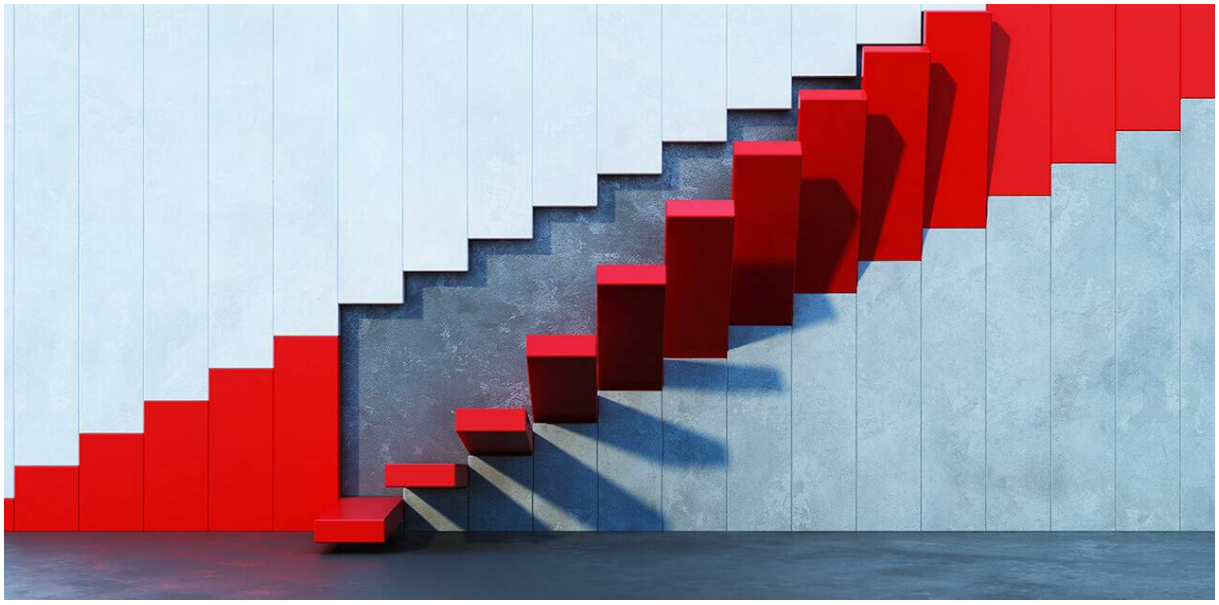
racine AVOCATS

Flash Info

23 octobre 2019



La Cnil a publié une liste de traitements qui ne sont pas soumis à PIA

En novembre 2018 la Cnil a publié, comme le RGPD le lui invite, une liste de traitements qui font obligatoirement l'objet d'un PIA. Cette liste n'est pas sans conséquence pour de nombreuses entreprises.

Rappelons que pour qu'un PIA s'impose, le traitement doit « rencontrer » deux critères sur les 9 dégagés par le G29.

En effet si cette liste vise essentiellement des responsables de traitements sectoriels (santé, banque, …), elle vise aussi toutes les entreprises notamment celles qui ont mis en œuvre des procédures d'alerte interne.

Hier la Cnil a publié une seconde liste : celle des traitements qui ne sont pas soumis à PIA.

Il faut là aussi distinguer les cas sectoriels des cas génériques.

Les cas sectoriels visent principalement les professions juridiques (avocats, notaires, greffiers des tribunaux de commerce), les professionnels de santé, mais aussi les comités d'entreprises (disons plutôt maintenant CSE), les associations pour leurs membres et donateurs, collectivités territoriales pour certains traitements.

Deux cas particuliers sont également traités : le contrôle d'accès des salariés (hors biométrie) et les tests alcooliques ou relatifs à la prise de stupéfiants pour les activités de transport.

Reste le cas des traitements « mis en œuvre uniquement à des fins de ressources humaines et dans les conditions prévues par les textes applicables, pour la seule gestion du personnel des organismes qui emploient moins de 250 personnes, à l'exception du recours au profilage » qui laisse un peu perplexe …

En effet, à la différence de la liste précédente, la Cnil ne précise pas les critères qui fondent cette liste. Deux interprétations sont donc possibles ce qui expose les entreprises…

Interprétation 1 – Toutes les entreprises qui ont plus de 250 employés doivent mettre en œuvre un PIA pour leur SI RH au motif que deux critères sont identifiés : personne vulnérable d'une part (dont on sait que la Cnil y inclus les salariés) et « collecte à large échelle » d'autre part….

Cela reviendrait donc à imposer un PIA en matière RH à un grès grand nombre d'entreprise… Gageons que ce ne soit pas le cas…

Interprétation 2 – Pour les entreprises de moins de 250 salariés, même si le SI RH rencontre deux critères sur 9 (dont un est déjà la personne vulnérable) ces entreprises ne sont jamais soumises à un PIA sauf pour les cas de profilage. Pour les entreprises de plus de 250 salariés, la question doit se régler au cas par cas en analysant si en plus du critère « personne vulnérable » un autre critère est applicable.

Si tel est le cas là encore cela nécessitera un travail important pour les entreprises de plus de 250 personnes qui devront obligatoirement analyser chaque SI RH pour identifier si les critères dégagés par la Cnil et le G29 s'appliquent.

Une précision sur la portée de cette exception semble nécessaire…..

Pour en savoir plus :

https://www.cnil.fr/fr/liste-traitements-aipd-non-requise

Auteur

Eric Barbry
Associé
Responsable Equipe IP-IT & Data Protection
ebarbry@racine.eu