Bureau d'information et de communication

Rue de la Barre 2
1014 Lausanne

COMMUNIQUÉ DE PRESSE
Cour des comptes

Protection des données dans l'administration cantonale: un audit pointe des lacunes de mise en œuvre par les entités-métiers

L'audit de la Cour des comptes consacré à la protection des données dans l'administration cantonale révèle une mise en œuvre inégale des dispositions y relatives dans les entités-métiers. Toutefois, la Cour relève que la confidentialité des données et leur sécurité sont globalement assurées grâce au secret de fonction et aux mesures de sécurité relatives à l'architecture informatique.

La législation sur la protection des données personnelles vise à prévenir le traitement abusif des données relatives aux personnes et à protéger tant leur personnalité que leur sphère privée. La question de la sécurité informatique constitue un enjeu majeur ; en témoignent les cyberattaques dont les entités publiques sont la cible.

La Cour a audité cette thématique selon deux axes : la protection selon la loi vaudoise sur la protection des données (LPrD) et la sécurité. Elle a centré son analyse sur l'administration cantonale vaudoise (ACV) en auditant les conditions-cadres mises en place par les entités transversales que sont l'Autorité de protection des données et de droit à l'information (APDI), le Service du personnel (SPEV) et la Direction générale du numérique et des systèmes d'information (DGNSI).

L'application de la LPrD a également été examinée dans huit entités-métiers traitant des données administratives, médicales, en lien avec l'enseignement ou avec des mesures d'aide sociale. Des manquements parfois importants ont été constatés : peu d'entités ont procédé à une identification exhaustive des données personnelles traitées ; aucune n'en a effectué une analyse complète en regard des exigences de la LPrD et n'a adopté de stratégie adaptée à son activité. Parmi les lacunes constatées, la Cour a notamment relevé des clauses contractuelles insuffisantes en cas de sous-traitance ou de délégation de tâches, une gestion insuffisante des accès aux applications ou l'envoi par messagerie électronique de fichiers contenant des données sensibles sans sécurisation adéquate. Ces entités-métiers n'ont pas ou peu entamé de réflexion sur la conservation des données personnelles qu'elles gèrent, les stockant le plus souvent indéfiniment sans les avoir anonymisées.

Pour la Cour, ces problèmes sont essentiellement dus à un manque de connaissance des employées et employés sur les dispositions LPrD, et ce à tous les échelons hiérarchiques de l'ACV. Il en est de même avec les règles de sécurité informatique: des tests de « hameçonnage » (phishing) réalisés par la DGNSI ont montré qu'une partie non négligeable du personnel de l'ACV n'est pas non plus au fait des bonnes pratiques. La Cour relève en outre que l'APDI, dont l'activité est centrée actuellement sur le conseil et l'appui aux entités-métiers, n'en consacre qu'une part marginale à la surveillance de l'application de la LPrD.

Sur la base des constats et des conclusions d'audit, la Cour adresse 20 recommandations :

Treize recommandations visent l'amélioration des conditions-cadres et s'adressent :

- Au Conseil d'Etat qui les accepte toutes (3) :

- Instituer la fonction de déléguée ou délégué en protection des données dans chaque entité ;

- Rendre obligatoire l'annonce de toute violation en matière de sécurité des données ;

- Adapter le cadre légal pour intégrer les impératifs de protection des données.

- Aux entités-cadres (APDI, DGNSI et SPEV) qui les acceptent toutes (9) :

- Instaurer une formation minimale en protection et sécurité des données (SPEV) ;

- Informer les entités-métiers de leurs responsabilités en matière de protection et sécurité des données et de formation de leur personnel (APDI, DGNSI et SPEV) ;

- Renforcer la surveillance des entités-métiers par l'APDI (APDI) ;

- Compléter les compétences en informatique de l'APDI (APDI) ;

- Actualiser tous les processus de la DGNSI et le cadre contractuel pour intégrer les impératifs de protection des données et du secret de fonction (DGNSI) ;

- Réviser la directive LPers 50.1 et consolider une liste de règles de bonnes pratiques en matière de sécurité informatique (SPEV, DGNSI).

- À l'ensemble des entités-métiers auditées qui l'acceptent (1) :

- Identifier toutes les données personnelles gérées et documenter leurs mesures de protection.

Sept recommandations visent à combler des lacunes précises relevées dans les entités-métiers. Seule une entité-office refuse celle qui lui est adressée et en propose une variante plus légère.

Malgré les manquements constatés dans l'application de la LPrD, la Cour relève cependant que la culture de la confidentialité assurée par le secret de fonction ou le secret professionnel, tout comme la sécurité informatique, permettent de garantir un

certain niveau de protection des données. Mais les lacunes constatées augmentent les risques en cas de fuite ou vol de données.

Plus de dix ans après l'entrée en vigueur de la LPrD, la Cour estime qu'il est temps que l'entier de l'Administration cantonale s'implique dans sa mise en œuvre afin de garantir efficacement la protection des données personnelles des citoyennes et des citoyens.

Bureau d'information et de communication de l'Etat de Vaud

Lausanne, le 12 janvier 2022

RENSEIGNEMENTS

Valérie Schwaar, Présidente de la Cour des comptes, valerie.schwaar@vd.ch,
021 316 58 14

LIENS

Rapport n° 74 et sa synthèse
Capsule vidéo de présentation