DIEN IK EEN GEGEVENSBESCHERMINGSEFFECTBEOORDELING UIT TE VOEREN OF NIET? (*)

De GDPR vereist een risicobewuste benadering van de verwerking van persoonsgegevens. De algemene informatieplicht van de Verwerkingsverantwoordelijke de ten aanzien van de Toezichthoudende Autoriteit *voor* de gegevensverwerking, wordt niet gehandhaafd. Als de beoogde verwerking een hoog risico inhoudt voor de privacy (rechten en vrijheden) van de betrokkenen, dan is een Gegevensbeschermingseffectbeoordeling/Data Protection Impact Assessment (DPIA) aangewezen en – naargelang de resultaten – kan de Verwerkingsverantwoordelijke verplicht worden om de Toezichthoudende Autoriteit te raadplegen vooraleer de bewuste verwerking aan te vatten (Art 35 en 36 GDPR).

Wat is een Gegevensbeschermingseffectbeoordeling (hierna "DPIA")?

Art 35 (1) GDPR geeft een functionele beschrijving van de omstandigheden waarin een DPIA nodig kan zijn. Hierin begrepen zit de verwerking waarbij nieuwe technologieën worden gebruikt met mogelijk een hoog risico voor de rechten en vrijheden van natuurlijke personen. Een DPIA is een procedure om GDPR-conform te worden en dit aan te tonen. In de Richtsnoeren voor Gegevensbeschermingseffectbeoordelingen (laatst gewijzigd op 4 oktober 2017) wordt een dergelijke beoordeling als volgt omschreven: *'Een proces dat is bedoeld om de verwerking van persoonsgegevens te beschrijven, de noodzaak en evenredigheid ervan te beoordelen en de daaraan verbonden risico's voor de rechten en vrijheden van natuurlijke personen te helpen beheren door deze risico's in te schatten en maatregelen te bepalen om ze aan te pakken.'*

Wanneer dient u een DPIA uit te voeren?

Zelfs al kan een DPIA vereist zijn in andere omstandigheden, Art 35 (3) GDPR geeft drie voorbeelden waar verwerking waarschijnlijk een 'hoog risico' inhoudt waardoor een dergelijke beoordeling aan de orde is:

- "een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking", …
- "grootschalige verwerking van bijzondere categorieën van persoonsgegevens"…
- "een stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten".

De Belgische Gegevensbeschermingsautoriteit (voorheen "Privacycommissie") zal lijsten opstellen en publiceren inzake het soort verwerkingen waarvoor al dan niet een DPIA vereist is overeenkomstig Art 35 (4)(5) GDPR. Dergelijke lijsten zullen slechts vanaf mei 2018 ten vroegste beschikbaar zijn.

Wat dient een DPIA te bevatten?

De Beoordeling dient minstens de volgende gegevens te bevatten (Art 35 (7) GDPR):

- *Een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinde, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;*
- *Een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;*
- *Een beoordeling van de risico's voor de rechten en vrijheden van de betrokkenen;*
- *De beoogde maatregelen om de risico's aan te pakken (…)*

Indien een onderneming geen DPIA uitvoert terwijl ze daartoe nochtans verplicht wordt door de GDPR, kan de Gegevensbeschermingsautoriteit corrigerende maatregelen nemen ten aanzien van de Verwerkingsverantwoordelijke. Zo kan deze een berisping geven en een geldboete opleggen tot het grootste bedrag van 10 miljoen EUR of 2% van de totale wereldwijde jaaromzet.