Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

With The GDPR, The Dawn Of The New Normal Approaches

By **Maarten Stassen** (March 23, 2018, 3:22 PM EDT)

Maarten Stassen

As we approach May 25, the day that the General Data Protection Regulation (GDPR) becomes applicable, many companies have already spent considerable time, budget and sleepless nights on this four-lettered boardroom buzzword. While some early adopters are busy fine-tuning their processes and procedures, many companies are not there yet and still struggle to decide which actions to prioritize. These discussions also take place within non-EU-based companies, as the GDPR will apply if they offer goods or services to individuals within the EU, or monitor their behavior within the EU.

Prioritization discussions often focus on budget, resources and, of course, risk. The GDPR's risk-based approach is meant to focus on the risk to the individual, but management discussions tend to focus on the risks to the company. And who can be blamed for such approach, considering the possibility of fines of up to 4 percent of your total global annual revenue? There is much guessing these days about whether the soup will be eaten as hot as it is cooked. Will regulators impose a few high fines to show it means business about the GDPR? And if so, will the first fines be levied on the established tech giants or will smaller and less data-driven companies also be a regulatory target?

In this case, the proof of the pudding will also involve the eating, but what we can't deny is that regulators are performing significant outreach to alert companies about the GDPR obligations and associated enforcement. For example, there is the entertaining YouTube video made with the collaboration of the French data protection authority CNIL.[1] Then there is the U.K.'s information commissioner posting "GDPR myth busting blogs"[2]; the Spanish data protection authority AEPD with blogs[3], tools and guidelines; and the Belgian authority with its "a new wind, not a hurricane" GDPR page[4].

We are already gaining insights into the approach that these regulators will take after May 25. For example, the U.K.'s information commissioner's office will "intend to use those powers proportionately and judiciously" and states that "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."[5] The confirmation

— “if you can demonstrate that you have the appropriate systems and thinking in place you will find the ICO to be a proactive and pragmatic regulator aware of business needs and the real world”[6] — sounds more like an invitation and clearly puts the ball in the companies’ court.

The race to GDPR compliance to drawing many comparisons to the Y2K Millennium Bug, mainly because of the fuzz created around both acronyms and the efforts of many to come up with the right solution. Optimists like to remind that “Y2K wasn’t such a disaster after all,” and even “much to do about nothing.” While I will not dive into the details of the problems that two-digit date programming caused 18 years ago, what I will say is that the GDPR is certainly not “much about nothing,” and that for me both matters even play in a totally different league.

To continue with the same metaphor, even before the first GDPR infringement or sanction imposed as a result of it, the GDPR has already changed the rules of the game dramatically. Not because of its extreme novelty — as most of the concepts already existed under the Data Protection Directive of 1995 — but because of the way that companies will have to interact with individuals and think about the way they use, store and delete these individuals’ data.

Much more than the directive and any related national legislation, the GDPR is making headlines not only in the professional but also in the mainstream press. Individuals are being made aware of their data protection-related rights and will expect companies to comply. And they will, without any doubt, challenge them on it. The reputational damage that would result from noncompliance with such an infamous piece of legislation cannot be underestimated.

Furthermore, the operational impact of the GDPR and its possible sanctions are huge. The impact, for example, of a ban of processing is a major operational risk. On the other hand, building GDPR compliance in within business processes requires important changes. Take, for examples, the execution of data access rights. While they already existed under the current directive, there aren’t many companies that received more than a handful requests a year. Now that more activity on that end is expected, processes and procedures need to be rewritten or drafted from scratch, just like for data breaches, records of processing activities, and the implementation of privacy by design. And we should not forget, of course, the documentation of all these compliance efforts must be able to demonstrate compliance in line with the accountability principle.

In this “big data” age, where statements like “data is the new oil” are frequently used, we have to conclude that the GDPR has changed this understanding: Data has become a liability instead of an asset, and instead of wanting more, companies need to rethink how they can focus on having “smart data” instead of “big data.” And while getting their data house in order, companies must start realizing that less is indeed often more. When focusing on the relevance of the data instead of the size of the database, companies end up with more accurate, and thus more valuable data. This is, without any doubt, a positive effect of the GDPR.

So, as May 25 is virtually tomorrow, what should companies really focus on?

First of all, companies' GDPR governance should be duly set up and should work seamlessly. The question of whether a data protection officer is mandatory is therefore often not the most fortunate one, and a negative answer is certainly not good news. Someone must monitor GDPR compliance, address questions from regulators or individuals, ensure that deadlines are met (e.g. in case of data access requests or data breach notification), and keep track of regulatory guidance and case law. This could be one person, or a team of professionals, as long as it is tailored to the structure of the organization, given that effective GDPR governance is an absolute must.

Once the governance has been established, everyone with GDPR roles and responsibilities should ensure that individuals' rights are duly taken into account. The purpose of the GDPR is to protect these rights, making this an obvious priority. This individual-focused approach should cover the entire data lifecycle, from providing sufficient and transparent information at the moment of collection of personal data to ensuring that requests related to these rights are duly followed up upon and that data are not stored for longer than required for the purpose for which they were collected.

One of the other key areas should be the training and awareness of employees, as a company's strongest assets — its employees — might unintentionally become its weakest link. When things go wrong, if is often because employees wanted to do their job well — or too well — while not being aware of the data protection-related risk. It is not a bold statement to say that a company's biggest security risk sits behind the keyboard, so it is up to the company to mitigate such risk.

Another priority should be data mapping, and not only in a one-dimensional way (point A to point B) but multidimensionally (how much information for which purpose). Understanding the data flows is key, and a company wants to avoid a supervising authority asking, "How can you say that you duly protect personal data, if you don't know where they are?" The mandatory records of processing activities should therefore not be seen as a mere tick-the-box exercise, but could serve as a single-truth, one-stop-shop go-to document where all the information on data processing activities is centralized.

It goes without saying that companies need to have the right policies and procedures in place to ensure the implementation of data protection by design and data protection by default, to ensure that data breaches are duly reported both internally and externally, but if there is one other priority that cannot be left aside it is third-party management. Companies can protect personal data as much as they want, but if third parties processing the same data do not do this in a similar way, all the efforts might have been in vain. Having the right contractual language in place is one thing, but service providers should give a sufficient level of comfort that they have the right technical and organizational measures in place to keep the data safe. Because ultimately the companies that have instructed them remain responsible and accountable for the third parties they entrust with the data.

While the Y2K-related efforts did not change the way we do business, the GDPR does significantly change the way companies handle personal data. As your compliance efforts will have effects beyond May 25, it is worth investing time and budget in the way business will be done from now on.

Maarten Stassen is a senior counsel with Crowell & Moring LLP in Brussels.

[1] https://www.cnil.fr/fr/video-le-youtubeur-cookie-connecte-repond-vos-questions-sur-larrivee-du-rgpd

[2] https://iconewsblog.org.uk/tag/gdprmyths/

[3] http://www.agpd.es/blog/

[4] https://www.privacycommission.be/nl/algemene-verordening-gegevensbescherming-

[5] https://iconewsblog.org.uk/2017/08/09/gdpr-sorting-the-fact-from-the-fiction/

[6] https://iconewsblog.org.uk/2017/12/22/gdpr-is-not-y2k/#more-3212