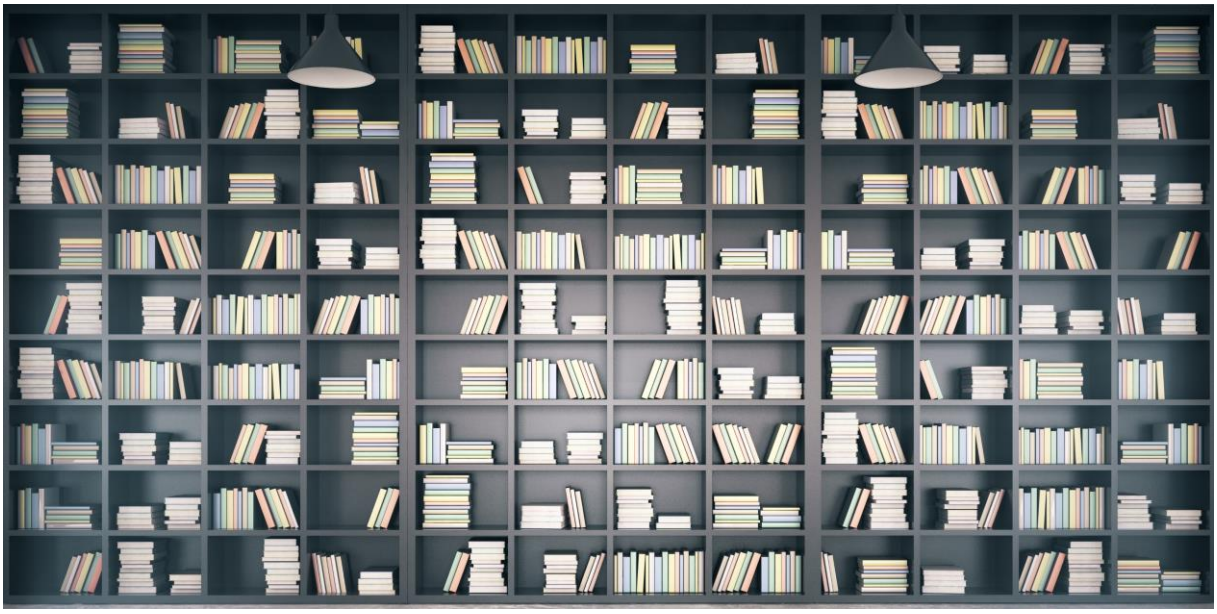
racine AVOCATS

# Flash Info

06 février 2018



## La Cnil publie un guide de la sécurité

Moins de 4 mois avant l'entrée en vigueur du règlement européen sur la protection des données[1] (ci-après « RGPD »), la Cnil dote les entreprises d'un nouveau guide pratique afin de les accompagner dans leur démarche de mise en conformité.

Après la publication d'un guide orienté sous-traitants, la Cnil publie sur le deuxième volet le plus important du RGPD à savoir la sécurité. Elle souhaite, par ce biais, assister les entreprises dans la gestion de leurs risques, en quatre étapes :

- recenser les traitements ;
- apprécier les risque ;
- mettre en œuvre et vérifier les mesures prévues ;
- faire réaliser des audits de sécurité périodiques.

C'est en tout 17 fiches pratiques qui sont mises à la disposition des entreprises et notamment, des DSI et RSSI, afin de les sensibiliser aux questions de sécurité, questions à grands enjeux, notamment financiers.

Plus encore, la Cnil établit une véritable checklist afin que les entreprises puissent évaluer le niveau de sécurité des données à caractère personnel collectées par l'organisme.

[1] RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Quelles précautions les entreprises doivent-elles finalement adopter, de manière systématique, afin d'assurer la conformité de ses traitements à la réglementation européenne de protection des données ?

C'est l'article 32 du RGPD qui fait peser tant sur les responsables du traitement que les sous-traitants, une obligation accrue en terme de sécurité en les enjoignant de mettre en œuvre « les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (…) ».

Un plan d'actions en quatre temps doit être envisagé afin d'assurer le minimum requis en termes de sécurité :

- l'implémentation de solutions techniques : il peut s'agir de solutions d'authentification sécurisées des utilisateurs du système d'information, mais également des procédés de journalisation des accès, ou encore de prévention d'accès frauduleux ;

- l'adoption d'un PCA (plan de continuité d'activité) qui garantit la survie d'une entreprise en cas d'attaque touchant l'intégralité du système informatique. Ce plan permettra un redémarrage de l'activité, le plus rapidement possible, avec le moins de perte possible ;

- l'adoption d'un PRA (plan de reprise d'activité) qui garantit, en cas de crise informatique, la remise en route de l'activité d'une entreprise ;

- la mise en place de procédures d'audit : les audits sont nécessaires afin de garantir un niveau de sécurité optimal de son système d'information. Il permet également de s'assurer d'un niveau de sécurité équivalent chez les prestataires avec lesquels on contracte. Rappelons le, la dernière condamnation de la Cnil mettait en cause un défaut de contrôle du responsable du traitement de son prestataire et l'audit reste aujourd'hui la meilleure façon de vérifier sa conformité.

Il existe évidemment bien d'autres outils afin de sécuriser son système d'information, notamment la traçabilité des accès ou encore des procéder de pseudonymisation et d'anonymisation des données.

Une étude des risques est aujourd'hui essentielle afin de déterminer quelles mesures de sécurité doivent être implémentées dans l'entreprise afin de faire face à toute situation de crise, mais également afin d'être en mesure de se préparer contre des cyber-attaques, de plus en plus redoutées.

***

**Pour en savoir plus**

Pour en savoir plus, rendez-vous sur le site de la Cnil

## Auteurs


**Eric Barbry**
Avocat associé
ebarbry@racine.eu

**Marianne Long**
Avocat
mlong@racine.eu