GDPR COMPLIANCE – DO I NEED (TO CARRY OUT) A DATA PROTECTION IMPACT ASSESSEMENT ("DPIA") OR NOT? (*)

The GDPR requires a risk based approach to the processing of personal data. A general requirement for the data controller to pre-notify the Data Protection Supervisory Authority ("DPSA") before processing personal data is not maintained. However, if a 'high risk' to the privacy (rights and freedoms) of data subjects could result from proposed processing a DPIA must be carried out and - depending on the results - the controller may be required to consult the DPSA before it begins the processing in question (Arts 35 & 36 GDPR).

What is a DPIA?

The GDPR Art 35 (1) offers a functional description of circumstances that may trigger a DPIA. These include processing using new technologies where a high risk to the rights and freedoms of natural persons could arise. Guidelines about DPIAs (last revised on 4 October 2017) describe DPIAs as: *"a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them".*

When do you need to carry out a DPIA?

Even though a DPIA could be required in other circumstances GDPR Art 35 (3) provides three examples where processing is likely to result in a 'high risk' requiring a DPIA to be carried out:

- "a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing", …
- "processing on a large scale of special categories of data" …
- "a systematic monitoring of a publicly accessible area on a large scale".

The Belgian Privacy Commission CVPV/CBPL can be expected to establish and publish lists of processing operations that will be/will not require a DPIA in accordance with Arts 35 (4)(5) GDPR; but such lists will not be available until May 2018 at the earliest.

What should be in the DPIA?

The DPIA should contain at least the following information (Art 35 (7) GDPR):

- *A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
- *An assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
- *An assessment of the risks to the rights and freedoms of data subjects;*
- *The measures envisaged to address the risks (…)*

If an organization does not carry out a DPIA although it is obliged to do so under the GDPR, the relevant DPSA (currently the CVPV/CBPL) can take a range of remedial measures against the data controller under its investigative, corrective and fining powers, including issuing a reprimand and imposing a fine of up to 10M EUR or up to 2% of the total worldwide annual turnover, whichever is greater.