VOICU FILIPESCU
Attorneys at Law
News in Laws – Legal Monthly Newsletter
December 2017

Cover article

Data protection officer – internal or external?

With the coming into force of the new European General Data Protection Regulation (GDPR), in less than 6 months from now (18 May 2018), this article addresses the various interpretations of privacy professionals, but also the concerns of the business teams regarding the special status of the Data Protection Officer (DPO). Is the person appointed as a DPO under a conflict of interest, when also employed in this area by the data controller (the company that appointed him)? Is it possible for the DPO to wear two hats, one of employee who handle information processing and one of supervisor over the same issues?

Data Protection Officer (DPO) – the notion

The GDPR has created the obligation for certain companies, under certain circumstances, to create a new role within their organization i.e. a person who is properly and timely involved in all aspects of the protection of personal data. The regulation specifically prescribes the tasks of the DPO, including its oversight of company compliance with GDPR requirements, and the responsibility for interacting with the data protection authority (DPA) and the data subjects to the company's processing. Its role includes GDPR counseling within the company.

As of November 21, 2017, the occupation classification in Romania was supplemented to include the new role, namely "personal data protection officer", which received COR code 242231 by Order no. 1786/5384/2017 regarding the amendment and completion of the Classification of Occupations in Romania - level of occupation (six characters), approved by the Order of the Minister of Labor, Family and Social Protection and of the President of the National Institute of Statistics no. 1832/856/2011.

Data Protection Officer (DPO) – when is the appointment obligatory for companies?

If a company carries out large-scale monitoring of individuals or large-scale processing of special categories of data (those provided for in Articles 9 and 10 of GDPR, e.g. ethnic origin, political affiliation, religious, genetic, biometric, health or crime data) will be required to appoint a DPO.

Since the GDPR refers to the processing of personal data of EU citizens, wherever and by anyone else, even non-EU companies (e.g. companies in the U.S.) might be in a position to appoint a DPO.

Data Protection Officer (DPO) – is an internal DPO in conflict of interest with the appointing company?

The GDPR clearly establishes that the DPO does not receive any instructions regarding the performance of its tasks. It shall not be dismissed or sanctioned by the controller or by the processor for reasons related to the performance of its duties as DPO. The DPO responds directly to the highest level of management of the controller or processor, being part of the so-called "senior management".

These provisions, contained in art. 38 of the GDPR raised a number of questions about the special status of the DPO, from the apparent immunity of the DPO as regards the dismissal or sanctioning by the controller, to the optimal choice

between appointing a DPO as a member of the controller's staff and one that is an independent contractor under a service contract, as the GDPR allows both variants.

The concern increased with the December 2016 guidance provided by the Art. 29 WG on the DPO's independence, according to which the DPO "cannot hold a position within the organization that leads him or her to determine the purposes and means" of data processing.

The natural tendency of companies, especially small ones, is to appoint as DPO an employee who is already familiarized with the matter, mainly dealing with the processing of personal data within the company. Some privacy professionals, consider, though, that these employees cannot perform a double duty as the DPO, because they are in a clear conflict of interest.

However, requiring a DPO to be independent (as provided under the GDPR) means that the role of the DPO cannot be fulfilled by company employees who are also responsible for daily decisions on personal data processing, such as people working in human resources, IT, or marketing. This implies that a consistent demand of external candidates for this role will be created, to pass the test of "independence" required by GDPR, but this also creates difficulties in finding them. Some companies are expected to look for these resources externally, including from lawyers. It appears at this time that the companies who will be able to openly demonstrate that the person appointed to the role of DPO is independent will be better positioned.

In any case, we believe that the supervisory authority will have to show some degree of flexibility in interpreting the conflict of interest rules by not interpreting them too restrictively. National authorities in Member States are expected to provide rules in addition to the guidance provided by the Art. 29, rules to better clarify situations of conflict of interest and to provide greater flexibility as to the incompatibilities of the role of the DPO with other internal functions of the company.

Do you wonder if it is necessary to appoint a DPO in your organization? Do you have any questions about the gray areas of the legislation on the appointment and role of DPO? Do not hesitate to contact our lawyers, specialized in data privacy matters.