— RGPD : Dans quels cas effectuer l'analyse d'impact relative à la protection des— données

Depuis le 25 mai 2018, le Règlement européen sur la protection des données (RGPD) renforce les droits des personnes en matière de collecte de données personnelles. Les entreprises réalisent ainsi une analyse d'impact relative à la protection des données (AIPD) lorsqu'un traitement est susceptible d'engendrer « un risque élevé pour les droits et libertés des personnes physiques ». La CNIL vient de donner la liste de 14 types d'opérations pour lesquelles l'AIPD est requise, dont certains touchent la gestion des ressources humaines.

Notez- le :
L'analyse d'impact relative à la protection des données (AIPD) est menée avant la mise en œuvre du traitement. Elle est ensuite revue régulièrement, au minimum tous les 3 ans, pour s'assurer que le niveau de risque reste acceptable. Elle contient au minimum :

- une description systématique des opérations de traitement envisagées et de ses finalités ;
- une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
- une évaluation des risques pour les droits et libertés des personnes concernées ;
- les mesures envisagées pour faire face aux risques.

Le RGPD donne 3 types de traitements susceptibles de présenter un risque élevé :

- l'évaluation systématique et approfondie d'aspects personnels fondée sur un traitement automatisé et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;
- le traitement à grande échelle de données sensibles ou relatives à des condamnations pénales et des infractions ;
- la surveillance systématique à grande échelle d'une zone accessible au public.

Le Comité européen à la protection des données (CEPD) a également identifié 9 critères permettant de caractériser les traitements pouvant entraîner un risque élevé.

La CNIL considère que si un traitement remplit au moins 2 de ces 9 critères, une AIPD doit être effectuée.

Toutefois, si vous estimez que le traitement que vous mettez en place, bien qu'il remplisse au moins 2 critères, ne présente pas de risque élevé, vous n'êtes pas dans l'obligation de procéder à une AIPD. Mais, vous devrez expliquer votre décision, accompagnée de l'avis de votre délégué à la protection des données (DPO), s'il existe.

De plus, vous pouvez également effectuer cette AIPD si vous remplissez moins de 2 critères mais que vous estimez que le traitement présente un risque élevé.

En cas de doute, la CNIL recommande que l'AIPD soit effectuée.

<u>Analyse d'impact relative à la protection des données : ce qui est prévu par la CNIL</u>

Le RGPD impose aux Etats d'établir une liste de traitements pour lesquels une analyse d'impact serait requise. La CNIL vient de préciser 14 types d'opération de traitement concernés par l'AIPD.

Différents types d'opérations de traitement concernent les salariés et la gestion des ressources humaines. C'est le cas notamment des traitements :

- établissant des profils de personnes physiques à des fins de gestion des ressources humaines;
- ayant pour finalité de surveiller de manière constante l'activité des employés concernés ;
- ayant pour finalité la gestion des alertes et des signalements en matière professionnelle.

Attention :
La liste établie par la CNIL est non-exhaustive et sera régulièrement revue par la CNIL selon son appréciation. Et n'oubliez pas qu'une AIPD est réalisée dès qu'il y a un risque élevé.

La CNIL devrait établir une liste des traitements qui ne présentent pas de risque élevé et qui ne seront donc pas soumis à la réalisation d'une AIPD.

Notez-le :
Sous certaines conditions, les traitements répondant au respect d'une obligation légale ne sont pas soumis à AIPD. Il en est de même lorsque la nature, la portée, le contexte et les finalités des traitements envisagés sont très similaires à un traitement pour lequel une AIPD a déjà été menée.

Délibération n° 2018-326 du 11 octobre 2018 portant adoption de lignes directrices sur les analyses d'impact relatives à la protection des données (AIPD) prévues par le règlement général sur la protection des données (RGPD), Jo du 6 novembre

Délibération n° 2018-327 du 11 octobre 2018 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise, Jo du 6 novembre

Source : Edition Tissot du 12 novembre 2018