# GDPR COMPLIANCE – DO I NEED (TO APPOINT) A DATA PROTECTION OFFICER? (*)

Even when it is not an obligation under GDPR, by designating and adequately supporting a Data Protection Officer ("DPO") an organisation can provide a focus for compliance efforts, including maintaining records of processing activities, for enquiries from data subjects and to be a point of contact for the relevant Data Protection Supervisory Authority ("DPSA"). Both the Belgian Privacy Commission (CVPV/CBPL) and the existing Data Protection Working Party (commonly referred to as "WP29") recommend that all Data Controllers and Processors consider designating a DPO.

## What are the DPO's responsibilities?

The DPO assists the Controller or Processor to monitor internal compliance with the GDPR. He or she is designated on the basis of professional qualities and in particular expert knowledge of data protection law and practices – but a specific professional qualification is not mandated by the GDPR.

The DPO must be able to fulfil at least the following tasks (Arts 37 (5) and 39 (1) GDPR):

- to inform and advise the controller or the processor and the employees who carry out processing of their [data protection] obligations;
- to monitor compliance with the GDPR 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;
- to provide advice where requested as regards data protection impact assessments;
- to cooperate with the supervisory authority;
- to act as the contact point for the supervisory authority on issues relating to processing and to consult with regard to any other matter.

The DPO is required to act independently in relation to data protection matters and '*does not receive any instructions regarding the exercise of [his or her] tasks'* (Art 38 (3) GDPR). Companies are required to resource the DPO adequately. The DPO is to report on compliance at the 'highest management level' (normally to the Board or a main Board Director) of the controller or processor.

## Who <u>must</u> designate a DPO?

An organization must appoint a DPO in three specified cases (Art 37 GDPR) where:

- the processing is carried out by a public authority or body;
- the core activities consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale;
- the core activities consist of processing on a large scale of special categories of personal data (e.g. data revealing racial or ethnic origin, political, religious or philosophical beliefs, data concerning health or genetic data…) or data relating to criminal convictions and offences.

Core activities are not defined but GDPR recital 97 states that, in the private sector, the core activities of a controller relate to its primary activities and not to *'the processing of personal data as ancillary activities*'.