22 June 2017

GDPR is mainly about corporate governance

…and not about systems or cyber security

Cătălin Grigorescu, LL.M.Eur

Over the past few months our technology team has organised, led or attended several meetings, presentations and conferences on the new data protection regime introduced by the GDPR, as the adrenaline of the race to achieve compliance by May 2018 starts to kick in for many controllers and processors.

Almost inevitably the discussion or at least the first questions gravitate around the security of data and systems. And there are good reasons for people, especially people tasked with implementing practical measures to ensure compliance, to drift to this area of GDPR compliance first. Everybody understands, from his or her own personal or business context, that personal data is an asset that requires protection and protection is naturally associated with security. It is a concrete concept, easier to grasp and to translate in immediately executable actions. In addition, there is an intuitive perception, confirmed by media reports of (in)famous data breach cases, that if a security breach occurs and personal data is lost or put at risk, this will have the biggest reputational and financial impact on their businesses, hence they need to worry about this before anything else. Finally, if security is so important, one needs to invest heavily in securing their systems, communications and processes, so let's focus on this big expenditure item first.

I would argue, though, that while security is no doubt an important part of the GDPR compliance concept, it is definitely not the one to place now at the top of the agenda. Here are some thoughts on what companies could be first concerned with.

1. GDPR requires a self-assessment risk-based approach to compliance. It is the controller's or the processor's own responsibility to identify the risks and implement the required measures. There will be no official prescription of what the concretely required measures are depending on the business you are in (save for the general concepts of pseudonymisation and encryption), so stop searching for one.

2. It is a matter for the boards of directors or for the higher management to define their own company's risk policies. If they ignore that GDPR compliance is a board matter, they might be in breach of their fiduciary duty to the company.

3. GDPR compliance may soon become so important that you may not be able to do business with some or many of your existing customers or partners, who are bound to analyse your compliance level beyond firewalls, security software and VPNs.

4. A controller's or a processor's duty concerning personal data is not merely related to preventing the loss of that data to hackers or other maleficent people. It extends to handling that data properly even when the data is not at risk of destruction or loss. GDPR includes a catalogue of rights of the individuals in relation to their own personal data that virtually creates a "Constitution" of rights to personal data, bringing them into the realm of fundamental rights.

5. One cannot talk about security unless he or she knows what is there to secure and if that is worth securing. If it is not worth securing then perhaps that information is not needed, therefore not required to be captured, stored or otherwise processed in the first place.

6. Knowing what you have to secure will eventually help you make the best decision about the appropriate security measures. It will also help you not over-spend on security efforts, thus improving the company's bottom-line.

To all people approaching GDPR as a security project, I have one word of caution: **you may be impenetrable, but still fail to be GDPR-compliant.**

For more information:

Cătălin Grigorescu, LL.M.Eur
Managing Partner
catalin.grigorescu@bpv-grigorescu.com