Un nouvel outil de conformité au RGPD : les certifications

écrit par Marine de la Clergerie | 21/05/2018

Avec l'entrée en application prochaine du règlement européen à la protection des données (RGPD), la CNIL met en place un nouvel outil de conformité, la certification, et met progressivement fin à son activité de labellisation.

Conformément à l'article 42 du RGPD, les certifications seront délivrées par des organismes certificateurs agréés par la CNIL ou accrédités par l'organisme national d'accréditation (COFRAC). La CNIL aura pour mission d'élaborer ou d'approuver les référentiels de certification qui seront utilisés par les certificateurs, ainsi que, le cas échéant, les référentiels d'agrément.

Que deviennent les labels actuels à l'entrée en application du règlement ?

- La CNIL prévoit de ne plus délivrer de nouveau label après le 25 mai 2018.
- Les labels émis avant l'entrée en application du règlement restent valables jusqu'à leur date d'échéance, mais n'emportent pas tous de conséquence sur le plan de la conformité RGPD.
- Seuls les labels Gouvernance et Formation dont les référentiels ont été mis à jour pour tenir compte du RGPD, pourront offrir à leurs bénéficiaires un tel argument de conformité.

Quand sera-t-il possible de se faire certifier ?

- Les référentiels de certification seront élaborés après une phase de consultation publique, approuvés par la CNIL et publiés sur son site. Il appartiendra ensuite aux candidats de se rapprocher des certificateurs, qui procèderont à l'instruction de leurs demandes.
- Les travaux sur les premiers référentiels ont déjà débuté. Une certification de Délégués à la Protection des Données est ainsi en cours d'élaboration : des organismes de certification agréés par la CNIL délivreront des certifications de DPO, sur la base d'un référentiel rédigé par la CNIL. Parallèlement, des travaux sont menés en matière de certification de formation RGPD avec le COFRAC.

Quels sont les avantages de la certification ?

La certification ne limite pas la responsabilité des responsables de traitement ou des sous-traitants en cas de violation du Règlement et n'interdit pas un contrôle ou une sanction de la CNIL. Toutefois, l'application de mécanismes de certification **permet aux responsables de traitement de démontrer le respect de leurs obligations et de limiter, le cas échéant, les amendes administratives susceptibles d'être prononcées.**

Combien de temps une certification est elle valable ?

La certification sera délivrée à un responsable du traitement ou à un sous-traitant pour une durée maximale de trois ans et pourra être renouvelée tant que les exigences applicables continueront d'être satisfaites.

Auteur: Damien Billerit, élève-avocat

Références :

- Article 42 du RGPD
- Article de la CNIL du 28.02.2018