GDPR – sorting the fact from the fiction
By Elizabeth Denham, Information Commissioner.

The General Data Protection Regulation comes into force on 25 May 2018.
That's not new news. But it is a fact.
It's also fact that not everything you read or hear about the GDPR is true.
For the most part, writers, bloggers and expert speakers have their facts straight. And what they say – and sometimes challenge – helps organisations prepare for what's ahead.
And there's a lot to take in. The Data Protection Bill announced this week gives more detail of the reforms beyond the GDPR, for example.
But there's also some misinformation out there too. And I'm worried that the misinformation is in danger of being considered truth.
"GDPR will stop dentists ringing patients to remind them about appointments" or "cleaners and gardeners will face massive fines that will put them out of business" or "all breaches must be reported under GDPR". I've even read that big fines will help fund our work.
For the record, these are all wrong.
If this kind of misinformation goes unchecked, we risk losing sight of what this new law is about – greater transparency, enhanced rights for citizens and increased accountability.
So, I want to set the record straight. I want to bust the myths. Because I know that most organisations want to get the GDPR right when it comes into force in 289 days.
This is the first in a series of blogs to separate the fact from the fiction. We'll be publishing future myth-busting blogs on consent, guidance, the burden on business and breach reporting.
Myth #1:
The biggest threat to organisations from the GDPR is massive fines.
Fact:
This law is not about fines. It's about putting the consumer and citizen first. We can't lose sight of that.
Focusing on big fines makes for great headlines, but thinking that GDPR is about crippling financial punishment misses the point.
And that concerns me.
It's true we'll have the power to impose fines much bigger than the £500,000 limit the DPA allows us. It's also true that companies are fearful of the maximum £17 million or 4% of turnover allowed under the new law.
But it's scaremongering to suggest that we'll be making early examples of organisations for minor infringements or that maximum fines will become the norm.
The ICO's commitment to guiding, advising and educating organisations about how to comply with the law will not change under the GDPR. We have always preferred the carrot to the stick.
Our Information Rights Strategy – a blueprint for my five-year term in office – confirms that commitment.
And just look at our record:
Issuing fines has always been and will continue to be, a last resort. Last year (2016/2017) we concluded 17,300 cases. I can tell you that 16 of them resulted in fines for the organisations concerned.
And we have yet to invoke our maximum powers.
Predictions of massive fines under the GDPR that simply scale up penalties we've issued under the Data Protection Act are nonsense.
Don't get me wrong, the UK fought for increased powers when the GDPR was being drawn up. Heavy fines for serious breaches reflect just how important personal data is in a 21st century world.
But we intend to use those powers proportionately and judiciously.
And while fines may be the sledgehammer in our toolbox, we have access to lots of other tools that are well-suited to the task at hand and just as effective.

Like the DPA, the GDPR gives us a suite of sanctions to help organisations comply – warnings, reprimands, corrective orders. While these will not hit organisations in the pocket – their reputations will suffer a significant blow.
And you can't insure against that.