

# Règlement européen sur la protection des données : ce qu'en pensent les entreprises

La Commission nationale de l'informatique et des libertés (CNIL) a rendu publique lundi la [synthèse](#) de contributions proposées lors d'une consultation sur le [Règlement européen sur la protection des données](#) (RGPD ou GDPR, en anglais). Rappelons que ce Règlement, qui entrera en vigueur en mai 2018, introduit de nouveaux droits des personnes et des obligations nouvelles pour les entreprises. Le texte renforce également les sanctions administratives à l'encontre des responsables de traitement et des sous-traitants qui ne respecteraient pas les dispositions du texte. Les entreprises et les administrations actives dans l'Union européenne sont toutes concernées, et pas seulement celles qui ont adopté le Cloud. Les professionnels ont été consultés cet été par la CNIL.

225 contributeurs, entreprises et fédérations professionnelles, ont posté plus de 540 contributions, soumises à 994 votes. Quatre premiers thèmes inscrits au plan d'action du G29, le groupe des CNIL européennes, ont été abordés. La mission de délégué à la protection des données inquiète le plus.

## **CIL, de futurs DPO ?**

Un délégué à la protection des données (DPO) est-il responsable pénalement ? Peut-il être licencié pour faute ? Pourra-t-il exercer une autre fonction ? Les interrogations des entreprises sont nombreuses. Elles attendent des clarifications sur la responsabilité, le rôle, les moyens et les missions de ce DPO, qui n'est pas sans rappeler le CIL (correspondant informatique et libertés).

Pour répondre à ces attentes, la CNIL se dit prête à réaliser « *des actions de communication auprès des organismes ayant actuellement un CIL, et auprès des fédérations professionnelles concernées par la désignation obligatoire d'un DPO (courriers spécifiques, fiches pratiques)* ». Par ailleurs, les ateliers CIL seront enrichis (format, volume et contenus), a fait savoir le régulateur français.

Selon les prévisions de l'IAPP (International Association of Privacy Professionals), [75 000 postes de DPO](#) seront à pourvoir dans le monde, dont au moins 28 000 en Europe et aux États-Unis. Le but : répondre présent dès le lancement du Règlement européen sur la protection des données.

## **Portabilité mal perçue**

Le droit à la portabilité permet à une personne de récupérer des données à caractère personnel, sous une forme aisément réutilisable, et, si elle le souhaite, de les transférer à un tiers. Les entreprises y voient l'occasion de « *redonner confiance au client dans l'exploitation qu'elles font de ses données* ». Mais elles s'interrogent aussi beaucoup sur le coût et le périmètre réel de ce nouveau droit, qu'elles souhaitent « *limiter au strict minimum* », selon la CNIL.

Le groupe technologie du G29, de son côté, planche sur un avis visant à clarifier ce périmètre, « *en fonction duquel les actions à mettre en oeuvre pourront être définies* ». À préciser, par conséquent.

# Certification et labellisation

Le Règlement européen encourage aussi la mise en place de mécanismes de certification et de labels de protection des données. La délivrance de ces labels pourra être réalisée par le régulateur ou des organismes de certification accrédités. Les entreprises y sont plutôt favorables, à la condition que le cadre européen garantisse « *un niveau élevé et homogène des normes utilisées* ». Et les PME ne veulent pas de processus coûteux et complexes de certification ou labellisation. Les attentes des CIL, organismes et fédérations professionnelles sont fortes dans ce domaine. La CNIL, en plus d'actions déjà menées à leur attention, leur proposera de nouveaux supports et outils didactiques.

## Études d'impact

Le nouveau cadre européen sur la protection des données prévoit une analyse d'impact sur la vie privée (PIA ou DPIA, en anglais) « *pour tous traitements susceptibles d'engendrer des risques élevés* ». Les entreprises demandent à la CNIL de clarifier le flou autour de ces notions. « *Les points durs concernent les critères qui guideront la décision de mener un DPIA, l'harmonisation de la démarche au niveau européen, et la consultation préalable* », précise la Commission informatique (qui propose déjà des guides PIA). L'avis du G29, qui tiendra compte des contributions des entreprises, est très attendu par l'industrie.

Les CNIL européennes ne sont pas seules à s'engager, des organisations professionnelles le font aussi. C'est le cas de l'Afai (auditeurs), du Cigref (DSI de grandes entreprises) et de Tech in France (éditeurs de logiciels). Ils ont lancé [une réflexion commune](#) sur la question des données personnelles. Leur objectif : « *simplifier l'appréhension des réglementations par les entreprises* ».

### Lire aussi :

- [Données personnelles : l'Afai, le Cigref et Tech in France plangent sur le règlement de l'UE](#)
- [CISPE, lobby européen du Cloud, publie un code de conduite conforme GDPR](#)
- [Protection des données personnelles : nouvelles contraintes en vue pour les entreprises](#)

Photo credit: blakewinton via Visualhunt / CC BY