Analyse d'impact : les principes instaurés par le RGPD

Question 1 : *le traitement est-il susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques ? (RGPD, art. 35, § 1, 3 et 4) ?*

NON → *Le traitement ne nécessite pas d'analyse d'impact*

OUI ↓

Question 2 : *le traitement est-il couvert par une exception excluant l'analyse d'impact ? (RGPD, art. 35, § 5 et 10) ?*

OUI → *Le traitement ne nécessite pas d'analyse d'impact*

NON ↓

Le responsable du traitement doit réaliser une analyse d'impact (RGDP, art. 35, § 7) :
- *il demande son avis au DPO (RGPD, art. 35, § 2) ;*
- *il doit respecter les codes de conduite (RGPD, art. 35, § 8) ;*
- *il demande l'avis des personnes concernées ou de leurs représentants (RGPD, art. 35, § 9) ;*
- *le DPO vérifie l'exécution de l'analyse d'impact (RGPD, art. 39, § 1, c) ;*
- *si nécessaire, le responsable du traitement procède à un examen afin d'évaluer si celui-ci est effectué conformément à l'analyse d'impact (RGPD, art. 35, § 11).*

↓

Question 3 : *les risques résiduels sont-ils élevés ? (RGPD, art. 36, § 1)*

NON → *Il n'est pas nécessaire de consulter l'autorité de contrôle*

OUI ↓

Le responsable doit consulter l'autorité de contrôle (en France, la CNIL) avant la mise en place du traitement

© Editions Législatives – 2017