RGPD : la recette « conformité » de l'Afai, du Cigref et de Tech in France

Il y a urgence pour les entreprises à se conformer au Règlement général sur la protection des données (RGPD ou GDPR en anglais). Le texte entrera en vigueur le 25 mai 2018.

Rappelons que le RGPD indroduit de nouveaux droits pour les personnes (dont la portabilité des données) et des obligations pour les entreprises (dont la notification de toute violation de données à la CNIL). Le texte renforce également les sanctions administratives à l'encontre des responsables de traitement et des sous-traitants en infraction. Avec des amendes pouvant s'élever de 2 à 4% du chiffre d'affaires annuel mondial de l'entreprise concernée ou 10 à 20 millions d'euros.

Trois organisations – L'Association française de l'audit et du conseil informatiques (AFAI), le Cigref (qui représente les DSI de grandes entreprises françaises) et Tech in France (les éditeurs de logiciels) – se sont mobilisées sur le sujet dès l'été 2016. Elles ont engagé l'initiative *« données personnelles et systèmes d'information »* (DPSI) pour sensibiliser les clients et les fournisseurs. Et produire un guide pratique. Le tout avec le soutien de cabinets d'avocats et la participation *« régulière »* de la Commission nationale informatique et libertés (CNIL).

Les résultats de leurs travaux ont été restitués cette semaine et publiés sous la forme d'un document de 144 pages. *« La mise en conformité au GDPR implique des changements de taille au sein des entreprises »*, expliquent l'Afai, le Cigref et Tech in France. Leurs travaux ont donc pour objectif de les aider à *« élaborer un dispositif complet de protection des données »*.

« Privacy by re-design » des systèmes hérités

Le document rendu public mercredi 14 novembre inclut :

- Un guide d'auto-évaluation (« Check-list GDPR »).

Les entreprises peuvent répondre à 50 questions. Elles ont ainsi la possibilité d'évaluer leur niveau de conformité au Règlement européen.

- Des recommandations et mesures techniques.

Elles sont plus de 300, ces recommandations et mesures axées sur la sécurité du SI, la protection des données et le droit des personnes.

- Des outils juridiques de mise en conformité.

Les entreprises doivent *« être à tout moment en mesure de démontrer leur conformité au règlement »*, expliquent les trois organisations.

Par ailleurs, elles mettent en exergue l'intégration de la protection des données dès la conception (privacy by design). Et ce pour un projet, produit ou service de traitement. Mais également *« par défaut »*. En réduisant tout traitement de données personnelles *« au minimum nécessaire »*,

conformément au principe de minimisation introduit par le RGPD.

Dans ce contexte, *« certains systèmes legacy devront potentiellement faire l'objet de privacy by re-design s'ils sont sensibles »,* ajoutent les organisations professionnelles.

Budget « proportionnel à l'enjeu »

L'Afai, le Cigref et Tech in France recommandent entres autres mesures :

- une gouvernance forte avec un rattachement du délégué à la protection des données (data protection officer – DPO) *« au plus haut niveau de l'entreprise »* ;
- un registre permettant de recenser les traitements de données personnelles ;
- une stratégie formalisée de mise en oeuvre du dispositif ;
- la prise en compte des problématiques de protection dans différents processus opérationnels : des développements internes à la gestion de sous-traitants et de tiers ;
- un programme d'audit régulier.

« Au sein des entreprises, la conformité doit être gérée comme un projet », estiment l'Afai, le Cigref et Tech in France. *« Avant d'être juridique ou légal, ce projet est global. Avec une forte composante SI, puisque la mise en conformité nécessite la mise en place de mesures techniques liées à la sécurité des systèmes d'information et à la protection des données*, ajoutent-ils. *Il est donc absolument crucial*, selon eux, *d'y consacrer un budget qui soit proportionnel à l'enjeu. »*

Lire également :

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

Données personnelles : Afai, Cigref et Tech in France planchent sur le règlement de l'UE

crédit photo © Rawpixel.com / Shutterstock