08 March 2017

THE THREAT OF EUR 20 MILLION DAMAGE CLAIMS AGAINST D&Os…

…and 4 measures to avoid paying it

Cătălin Grigorescu, LL.M.Eur

There is a new villain sowing fear in the global corporate world called Regulation (EU) 2016/679 a.k.a. GDPR (General Data Protection Regulation), who is expected to help the European Commission help individuals (re-)take control over their personal data. To a large extent, the fear might be grounded, as the Regulation is unprecedented in introducing administrative sanctions, directly from the EU level to national level, of a magnitude comparable to the administrative sanctions that may be applied by antitrust authorities for breaches of competition laws. In certain case and under certain circumstance, the administrative sanctions may reach EUR 20m or 4% of the global turnover of the sanctioned entity, before any damage claims from aggrieved individuals.

Almost any law firm or entity concerned with data security has written a piece on GDPR and has organised an event or discussion on this topic (except for our firm who will have its event later this March). Therefore, I would not dwell on the intricacies of the Regulation, but wish to briefly discuss the potential implications on the liability of the Directors and CEOs of Romanian companies.

So, how does a Director or a CEO guard against a potential claim by the company he or she directs or manages for losses arising from administrative sanctions or third party damage claims in relation to a breach of GDPR? In essence, the answer is quite simple: by exercising the duties of the office with the care and diligence required from a director.

The standard of diligence under Romania law is defined in specific regulations, legal scholars and case law as the standard of a good manager (administrator), i.e. of a person who, when taking a business decision, is reasonably entitled to believe, on the basis of adequate information, that he/ she is acting in the interest of the company. A decision taken while observing this standard releases the director from personal liability for damages, even if the taken decision has caused damages to the company.

Consequently, decisions relating to measures required on the basis of GDPR, taken with the proper care and diligence as outlined before, are not likely to trigger the personal liability of a director, despite the company being held liable to pay administrative fines or damages to third party individuals.

To prove that he/ she exercised the duties of the office with proper care and diligence, a director or CEO might want to consider following a plan that would include, as a minimum, the following:

1. Directors and CEOs should assess the extent to which GDPR applies to the business he/ she is running. When making the assessment and gathering the required information, a director should resort to in-house or external legal expertise. Given the complexity of the issues and the potential magnitude of any negative impact of failure to comply, the director should have reasonable assurance that the consulted legal counsels have actual expertise and experience in dealing with data protection issues. Addressing these data protection issues to the in-house counsel or the company's regular external counsel, albeit handy, might not always be sufficient proof of acting diligently.

2. Directors should ensure that at board level, through the care of the audit and risk committee, if appointed, the company adopts policies which are adequate for preventing the risks associated with the processing of personal data, with the protection systems and procedure, as well as for preventing breaches and employing proper response and follow-on adjustment procedures and actions when breaches occur.

3. To the extent that GDPR or the related risk policies require the appointment of a Data Protection Officer (DPO), whether in-house or outsourced, a director should ensure that the appointed person or entity fully complies with the legal requirements for professional qualification and expertise. Throwing the problem into the hands of the company's existing compliance function does not necessarily account for an adequate solution if the required qualifications and expertise are not available. It is worth mentioning that GDPR requires that a DPO directly reports to the highest management level of the company, thus, depending on the corporate structure, to the board directly, or otherwise to the CEO. Therefore, the level of diligence in selecting and appointing a DPO may play a crucial role in establishing a potential future personal liability of the director or of the CEO for administrative sanctions or other damages incurred by the company for breaches of GDPR.

4. Directors should monitor and regularly assess the extent to which the measures decided or recommended by the audit and risk committee or by the DPO are implemented, supplemented or adjusted dynamically, depending on the development of the company's business. They should further assess the adequacy of the existing measures in response to actual cases when breaches of the applicable data protection regime occur.

Finally, it is worth reminding that the standard of care and diligence applied to executive directors and CEOs might be stricter than the standard applicable to non-executive directors. In spite of this, it is not expected of a director or a CEO that himself or herself becomes a data protection specialist, however, directors and CEOs should be aware and concerned with personal data protection in direct proportion to the significant importance that GDPR and supervision authorities place on the topic under the new regime.

For more information:

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