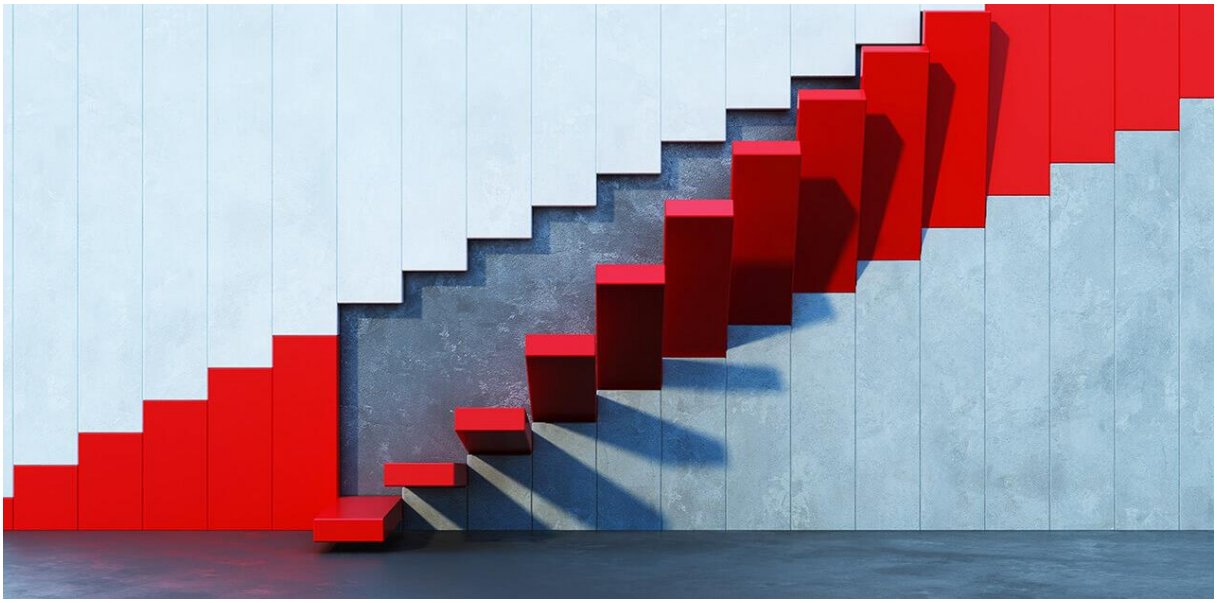
racine
AVOCATS

Flash Info

17 janvier 2018



Défaut de contrôle d'un sous-traitant, Darty condamnée par la Cnil à une sanction pécuniaire de 100 000 euros

La délibération de la formation restreinte n° SAN-2018-001 du 08/01/2018 prononçant une sanction pécuniaire de 100.000€ à l'encontre de Darty devrait conduire toutes les entreprises publiques ou privées à se lancer dans une véritable réflexion sur la sous-traitance.

Cette prise de conscience est d'autant plus importante que le RGPD va profondément bouleverser les relations entre le responsable du traitement et le sous-traitant, et qu'il ne reste guère plus de 4 mois pour une mise en conformité.

Le premier bouleversement concerne le choix du sous-traitant. L'article 28 prévoit en effet que le responsable du traitement fait « uniquement appel » à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée.

Le second bouleversement porte sur l'aspect contractuel. Avec le RGPD, exit les contrats et les clauses minimalistes en termes de données personnelles. Non seulement l'article 28 impose, comme c'est déjà le cas avec l'article 35 de la loi de 1978 actuelle, qu'un contrat soit rédigé entre les parties, mais il impose surtout que 8 dispositions figurent dans ce contrat (article 28/ point 3. Dispositions a) à h)).

Combiné de l'article 28.3 h) et des délibérations de la Cnil, notamment celle affectant Darty, le troisième bouleversement porte sur l'auditabilité du sous-traitant et la mise en œuvre effective

Responsable de publication : Eric Barbry

de ces audits. C'est bien sur le terrain du « manquement à l'obligation d'assurer la sécurité des données » que la Cnil a considéré Darty comme défaillante. La formation restreinte de la Cnil retient que « la circonstance que des opérations de traitement de données soient confiées à des sous-traitants ne décharge pas le responsable de traitement de la responsabilité qui lui incombe de préserver la sécurité des données traitées pour son compte ».

Le quatrième bouleversement porte sur la sous-traitance des sous-traitants. Le RGPD renforce l'obligation pour le sous-traitant d'informer le responsable du traitement de changements affectant les sous-traitants et confère sur ce point plus de droit au responsable de traitement, dont un nouveau droit, le droit « d'objection ».

Il existe bien d'autres impacts mais une brève n'y suffirait pas…

La mise en place de ces nouvelles règles et obligations passe nécessairement par :

- Action 1 : Adoption de pré-requis juridiques permettant de s'assurer en amont de la contractualisation que le sous-traitant pressenti présente les garanties suffisantes de respect du RGPD ;

- Action 2 : Cartographier les sous-traitant pour éviter notamment les cas de shadow IT;

- Action 3 : Réaction de clauses contractuelles conformes au RGPD, de préférence sous forme d'une annexe contractuelle dédiée à cet effet. Cette annexe devra être appliquée à tous les contrats à venir, mais également sous forme d'avenant aux contrats en cours au 25 mai 2018 ;

- Action 4 : Adoption d'une méthodologie d'audit des sous-traitants et surtout de leur mise en œuvre effective ;

- Action 5 : Anticipation par des simulations de situations de crise et de contrôle Cnil.

Il est à noter que cette décision est susceptible de faire l'objet d'un recours devant le Conseil d'Etat par la société Darty et Fils, affaire à suivre …

***

Pour en savoir plus

Consulter la délibération sur le site de Legifrance

Auteurs

Eric Barbry
Avocat associé
ebarbry@racine.eu

Marianne Long
Avocat
mlong@racine.eu

Responsable de publication : Eric Barbry