothing – the likelihood of any major data problem arising is minimal, and it's just an excuse for IT security people to take their money. After all, nobody's even been fined yet.

And that's the important word – YET.

The European Data Protection Supervisor, Giovanni Buttarelli, recently told Reuters to expect the first round of fines to take place by the end of the year. The commissioners have reportedly been "overwhelmed" with consumer complaints since the GDPR came into force on May 25th, and when do come to enforcing them, the fines won't be small.

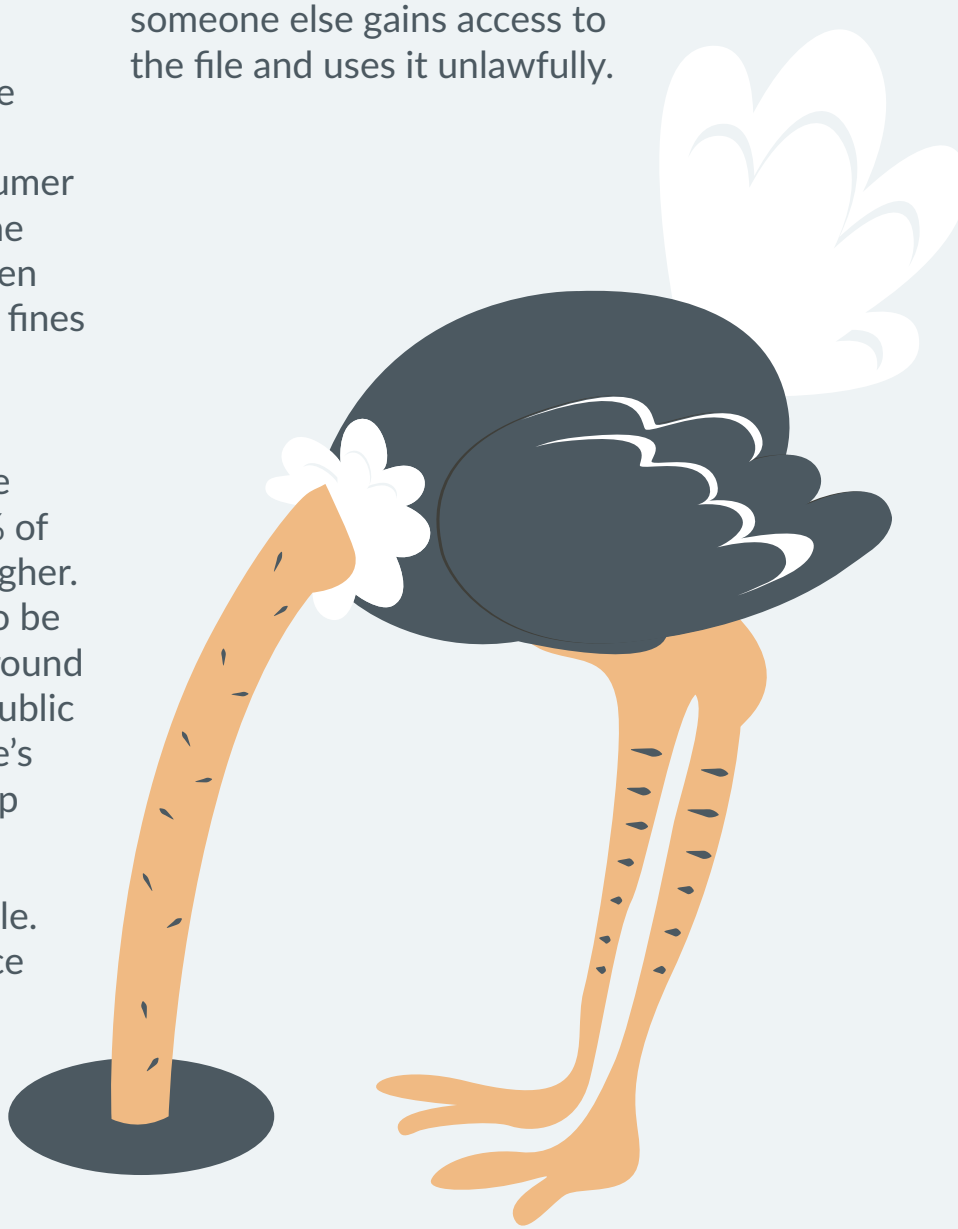
Any organisation found to be in breach of the new rules will face fines of up to €20 million, or 4% of global revenue - whichever is higher. Buttarelli believes those likely to be sanctioned will come from all around the EU, including a number of public bodies. He also warns that there's no excuse for companies to keep dragging their feet:

"E-privacy is simply indispensable. It is essential, it is a missing piece in the jigsaw of data protection and privacy. (Failure to update) would really be a dereliction of duty."

On the flip side, the Information Commissioner's Office - the UK's own data protection body - has been inundated with calls that don't meet the threshold for a data incident.

While it's encouraging that these organisations are taking their obligations seriously, it demonstrates a huge lack of understanding about the GDPR and what it really means for businesses.

Many reports received by the ICO are incomplete or unnecessary, suggesting that companies think they need to report everything data related, like someone leaving their desk for 30 seconds with a client file on display. While this is clearly bad practice, it's not a breach until someone else gains access to the file and uses it unlawfully.



Q&A

WHAT IS IT?

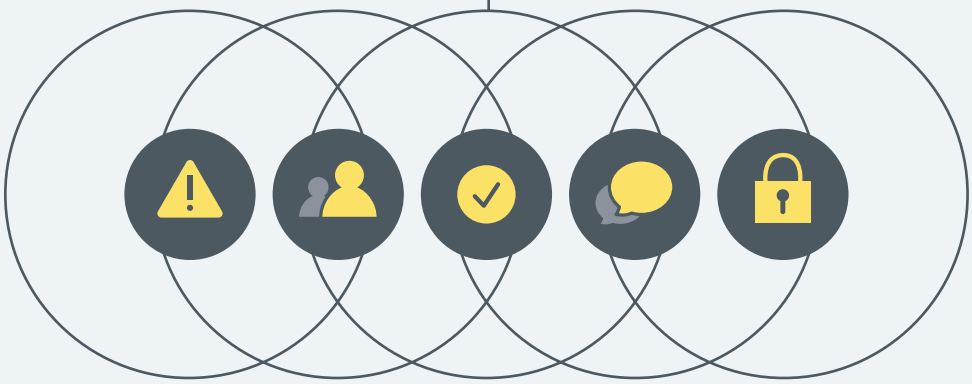
The General Data Protection Regulation strengthens the data rights of EU residents across all member states. It makes it easier for people to access the information companies hold about them and increases the punishments for misusing – and losing – data.

WHY WAS IT INTRODUCED?

The world has changed since the previous regulations (the European Data Protection Directive of 1995 and the UK Data Protection Act of 1998) were introduced. The new laws address the threats of online communication and information sharing, such as through social media and internet shopping.

WHEN DID IT COME INTO EFFECT?

The GDPR was officially introduced on 25th May 2018.



WHAT ABOUT BREXIT?

Because the UK government only triggered Article 50 in March 2017, the GDPR took effect before the legal consequences of the Brexit vote - so the UK must still comply.

WHAT'S THE DIFFERENCE BETWEEN A DATA CONTROLLER AND A DATA PROCESSOR?

A data controller defines the terms (how and why) of data processing, but doesn't necessarily carry out these activities themselves.

A data processor is a third party that performs the actual data collection and processing.

SO, AM I A CONTROLLER OR A PROCESSOR?!

The determining factor here is control of data, not possession. If you determine why you need to collect the information and what you're going to do with it, you're a controller. That might mean you're a high street retailer using customer data to inform marketing campaigns, or a charitable organisation collecting information that helps you provide a better service to your beneficiaries.

If you just collect information on behalf of another party, you're a processor. That might mean you're an IT company employed to store data remotely in a server on behalf of a client, or someone who compiles lists for someone else.

It's the controller's job to ensure the processor complies with data protection law, while processors must maintain adequate records of all their processing activities.

HOW AM I SUPPOSED TO PROCESS DATA UNDER THE NEW REGULATION?

All personal data must be processed lawfully, transparently, and for a specific reason. That means you must explain to everyone why you collect their data, what you do with it, and – if appropriate – how it meets any contractual or legal obligations.

HOW AM I SUPPOSED TO OBTAIN CONSENT FOR ALL THIS?

Consent must be actively agreed by the subject – a simple opt-out or pre-ticked box isn't good enough. Guidance on the ICO website says you should:

- keep your consent request separate from your general terms and conditions, and clearly direct people's attention to it;
- use clear, straightforward language;
- adopt a simple style that your intended audience will find easy to understand – this is particularly important if you are asking children to consent, in which case you may want to prompt parental input and you should also consider age-verification and parental-authorisation issues;
- avoid technical or legal jargon and confusing terminology (eg double negatives);
- use consistent language and methods across multiple consent options; and
- keep your consent requests concise and specific, and avoid vague or blanket wording.

Controllers must keep records of how and when an individual gave consent, and make it clear that the individual is free to withdraw that consent at any time.

WHAT IS "PERSONAL DATA" ANYWAY?

These days, personal data is about more than names and addresses. It can also include online identifiers like IP addresses and other information like economic, cultural or health information.

HOW CAN SOMEONE COLLECT THE INFORMATION WE HOLD ABOUT THEM?

GDPR states that individuals are able to request their data at "reasonable intervals", and provided with that data within a month.

People have the right to access any information a company holds on them, how long it's stored for, and who gets to see it.

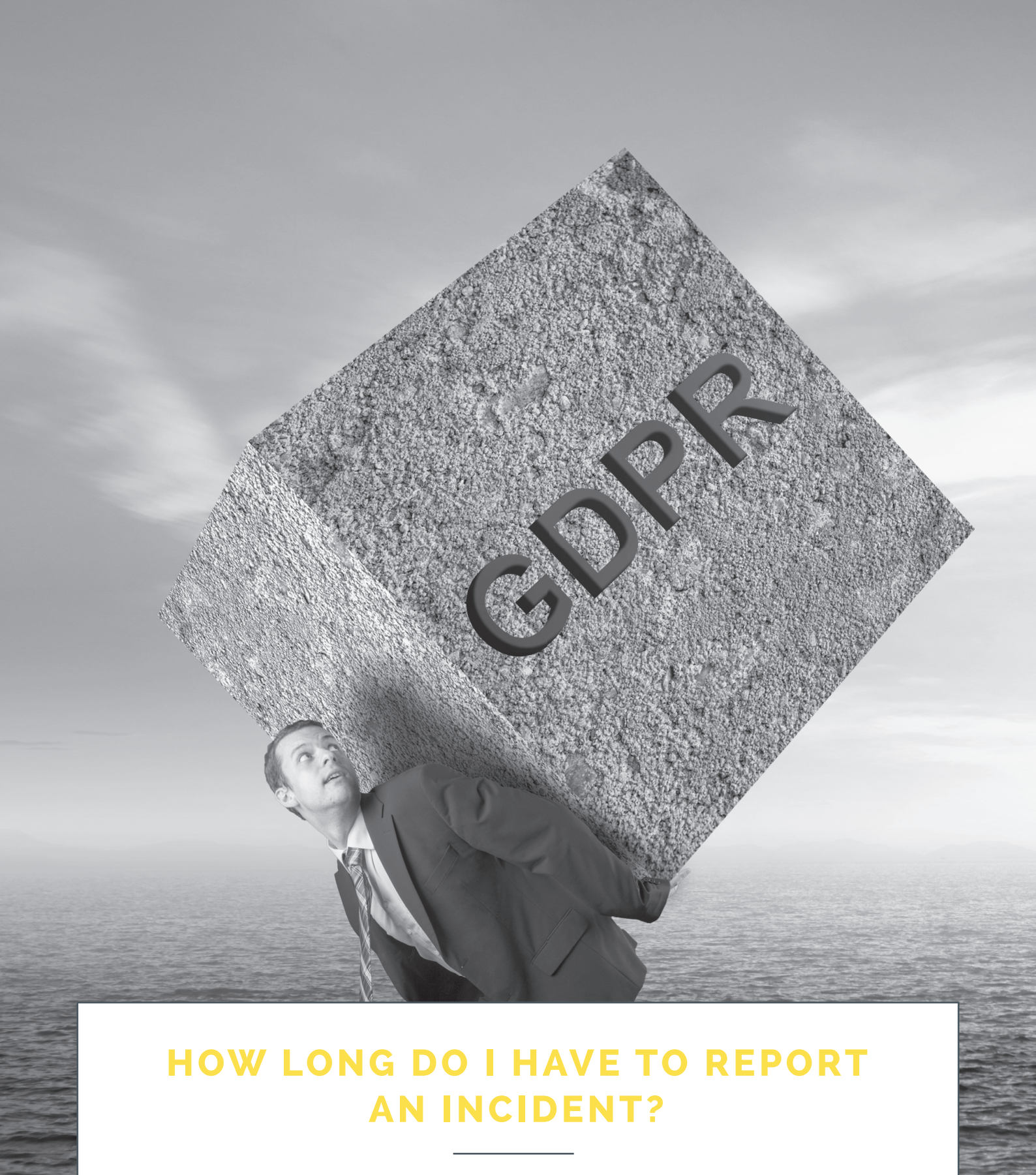
They can also ask for that data, if incorrect or incomplete, to be changed whenever they want.

Transparency is a key element – if you're using old fashioned terms and conditions, it's time to have them re-written in a more user-friendly way.

WHAT'S "THE RIGHT TO BE FORGOTTEN" ALL ABOUT?

Anyone you collect data on has the right to have it deleted if it's no longer relevant; e.g. if you no longer need it for the purpose originally used for.

If the data was collected under the consent model, an individual can withdraw this consent whenever they like – this might be because they object to how it's being used, or simply don't want to be included any more.



HOW LONG DO I HAVE TO REPORT AN INCIDENT?

All data breaches must be reported to the ICO within 72 hours of you becoming aware.

That's 72 actual hours, not working ones, so if you discover a problem at 9am on Monday you'll need to report it by the same time Thursday.

DO I NEED TO EMPLOY A DATA PROTECTION OFFICER?

You'll need a data protection officer if you're the head of a public body or any company whose core activities involve monitoring individuals "on a large scale". You don't necessarily have to employ them directly though – several public bodies can share the same data protection officer.

COME ON, AM I SERIOUSLY LIKELY TO GET FINED MILLIONS?

Two tiers of fines exist under GDPR, both of which are much bigger than any the UK has seen before.

Under the Data Protection Act 1998, the ICO was able to fine companies a maximum of £500,000. Under the GDPR, that figure rises to €20 (£17.6) million. While such hefty sums will be reserved for huge data breaches and wilful neglect of obligations, the enforcers have made it clear they're not playing games here. If you don't comply, expect to lose a lot of money along with your reputation.

But the bigger risk that a fine is the risk to your reputation. If you lose data, for example, you have to tell the people whose data you lost. In the case of a lost laptop containing thousands of client details, that could be very embarrassing for your business.

And if you are found to be in breach of GDPR, your company's details will be published by the ICO. That's something that's going to come up in Google searches for years to come.

FINAL QUESTION: WHAT CAN YOU DO TO HELP ME?

The bottom line is this. If you're still not fully compliant with the GDPR, you can't go on sticking your head in the sand. The fines are on their way, and by the end of the year lots of companies will find themselves significantly out of pocket. That's bad enough for the big fish, but smaller businesses who just didn't manage to get around to sorting things out have the most to lose.

Here's what we can do to help. We can make sure that from a technology point of view, you are fully up-to-date and protected.

That means making sure your data is safe and accounted for at all times. And you don't have to worry if someone in your business makes a small mistake, such as leaving a laptop on a train.

Essentially – we will give you peace of mind about the security of your data under GDPR.

So you can get your head out of that sand and dare to look at the light again.

Contact us today