



25.05.20

1. Pourquoi avez-vous choisi de valoriser dposystem à l'heure de la crise sanitaire ? Cette crise implique-t-elle de nouveaux enjeux pour vos activités ? La crise va-t-elle accélérer ou mettre entre parenthèse la mise en conformité au RGPD selon vous ?

Les circonstances exceptionnelles de l'épidémie de COVID-19 et l'explosion du travail à distance présentent les défis les plus importants du RGPD depuis 2 ans.

Notre activité est plus que jamais majeure dans ce contexte de crise et nous avons une responsabilité à orienter et conseiller en valorisant davantage les réflexions éthiques d'ores et déjà présentes dans nos missions.

Les collaborateurs au sein des organisations sont encore insuffisamment préparés aux risques pesant sur la protection des données, y compris des données personnelles.

Les cybermenaces circulent plus que jamais et la situation financière des entreprises n'encourage pas les investissements dans la sécurité et pourrait retarder la protection des données personnelles.

En pratique nous relevons un challenge « faire plus avec moins » et à ce titre nous ne manquons pas d'innovations telle que l'organisation en centre de service ou les sensibilisations en e-learning.

Par ailleurs, les mesures de lutte contre le COVID-19 ne peuvent pas servir d'excuse au non-respect du RGPD. La course de vitesse dans la crise actuelle ne doit pas être utilisée pour écarter la conformité et la confidentialité des données tant pour les services publics que pour les organisations privées.

Nos clients nous questionnent :

- Quelle conformité pour des scanners de température, dans les établissements scolaires ou les entreprises ?
- Une surveillance par drone est-elle envisageable ?
- Quelles sont les mesures à prendre vis-à-vis des données de santé pour une collectivité ou pour des projets de recherche ?
- Quels risques dans les applications de contact tracing ?
- Quels cadres de protection des données vis-à-vis du télétravail ?

La législation sur la protection des données reste donc une considération centrale dans les stratégies de nos clients. Les organisations doivent éviter d'être perçues comme ayant profité de la volonté des gens de partager leurs informations à des fins autres qu'utiles pour lutter contre l'épidémie. Il est plus important que jamais de se comporter de manière fiable avec les données des personnes sans quoi aucune transformation digitale ne pourra être engagée que ce soit pour les PME ou les grandes métropoles.

2. Le RGPD fête ses 2 ans : quel bilan en tirez-vous ?

Le RGPD a pris effet en mai 2018 : c'est une des plus grandes avancées dans la protection des données depuis plusieurs dizaine d'années. Globalement les exigences du RGPD ont signifié aux organisations qu'elles devaient être particulièrement attentives aux données qu'elles traitent, y compris la façon dont elles collectent, utilisent, partagent, sécurisent et conservent ces données pour elles-mêmes et leurs partenaires.

Mais le socle de conformité du RGPD visant à garantir un ensemble complet de protection des droits fondamentaux des individus face aux technologies actuelles et futures n'est pas uniforme. Ainsi, il y a encore pour de nombreuses organisations, un chantier ouvert pour une bonne compréhension des principes, concepts et règles du RGPD.

Le RGPD incite clairement les organisations à considérer leur conformité et leur stratégie en matière de protection des données comme un levier de création de valeur. Sans cela, la protection ne pourrait être que limitée et le développement de nouveaux produits et services serait inutilement entravé.

3. Le métier de DPO a-t-il évolué durant ces deux premières années ? Si oui, comment ?

Durant ces deux années, le RGPD a accru la responsabilité des responsables de traitements ainsi que des sous-traitants et les DPO ont permis une plus grande sensibilisation aux problèmes de protection des données à tous les niveaux.

Il existe de nombreuses raisons à cela, au-delà des risques d'amendes potentielles et des risques d'atteinte à la réputation, c'est surtout dû au travail des DPO.

Le DPO doit continuer d'être un expert du RGPD et des pratiques de confidentialité, il est responsable du pilotage de la conformité et doit contrôler le respect du RGPD. Les DPO sont censés aider et guider les responsables de traitements au-delà de la vérification, en suggérant les recommandations correctives appropriées.

Au cours d'une [enquête de la CNIL](#), les DPO ont affirmé pour un tiers être informaticien, pour un tiers être juriste et pour un tiers avoir d'autres domaines d'expertises ailleurs c'est un métier que les DPO recommandent largement pour son caractère éthique, sa transversalité et la variété des missions et compétences.

Au fil des mois, le métier de DPO évolue sur plusieurs axes :

- La nécessaire indépendance des DPO s'est affirmée : il n'est plus question de cumuler cette fonction avec une autre fonction et de nombreuses organisations externalisent et mutualisent leur DPO ou un ensemble de rôles.
- L'étendue des compétences technologique s'élargie :
 - Maîtrise des principes de security by design, Anonymisation, Archivage, Open Data, Cloud, IA, Objets Connectés etc.
- Les savoirs-être associés à la gestion de conflits s'avèrent essentiels :
 - Médiation avec les directions métiers etc.
- Les savoirs-faire associés au pilotage et à l'organisation d'un Système d'information sont importants :
 - Gestion de crise cyber, Gouvernance des données etc.

Enfin, le RGPD est exigeant mais reste « général », les entreprises et services publics font encore face à une absence d'aide opérationnelle et ont besoin d'énormément de conseils pour le maintien de leur conformité. Ainsi, leurs DPO ont tout intérêt à travailler en réseau et à s'appuyer sur un support méthodologique, technique et juridique.