Règlement sur les données personnelles : se mettre en conformité

Le 25 mai prochain, le règlement général sur la protection des données personnelles (RGPD) entrera en application. Les étapes clés pour l'appliquer.

Le nouveau règlement européen sur la protection des données personnelles confirme les grands principes d'ores et déjà en vigueur en France en matière de protection de la vie privée. Il initie cependant un changement d'approche. En contrepartie d'une réduction drastique des formalités déclaratives, il responsabilise les acteurs. Ceux-ci devront à tout moment pouvoir prouver qu'ils ont pris des dispositions *ad hoc* pour protéger les données personnelles dont ils ont la charge. En cas de manquement, les sanctions pourront atteindre 20 millions d'euros. À quelques semaines de l'échéance, il n'est pas trop tard pour agir.

1 Nommer un délégué à la protection des données

Le délégué à la protection des données (DPD) remplace le correspondant informatique et liberté (CIL) et devient obligatoire. Ce DPD a une mission d'information, de conseil et de contrôle des obligations. Il intervient dans les choix de logiciels, la mise en place de services numériques ou encore l'ouverture des données publiques.

On notera que le règlement européen autorise la mutualisation du DPD qui peut se faire à l'échelle intercommunale, d'un syndicat informatique ou d'un centre de gestion. Mais celle-ci implique malgré tout un agent communal pour suivre le dossier.

2 Recenser les traitements

La phase « état des lieux » établit une cartographie des traitements : quels services utilisent des données personnelles (état civil, scolaire, bibliothèque, centre communal d'action sociale...) ? pour quelles finalités (obligation légale, suivi administratif...) ? Avec quels acteurs (écoles, association d'aide sociale, éditeurs...) ? Mis à jour régulièrement, ce document décrira les flux de données entre services et/ou avec les usagers et mettra en valeur les points de vigilance comme, par exemple, le site utilisé pour réaliser des formalités en ligne.

En savoir +

Le guide de la CNIL : www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes

3 Prioriser les actions

L'état des lieux aidera à prioriser les actions. Une priorisation fondée sur les risques que feraient peser une fuite de données personnelles ou un détournement d'utilisation du fichier. Les collectivités doivent se demander si le traitement respecte les grands principes de la loi : adéquation des données collectées par rapport à la finalité, base juridique du traitement, mode d'expression du consentement, mise en œuvre du droit d'accès et de rectification, sécurité des traitements (accès, chiffrement, formulaires, stockage...), droit à la portabilité...

4 Traiter les risques

L'identification des risques doit se traduire par un plan d'actions adapté aux moyens de la collectivité. Certaines sont relativement simples : suppression de données inutiles, renforcement de la sécurité informatique. D'autres impliquent une remise à plat des processus et, éventuellement, une étude. Le règlement européen sur les données personnelles exige en effet la réalisation d'une étude d'impact dès lors que le traitement concerne des données sensibles : personnes vulnérables, risque de croisements de fichiers, usages de technologies potentiellement intrusives...

5 Organiser et documenter les processus

La collectivité doit impliquer ses agents et modifier ses pratiques pour intégrer la protection des données personnelles à son fonctionnement quotidien. Formation des élus et des agents (notamment des nouveaux arrivants), gestion des demandes des citoyens, conduite à tenir en cas de fuite de données personnelles... Toutes ces questions doivent être documentées.

Il s'agit aussi d'intégrer la protection des données dans la phase de conception (design) des services, dans une logique dite de « privacy by design » (« protection de la vie privée dès la conception »).

Les marchés publics concernant des services utilisant des données personnelles devront se référer au règlement européen sur les données personnelles, sachant que cette clause ne dédouanera pas la collectivité de ses propres responsabilités.

Olivier DEVILLERS

Les mesures du RGPD

- L'obligation pour les organisations de tenir à jour un registre des traitements de données personnelles,
- De nouveaux droits pour les citoyens : portabilité de ses données personnelles, droit à l'oubli,
- La fixation d'une « majorité » (15 ou 16 ans) pour donner son consentement au traitement de ses données personnelles sans l'autorisation de ses parents,
- Des sanctions pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires d'une entreprise.