La conformité au RGPD est devenue une évidence, au service des collectivités et des citoyens

François COUPEZ
Avocat associé
Implid Legal

Il ne se passe pas quelques semaines, même pendant la période du mois d'août, sans que l'on ne parle d'une nouvelle décision d'un régulateur ou d'une cour de justice concernant l'application des règles en matière de protection des données personnelles (notamment le Règlement européen n°2016/679, dit « règlement général sur la protection des données » ou encore RGPD) :

- invalidation du Privacy Shield par la Cour de Justice de l'Union Européenne (prévisible, mais trop longtemps attendue) ;

- mise en cause plus largement du régime juridique de protection des données personnelles aux USA rendant problématique l'encadrement juridique de ces données entre l'Espace Economique Européen et les USA (idem) ;

- mise en cause par la CNIL de l'utilisation du reCAPTCHA de Google par les sites internet et application (elle aussi prévisible et trop longtemps attendue) - cf. décision MED-2020-015 de la CNIL d'audit de l'application StopCOVID ;

- ou encore mises en demeure par la CNIL en ce mois d'août 2020 de quatre communes du fait de la collecte et du traitement de photographies des véhicules, notamment en vue rapprochée de la plaque d'immatriculation, pour l'exercice du pouvoir de police par les communes (en lien avec la tranquillité publique ou la salubrité publique). La CNIL rappelle en effet que le traitement de ces photographies n'est pas autorisé en l'état actuel de la réglementation (notamment l'arrêté du 14 avril 2009 et son article 6).

Pourtant, tout comme la cybersécurité, la conformité RGPD n'est pas toujours prise au sérieux dans l'ensemble de ses composantes.

La réglementation française en matière de protection des données a beau avoir fêté ses 42 printemps et s'être renforcée au fil des années, notamment avec le RGPD depuis le 25 mai 2018, trop souvent encore, certaines collectivités en restent à la nomination d'un DPO mutualisé disposant de peu de moyens et sans que la gestion des données soit considérée comme devant réordonner la façon même dont la « relation citoyen » doit être fondée. L'e-administration (simplification administrative) est pourtant un axe important de modernisation de l'action publique et répond à une demande effective des citoyens dans le cadre de l'e-démocratie, le respect des règles de protection des données à caractère personnel par les collectivités étant un facteur de transparence et de confiance à l'égard des usagers, mais aussi du personnel qui y travaille.

Au-delà d'un renforcement de la sécurité des systèmes d'information, pierre angulaire de la conformité en matière de protection des données personnelles, la conformité en la matière suppose également l'adoption de mesures organisationnelles, sans oublier les nécessaires analyses juridiques préalables. Ainsi, le fait que la fiche « l'impact du RGPD sur le droit de la commande publique » émanant de la Direction des affaires juridiques (DAJ) du ministère de l'économie[1] ne mentionne que l'hypothèse d'un fournisseur forcément « sous-traitant » au sens du RGPD est révélateur du travail qui reste encore à parcourir sur le sujet. De plus en plus, nous constatons en pratique dans les dossiers dans lesquels nous intervenons que les qualifications essentielles en matière de traitement de données personnelles (quel est l'un des six fondements légaux utilisés pour le traitement ? Qui est responsable de traitement, sous-traitant, responsable conjoint, responsable disjoint, tiers autorisé ?) n'ont pas été analysées et que les mises en conformité effectuées par la suite s'avèrent en conséquence à reprendre en quasi-totalité.

Nous nous permettrons donc ici de rappeler que seule une approche intégrant les trois piliers fondamentaux (organisationnel, technique et juridique) met en œuvre de façon efficace les principes découlant du RGPD, étant entendu que la plupart des collectivités territoriales ont déjà un acquis sur le sujet sur lequel s'appuyer et peuvent souvent recourir à des solutions mutualisées et/ou éprouvées :

- cartographie des traitements existants ;

- identification des données traitées ;

- identification des acteurs de l'écosystème traitant les données (sous-traitant, fournisseurs, etc.), des lieux à partir desquels les données sont accédées et qualification de leur rôle au regard du traitement des données personnelles ;

- encadrement juridique approprié des relations économiques avec ceux-ci ;

- construction et sécurisation de traitements orientés « *privacy by design* » ;

- détermination des fondements légaux permettant leur traitement ;

- création/mise à jour d'un registre des traitements, d'un registre des sous-traitants et d'un registre des violations de données à caractère personnel ;

- transparence des informations à communiquer ;

- documentation de l'ensemble de la chaîne de traitement et des décisions prises ;

- nomination obligatoire de Délégués à la Protection des Données (DPD/DPO) pour les entités du secteur public ;

- réalisation d'études d'impact sur la vie privée dans les cas où les traitements ont les conséquences les plus graves pour les personnes ;

- création des processus de notification des violations de données personnelles ;

- etc.

Cet engagement dans un process de conformité au RGPD nécessite ainsi une dynamique portée par les élus, un chef de projet référent, un travail en collaboration avec l'ensemble des services, parfois l'accompagnement d'experts extérieurs de confiance, et un engagement sur le long terme afin de faire de cette réglementation un véritable atout pour les collectivités. Car à la fin, tout le monde, citoyens et collectivités territoriales, doit sortir gagnant de cette conformité !

[1] https://www.economie.gouv.fr/files/files/directions_services/daj/marches_publics/conseil_acheteurs/fiches-techniques/preparation-procedure/impact_RGPD_droit_Commande_Publique.pdf