www.actuel-expert-comptable.fr
Pays : France
Dynamisme : 3

Visualiser l'article

Les entreprises ont jusqu'au 24 mai 2021 pour réaliser l'analyse d'impact des traitements de données RH

La période laissée aux entreprises pour documenter l'analyse d'impact de leurs traitements de données prendra fin le 24 mai 2021. Cette procédure est requise en particulier pour trois types de traitements de données concernant les ressources humaines. Mais l'avocat spécialisé Eric Barbry se veut rassurant : rien de compliqué dans l'accomplissement de ces formalités.

Les déclarations préalable à la Cnil, c'est terminé depuis le 25 mai 2018. Le traitement des données personnelles, notamment celles des salariés par les services de ressources humaines, doit répondre aux obligations d'un règlement européen, le RGPD. Ce règlement n'a toutefois pas supprimé toutes les exigences d'analyse préalable de l'effet d'un traitement de données personnelles. Lorsque ce dernier est particulièrement sensible, les entreprises doivent mettre en oeuvre au préalable une analyse d'impact relative à la protection des données (AIPD, ou PIA en anglais).

Mais en 2018 lors de l'entrée en vigueur du RGPD, peu d'entreprises et de collectivités avaient pris le temps de se conformer à la nouvelle règlementation. En réaction, la Cnil leur a accordé un délai de grâce de trois ans pour réaliser l'analyse d'impact des traitements de données mis en place avant le 25 mai 2018. La date fatidique approche. Au 25 mai 2021, plus d'excuses pour avoir omis de réaliser cette étude d'impact.

Tous droits réservés à l'éditeur

Des contrôles accrus à partir de mai 2021 ?
L'approche de cette date pourrait donner le top départ de contrôles Cnil plus poussés, selon Eric Barbry, avocat associé du cabinet Racine, spécialisé en droit des données personnelles. "Je n'ai constaté chez mes clients aucun contrôle Cnil depuis mai 2018 concernant le respect des règles relatives aux analyses d'impact. Tous les traitements RH mis en oeuvre après mai 2018 devraient avoir fait l'objet d'une telle analyse, or ce n'est pas le cas. Je pense que la Cnil attend la fin du délai de mise en conformité pour opérer un tour de vis pour toutes les entreprises."

Il reste un peu plus d'un mois aux entreprises pour se conformer. Mais si tous les traitements de données doivent respecter le RGPD, seuls certains d'entre eux doivent faire l'objet d'une analyse d'impact. Afin d'identifier ces traitements, le Comité européen à la protection des données (CEPD) a listé neuf critères. **Si le traitement de données coche deux de ces cases, il doit faire l'objet d'une AIPD.**

Les neuf critères du CEPD permettant de caractériser un traitement susceptible d'engendrer un risque élevé
Données traitées à grande échelle ;
Données sensibles (origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques ou de santé, données biométriques et données concernant la vie ou l'orientation sexuelle) ou données à caractère hautement personnel (données relatives à des communications électroniques, données de localisation, données financières, etc.) ;
Données concernant des personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
Croisement ou combinaison de données ;
Evaluation/scoring (y compris le profilage) ;
Prise de décision automatisée avec un effet juridique ou similaire ;
Surveillance systématique de personnes ;
Traitement pouvant exclure du bénéfice d'un droit, d'un service ou d'un contrat ;
Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles.

AIPD requise pour trois types de traitements RH
En France, plusieurs délibérations de la Cnil publiées en 2018 et 2019 permettent d'y voir plus clair.

La délibération Cnil du 11 octobre 2018 liste les **opérations de traitement pour lesquelles une analyse d'impact est exigée .** En matière RH, trois types de traitements sont ainsi considérés comme "à risques" :

Les traitements "établissant des profils de personnes physiques à des fins de gestion des ressources humaines". Exemples : traitements de détection et de gestion de "hauts potentiels", traitements visant à faciliter le recrutement notamment grâce à un algorithme de sélection, traitements visant à proposer des actions de formation personnalisées grâce à un algorithme, traitements visant à détecter et à prévenir les départs de salariés sur la base de corrélations établies entre divers facteurs.

Les traitements "ayant pour finalité de surveiller de manière constante l'activité des employés concernés". Exemples : dispositifs de vidéosurveillance constante (par exemple pour les salariés manipulant de l'argent ou ceux travaillant dans des entrepôts filmés), analyse des courriels sortants (notamment afin de détecter des fuites d'informations), chronotachygraphes des véhicules de transport routier.

Les traitements "ayant pour finalité la gestion des alertes et des signalements en matière professionnelle". Exemple : procédures internes de recueil des signalements des lanceurs d'alerte (trafic d'influence, corruption, devoir de vigilance).

Tous droits réservés à l'éditeur

A contrario, une délibération Cnil du 12 septembre 2019 indique les cas dans lesquels **l'AIPD n'est pas requise :**

Les traitements mis en place dans une entreprise de **moins de 250 personnes** , uniquement à des fins de ressources humaines (gestion de la paie, des formations, suivi des entretiens annuels d'évaluation...) ;
Les traitements ayant pour seule finalité la gestion des contrôles d'accès physiques et des horaires pour le **calcul du temps de travail** (accès aux locaux de travail par badge, ...)
Les traitements destinés à la gestion des activités des comités d'entreprise et d'établissement (et, partant, du CSE) (gestion des programmes socio-culturels de l'entreprise, communication interne, formation des élus, fichier de gestion des membres...).
Ces listes ne sont pas exhaustives, et l'entreprise devra se référer aux neuf critères du CEPD pour vérifier que son traitement requiert ou non une AIPD. La Cnil propose sur son site internet une infographie qui récapitule les bonnes questions à se poser .

S'assurer de cocher toutes les cases
Il est temps de se mettre au travail, pour les entreprises qui ne se seraient pas penchées suffisamment près sur le sujet de l'analyse d'impact. Mais rien de sorcier, selon l'avocat Eric Barbry. "On s'en fait une montagne, car je pense que certains acteurs de la sécurité informatique ont sciemment laissé entendre que l'analyse d'impact était très compliquée et nécessitait une analyse profonde. Or, ce n'est pas du tout le cas ! Il ne s'agit pas d'un audit de sécurité de l'entreprise, mais bien d'une analyse documentée, qui doit montrer que l'entreprise s'est posé les bonnes questions. Le traitement est-il bien basé sur l'un des fondements juridiques du RGPD ? Les données collectées sont-elles nécessaires ? Les personnes sont-elles correctement informées ? A-t-on mis en place des mesures de sécurité adaptées ? Il s'agit de balayer le RGPD pour s'assurer qu'on a bien coché toutes les cases."

La Cnil propose sur son site internet un guide pour réaliser une analyse d'impact.

Les montants en jeu ne sont pas anodins. En effet, les autorités de contrôle peuvent prononcer des amendes administratives pouvant s'élever à 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial.

Tous droits réservés à l'éditeur