GDPR Mythbusters

Mark Smith, Founder & CEO
5 March 2018

The General Data Protection Regulation ("GDPR") comes into force in less than three (3) months – on May 25th 2018 – yet misleading statements and articles about the new law continue to persist.

In the second half of 2017 the UK's data protection regulator, the Information Commissioner's Office ("ICO") published a series of blog posts intended to dispel a number of GDPR-related myths, as it was becoming worried that certain misinformation was in danger of being considered truth. It was also concerned that some of the misinformation and outright scaremongering appeared to be commercially driven, particularly with respect to businesses selling "off the shelf" GDPR solutions.

These very helpful blog posts have been summarised in this "GDPR Mythbusters" article, which discusses the nine (9) common misconceptions about the GDPR identified by the ICO. Note that regulators in other EU countries may of course take a different approach in certain areas.

For those that want to read the full blog posts, they are still available on the ICO blog at: https://iconewsblog.org.uk.

1. Enormous multi-million-pound ICO fines will become routine after May 25th.

One of the key myths that the ICO is keen to bust is that the focus of the GDPR is on the introduction of huge fines.

Whilst the ICO recognises that focusing on big fines makes for great headlines, in its view thinking the GDPR is all about new fining powers misses the point, which is that the GDPR is about putting consumers and citizens first.

The ICO will certainly have powers under the GDPR to impose fines way in excess of the current limit of £500,000 – up to €20 million or 4% of global annual turnover, whichever is the higher, for the most serious breaches. This fact has undoubtedly been helpful in ensuring that the GDPR has received boardroom level attention.

However, the ICO has made it clear that it is scaremongering to suggest that it will be making early examples of organisations for minor breaches or that maximum fines will become the norm. In particular, predictions that the ICO will simply scale up the fines it has issued under existing legislation if similar breaches occur under the GDPR have been described as nonsense. The ICO has said it will use its fining powers proportionately and judiciously and has highlighted that it will have a range of other sanctions at its disposal under the GDPR, from warnings and reprimands to corrective orders, all of which could lead to significant reputational damage for the organisations concerned.

For context, in 2016/2017 the ICO concluded 17,300 cases, only sixteen (16) of which resulted in fines. Moreover, it is worth remembering that the ICO has yet to invoke its maximum fining powers under the current laws.

In a recent podcast Elizabeth Denham, the Information Commissioner, remarked that the ICO has always preferred the carrot to the stick, and that it will continue to do so. That said, she also mentioned that it will not be afraid to use its fining powers where organisations play fast and loose with personal data.

2. You must have consent if you want to process personal data.

The ICO acknowledges that there has been an understandable focus on consent as the GDPR is generally raising the bar and clarifying the requirements that must be met in order for consent to be valid.

For example, the GDPR explicitly sets out that pre-ticked opt-in boxes are not indications of valid consent and clearly mandates that organisations have to make it easy for individuals to withdraw their consent. Organisations need to check that existing consents they have on file meet GDPR standards – if not, they'll need refreshing.

However, the ICO has also become aware of myths such as "data can only be processed if an organisation has explicit consent to do so" being perpetuated. This simply isn't the case, as there are five other lawful bases for processing personal data under the GDPR, which may be more appropriate depending on the context. These are made up of the "contract", "legal obligation", "vital interests", "public task" and "legitimate interests" bases. Consent is not the only option!

Organisations should remember that whatever lawful basis they use for processing personal data they must document their decision so that they can demonstrate compliance with the GDPR's accountability rules.

3. Organisations can't start planning for the GDPR's new consent rules until the final version of the ICO's formal guidance is published.

For organisations that do intend to rely on consent as the lawful basis for some or all of their processing of personal data, the ICO has another myth it wants to explode – that organisations can only start their GDPR preparations in this regard once the ICO has published its finalised guidance on consent.

The ICO held a public consultation on draft consent guidance in March 2017, but a finalised version has not yet been published. This is because the ICO decided it should wait for the Article 29 Working Party ("A29WP") to publish its Europe-wide consent guidance to ensure consistency. The A29WP published draft guidance on consent for consultation on 12 December 2017. The consultation closed on 23 January 2018, but we are still awaiting the final version.

The ICO has made it clear that a lack of finalised guidance is no excuse for not making preparations for the GDPR rules on consent. It has highlighted that its draft guidance is a good place to start for the time being – as is the draft A29WP guidance – and that it is unlikely that it will change significantly in its final form.

4. The GDPR is an unnecessary and costly burden on organisations.

The ICO is keen to stress that the new GDPR regime is an evolution, not a revolution, in data protection. The GDPR is building on foundations that have been in place for the last twenty (20) years.

If an organisation is already complying with the terms of the Data Protection Act and takes data protection seriously then it will already be well on the way to being ready for the GDPR.

Indeed, many fundamentals of data protection law remain the same, such as fairness, transparency, accuracy, security and respecting data subject rights. That is not to say that organisations should be complacent – there are certainly new provisions to comply with and they should be preparing accordingly – but from the ICO's perspective the GDPR is a step change rather than the leap into the unknown that some commentators have been suggesting.

The ICO has also emphasised that the GDPR scales the task of compliance to the level of risk involved in the data processing in question. It argues that many of the actions that SMEs should take are practical and straightforward, though those handling particularly sensitive data or processing personal data in particularly intrusive ways will of course have a higher compliance burden.

Moreover, the ICO's view is that building trusted relationships with the public will allow organisations to sustainably build their use of data and derive more value from it in the longer term. It will also mean that organisations will avoid the reputational damage and consequent loss of customers that can result from getting data protection wrong.

5. All personal data breaches will need to be reported to the ICO.

Another myth the ICO would like to bust is that all data breaches must be reported to it.

Under the GDPR it is mandatory to report a personal data breach if it is likely to result in a risk to people's rights and freedoms. Hence, if a particular breach is not likely to result in a risk to people's rights and freedoms, you don't need to report it.

This is a new requirement, as under current UK data protection law personal data breach reporting is best practice but not compulsory for most organisations, and it will naturally lead to changes to the way personal data breach situations are handled. It is clearly not, however, as onerous a requirement as having to report all personal data breaches.

The ICO recommends that organisations examine the possible data breach scenarios they face and develop a sense of what constitutes a serious incident in the context of their customers and data.

Remember that if the data breach involves a high risk to people's rights and freedoms, it will also need to be reported to the individuals affected. ICO guidance suggests that high risk situations are likely to include those where there is a high risk of the individuals in question suffering a significant detrimental effect, such as discrimination, damage to reputation or financial loss.

6. All details need to be provided as soon as a personal data breach occurs.

Where organisations are required to report a personal data breach under the GDPR they must do so without undue delay and, where feasible, no later than seventy-two (72) hours after having become aware of it.

The ICO has been keen to underline, however, that where the organisation does not have all of the details available, more can be provided later. It will not expect to receive comprehensive reports at the outset of a data breach coming to light, but it will want to know the potential scope and cause of the breach, the mitigation action the organisation plans to take, and the steps that will be taken to address the problem.

7. If you don't report a data breach in time a fine will always be issued and the fines will be huge.

Under the GDPR the ICO will have the ability to issue fines for failure to notify a personal data breach and for failure to notify a personal data breach on time.

The ICO considers it important that organisations that systematically fail to comply with the law or completely disregard it, particularly where significant data privacy risks are involved, are aware of this.

However, as stated earlier, the ICO has also provided reassurance that fines under the GDPR will be proportionate and not issued for every infringement. In the case of personal data breaches it suggests that fines can be avoided if organisations are open and honest and report without undue delay.

8. Data breach reporting is all about punishing organisations.

The ICO asserts that data breach reporting is designed to push organisations to improve their ability to detect and deter breaches, rather than being all about punishing them. Having more information on data breaches also allows the ICO to look for trends, patterns and wider issues in relation to organisations, sectors or types of technologies.

Organisations have been encouraged to prepare for the new data breach reporting regime by ensuring that they have the roles, responsibilities and processes in place for reporting. This is particularly important for larger organisations that have multiple sites or business lines.

More information about how to report a personal data breach to the ICO is available at: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach.

9. GDPR compliance is focused on a fixed point in time – it's like the Y2K Millennium Bug.

The ICO's final GDPR mythbusting blog post highlighted that comparisons between the GDPR and the Y2K Millennium Bug are way off the mark.

Whilst the predictions have not been as apocalyptic as the stories in late 1999 that planes would fall out of the sky or important computer systems would crash when the clock struck midnight on 1 January 2000, there have clearly been anxieties aplenty about the GDPR.

However, GDPR compliance will be an ongoing journey rather than something that will happen on a particular date and can then be forgotten about. Organisations will need to make an ongoing effort to identify new privacy and security risks.

Also, unlike the Y2K Millennium Bug, which turned out to be a false alarm, with the GDPR we all know what is coming. Much of it builds on existing data protection law and the ICO has published a considerable amount of guidance. Help is also available from the A29WP, industry bodies and data protection experts.

Finally, whilst there will be no "grace" period after May 25th, the ICO has said that it prides itself on being a fair and proportionate regulator, and that this will continue under the GDPR. Organisations that self-report, engage with the ICO to resolve issues and demonstrate effective accountability arrangements can expect this to be taken into account when the ICO considers any regulatory action. If organisations can demonstrate that they have the appropriate systems and thinking in place, the ICO claims they will find it to be a proactive and pragmatic regulator aware of business needs and the real world.

Businesses with queries about the GDPR or that require further information on any of the issues discussed above are welcome to get in touch by e-mailing me at mark.smith@purdysmith.com.