POPOVICI NIȚU STOICA & ASOCIAȚII
Attorneys at Law

239 Calea Dorobanți, 6th Executive Floor
Bucharest, 1st District, Postal Code 010567
Romania

Telephone: (0040) 21 317 79 19
Fax: (0040) 21 317 85 00 / 317 75 05

office@pnsa.ro
www.pnsa.ro

RO 15168518

DATA PRIVACY

OCTOBER 19, 2017

Companies are welcoming a new team player – the Data Protection Officer

The new General Data Protection Regulation ("GDPR") could not have enlarged data controllers' and data processors' obligations and apply such great sanctions without anticipating the need for companies to appoint a Data Protection Officer ("DPO").

While companies must now turn their focus on ensuring compliance with the GDPR every step of the way, the DPO will be a key player in reaching this goal.

Now this raises questions: who is the DPO? when is appointing a DPO mandatory? what are her/his main tasks? are there any other obligations?

1. Who?

The DPO may be an employee of the controller or processor, or an external contractor.

When considering appointing an employee as DPO, the companies should consider the following:

- the duties of the employee related to her/his DPO position must be separated from any other duties/ tasks/ responsibilities within the company, **provided that** such duties do not result in a conflict of interest **and** any other tasks leave the DPO enough time to perform the obligations and duties as DPO;
- the DPO cannot hold a position that leads her/his to determine the purpose and the means of processing.

Companies can also sign a service contract with a third party, such as a law firm, to exercise the function of the DPO. Taking into consideration the tasks to be performed by the DPO (as described below at question 3), engaging a team and combining individual skills and strengths might prove to be more efficient.

When deciding whether the DPO should be an employee or a third party, companies will take into account some general criteria set by the GDPR: the basis of professional qualities, expert knowledge of data protection law and

practices, as well as the ability to fulfil the required tasks.

A group of undertakings may decide to appoint a single DPO, but only as long as each establishment can easily and efficiently communicate with the DPO.

2. When?

Mandatory designation of the DPO

Appointing a GDPR is mandatory:

a) where the processing is carried out by a public authority or body;
b) in the private sector, for organizations that, as a core activity:
   - monitor individuals systematically (i.e. periodically, repeated at certain intervals, including all forms of tracking and profiling on the internet, including for the purpose of behavioural advertising; the notion of monitoring is not restricted to the online environment!) on a large scale; and/or
   - process on a large scale special categories of data or personal data relating to criminal convictions and offences.

When assessing whether their operations can be considered as "large scale" operations, the companies should consider, among others, the number of data subjects concerned, volume of data, duration of processing activities or geographical extent of the processing activity.

The companies, acting either as data controller or data processor, must determine whether the processing carried out meets any of the previous conditions and if so, to immediately appoint a DPO.

Voluntary designation of the DPO

Even in cases where the appointment of the DPO is not mandatory, the Data Protection Working Party established by EU and also the Romanian Data Protection Authority ("DPA") recommend to voluntarily appoint one. The reason? Ensuring compliance with the data privacy regulations and facilitating the communications between the DPA, the company, its employees and, most importantly, the data subjects. A voluntary appointment of a DPO may also be useful in case of a potential data breach or non-compliance, when the DPA will determine the applicable sanctions.

3. What?

The main activity of the DPO is to monitor compliance with the GDPR and advise the company in this respect. The GDPR lists DPOs minimum tasks:

a) to inform and to advise the controller or the processor and the employees who carry out processing of their obligations;
b) to monitor compliance with all data protection regulations and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing

operations, and the related audits;

c) to provide advice where requested as regards the data protection impact assessment and monitor its performance;
d) to respond to requests with regard to all issues related to processing of their personal data and the exercise of their rights;
e) to cooperate with the DPA and, where appropriate, consult it with regard to any matter;
f) to act as contact point for the DPA.

Based on the practice established so far under many national laws requiring the appointment of a DPO since before the GDPR, DPOs often have responsibilities when it comes to record-keeping. They create inventories and hold a register of processing operations based on information provided to them by the various departments in their company responsible for the processing of personal data.

DPOs are required to adopt a risk-based approach in performing the tasks, taking into account the nature, scope, context and purposes of processing. In essence, DPOs should focus, primarily, on the higher-risk areas, without neglecting to monitor compliance of data processing operations that have comparatively lower level of risks.

4. Other?

Although it may seem that once a DPO is appointed, the controller or processor has fulfilled its obligation, as usual, things are not that simple and the appointment is just the first step.

In order to secure the role of the DPO, the GDPR sets further obligations for controllers and processors:

a) to ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data;
b) to support the DPO in performing the tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain the DPO's expert knowledge;
c) to ensure that the DPO does not receive instructions regarding the exercise of the tasks and is not dismissed or sanctioned for performing her/his tasks.

Even though DPOs are responsible with regard to all processing of personal data within a company, they will not be responsible in case of non-compliance with the GDPR. Appointing a DPO is not an exception from the basic principle established by the GDPR that the controller or the processor is required to ensure and be able to demonstrate that the processing is performed in accordance with its provisions. Data protection is, has been and will remain a responsibility of the controller or the processor.

All in all, DPOs will play a crucial role in all companies starting with May 2018. Complying with the new requirements may as well start by appointing this key player.

This document is intended for informational purposes only, does not represent legal advice and does not focus on particular cases.

For further information or analysis on specific matters, please contact **Alexandru Ambrozie** (alexandru.ambrozie@pnsa.ro), **Luana Dragomirescu** (luana.dragomirescu@pnsa.ro) or **Ana Stoenescu** (ana.stoenescu@pnsa.ro).

For more information about Popovici Nițu Stoica & Asociații, please visit: www.pnsa.ro