ROPES & GRAY

ALERT

London

October 24, 2017

The UK's Data Protection Authority goes myth-busting: fining powers; consent; the "misconception" that the GDPR is an unnecessary burden; and data breach reporting

Attorneys
Rohan Massey

The UK's Information Commissioner's Office has published a series of blog pieces to "*bust some myths*" about the General Data Protection Regulation, which comes into effect on 25 May 2018. According to the Information Commissioner, Elizabeth Denham, "*there is a lot of misinformation out there …*" and "*I am worried that the misinformation is in danger of being considered truth*". She gives the following examples: "*the 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*". All of these are wrong. The blog series seeks to sort the fact from the fiction and covers: (i) the ICO's fining powers; (ii) the issue of consent; (iii) the "misconception" that the GDPR is an unnecessary burden on organisations; and (iv) data breach reporting.

Myth 1: the biggest threat to organisations from the GDPR is massive fines

"*This law is not about fines*", Ms Denham says. "*It's about putting the consumer and citizen first. We can't lose sight of that.*"

It is true that the ICO will have the power to impose fines much bigger than the £500,000 limit the law currently allows, Ms Denham explains. It is also true that the maximum penalty that can be imposed will be a huge £17 million or 4% of annual global turnover allowed under the new law. But, she describes it as "*scaremongering*" to suggest that the ICO will be making early examples of organisations for minor infringements or that maximum fines will become the norm.

Ms Denham says that 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*".

Issuing fines has always been and will continue to be, a last resort, Ms Denham continues. Last year (2016/2017) the ICO concluded 17,300 cases, only 16 of which resulted in fines for the organisations concerned.

In addition, the ICO has, in fact, still not invoked its maximum powers.

However, Ms Denham says, heavy fines for serious breaches reflect just how important personal data is in a 21st century world. But the ICO intends to use those powers "*proportionately and judiciously.*" They are also not the only tools in the ICO's toolbox. There are "*lots of other tools that are well-suited to the task at hand and just as effective.*"

Like the DPA, the GDPR gives the ICO a suite of sanctions to help organisations comply: warnings, reprimands, corrective orders. Using these does not hit organisations in the pocket, but they can deal a significant blow to their reputations, Ms Denham says.

Myth 2: you must have consent if you want to process personal data

Here, Ms Denham says, it is true that the GDPR is raising the bar to a higher standard for consent.

However, under data protection law consent "*has always required a clear, affirmative action*". All the GDPR does is clarify that pre-ticked opt-in boxes are not indications of valid consent.

The GDPR is also explicit, she says, in stating that organisations must make it easy for people to exercise their right to withdraw consent. The requirement for clear and plain language when explaining consent is now "*strongly emphasised*", she says. Further, organisations must make sure the consent they already have meets the standards of the GDPR. If not, it will have to be refreshed.

Ms Denham says that she has heard some "*alternative facts*". For example, that "*data can only be processed if an organisation has explicit consent to do so*". Ms Denham explains that the rules around consent "*only apply if you are relying on consent as your basis to process personal data*". In other words, consent is one way to comply with the GDPR, but it's not the only way.

The new law provides five other ways of processing data that may be more appropriate than consent, Ms Denham explains. "Legitimate interests" is one such ground and the ICO recognises that organisations want more information about it. Guidance will be published next year.

Myth 3: I can't start planning for new consent rules until the ICO's formal guidance is published

For those organisations that do rely on consent, there is no need to wait for the ICO final guidance on the subject before beginning preparations to comply with the new rules, Ms Denham says. The ICO is waiting until Europe-wide consent guidelines have been agreed before it publishes its final guidance. The current timetable is December.

However, Ms Denham says the ICO's draft guidance on consent is "*a good place to start right now*". It is "*unlikely that the guidance will change significantly in its final form*". Finally, when the formal guidance on consent is published, it will not include guidance on legitimate interests or any other lawful bases for processing.

Myth 4: GDPR is an unnecessary burden on organisations

This blog piece by Steve Wood, Deputy Commissioner (Policy), was published to deal with the misconception that the new regime is an "*onerous imposition of unnecessary and costly red tape*". Mr Wood says that, in fact, the new law is "*an evolution in data protection, not a revolution*".

Mr Wood explains that the ICO recognises that the GDPR is no different from any other new legislation in that it will have some sort of impact on an organisation's resources. However, thinking about burden indicates "*the wrong mindset to preparing for GDPR compliance*", he says.

The GDPR demands more of organisations in terms of accountability for their use of personal data and enhances the existing rights of individuals. The GDPR is in fact building on foundations already in place for the last 20 years.

Organisations that already comply with the terms of the DPA, and have an effective data governance programme in place, are already well on the way to being ready for the GDPR. Many of the fundamentals remain the same and have been known about for a long time, Mr Wood explains. Fairness, transparency, accuracy, security, minimisation and respect for the rights of the individual whose data an organisation wants to process, are all things they should already be doing with data. The GDPR seeks only to build on those principles.

That does not mean, however, that there is any room for complacency, Mr Wood warns. There are new provisions to comply with and organisations should start making preparations now, if they have not done so already. "*But by and large, the new GDPR regime represents a step change, rather than a leap into the unknown*", he says.

Much of the criticism about the GDPR has focused on the perceived burdens it will place on SMEs and smaller organisations. However, Mr Wood continues, many of these criticisms fail to recognise the flexibility that the key principles in the DPA and GDPR provide: they scale the task of compliance to the risk. Many of the principles reinforce tasks businesses will already undertake in relation to record keeping, for example, the principle on data minimisation.

The principles are essentially the same for small businesses and multinational corporations. It is not the size of the organisation that is relevant so much as the risk that particular businesses and types of data processing pose, Mr Wood says, for example, those handling particularly sensitive data, or processing personal data in potentially intrusive ways.

Whatever the size of the organisation, the GDPR is essentially about trust, Mr Wood says: "*Building trusted relationships with the public will enable you to sustainably build your use of data and gain more value. Through changing their data handling culture, organisations can derive new value from customer relationships.*"

On the other hand, failing to get data protection right is likely to damage reputation, customer relationships and, ultimately, finances.

The ICO's annual research on privacy and data protection consistently shows that levels of public trust remain low. Conversely, it also shows that they would be more willing to provide their data, and for different uses, if they felt they could trust organisations to handle it fairly, securely and responsibly. Mr Wood says that this provides "*a major opportunity and competitive advantage for those who can demonstrate that they get data protection right.*"

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

Here, Ms Denham explains that under the new GDPR it will indeed be mandatory to report a personal data breach if it is likely to result in a risk to people's rights and freedoms. However, if there is no such risk, there is no need to report.

In fact, Ms Denham continues, under the current UK data protection law, most personal data breach reporting is best practice, but not compulsory. Ms Denham recognises that mandatory reporting of a personal data breach that results in a risk to people's rights and freedoms under the GDPR will be a new requirement for many. Therefore, the new GDPR reporting requirements will mean some changes to the way businesses, organisations (and the ICO) identify, handle and respond to personal data breaches.

Ms Denham explains that the threshold to determine whether an incident needs to be reported to the ICO depends on the risk it poses to people involved. Pan-European guidelines will assist organisations in determining thresholds for reporting, but the best approach will be, she says, for organisations to start examining the types of incidents they face and develop a sense of what constitutes a serious incident in the context of their data and their customers.

Organisations need to remember that if there is the likelihood of a *high* risk to people's rights and freedoms, they will also need to report the breach to the individuals who have been affected.

The ICO has provided some initial guidance in its GDPR overviews that high risk situations are likely to include the potential of people suffering significant detrimental effects, for example, discrimination, damage to reputation, financial loss, or any other significant economic or social disadvantage.

If organisations are not sure about who is affected, Ms Denham says that the ICO will be able to advise and, in certain cases, order them to contact the people affected if the incident is judged to be high risk.

Myth 6: all details need to be provided as soon as a personal data breach occurs

Here, Ms Denham explains that under the GDPR there is a requirement for organisations to report a personal data breach that affects people's rights and freedoms "*without undue delay*" and, where feasible, not later than 72 hours after having become aware of it.

Ms Denham says that organisations will have to provide certain details when reporting, but if not all the details are available at the time, they can be provided later. Ms Denham says that her office does not expect to receive comprehensive reports at the outset of the discovery or detection of an incident. But the ICO will want to know the potential scope and the cause of the breach, mitigation actions the organisation plans to take, and how it plans to address the problem.

Myth 7: if you don't report in time a fine will always be issued and the fines will be huge

Here, Ms Denham reassures us that under the GDPR, fines will be "*proportionate and not issued in the case of every infringement.*"

However, organisations do need to be aware that the ICO will have the ability to issue fines for failing to notify and failing to notify in time. It is important that organisations that systematically fail to comply with the law or completely disregard it, particularly when the public are exposed to significant data privacy risks, know that the ICO has that sanction available, Ms Denham says.

In any event, Ms Denham says that fines can be avoided if organisations are "*open and honest and report without undue delay*". This goes alongside the basic transparency principles of the GDPR.

Ms Denham confirms that the ICO is currently working alongside other EU data protection authorities as part of the Article 29 Data Protection Working Party to produce guidance that will set out when organisations should be reporting, and the steps they can take to help meet their obligations under the new reporting requirements.

Organisations should be preparing now by putting in place the roles, responsibilities and processes for reporting, Ms Denham says. This is particularly important for medium to large organisations that have multiple sites or business lines.

Over the coming months the ICO will be introducing a new phone reporting service to enable businesses and organisations to report current personal data breaches and future breaches under the GDPR. It will sit alongside a web reporting form and provide organisations with a quicker and easier way of reporting to the ICO, enabling them to receive immediate advice.

Comment

The blog pieces, the ICO says, have proved to be "*incredibly popular*", perhaps proving the point that there are indeed many misconceptions and misunderstanding about what exactly the GDPR will entail and how disruptive and expensive it will be for businesses. Hopefully, the blog pieces have brought some comfort to those who have been concerned. In any event, the key to successful compliance must surely be preparation so that by the time the new law becomes effective in May 2018, the transition is as smooth as possible, resulting in less risk of the ICO having to become involved at all. Nevertheless the GDPR poses some significant challenges which can only be met if organisations implement systemic change to cater to the broader protections for individuals including the rights to data portability and free access to their data.