COUR DES COMPTES
CANTON DE VAUD

Cour des comptes du canton de Vaud

Audit de la protection des données personnelles dans l'Administration cantonale vaudoise

Synthèse du rapport d'audit

Rapport N°74

Décembre 2021

Cour des comptes du canton de Vaud
Rue Langallerie 11 - 1014 Lausanne
Téléphone : 021 316 58 00
Courriel : info.cour-des-comptes@vd.ch

Le rapport complet est librement accessible sur le site de la Cour des comptes du canton de Vaud : www.vd.ch/cdc.

Vous trouverez également sur ce site des informations générales sur les attributions, le fonctionnement et le champ de contrôle de la Cour des comptes.

POURQUOI UN AUDIT SUR LA PROTECTION DES DONNÉES DANS L'ADMINISTRATION CANTONALE VAUDOISE (ACV) ?

Qu'est-ce-que la protection des données personnelles ?

La législation sur la protection des données personnelles vise à prévenir le traitement abusif des données relatives aux personnes et à protéger leur personnalité ainsi que leur sphère privée. Il s'agit d'un droit fondamental ancré dans les Constitutions suisse et vaudoise. Les pouvoirs publics, qui gèrent bon nombre de données relatives à leurs administré·e·s, sont particulièrement concernés par les exigences qui en découlent.

Les entités publiques du canton de Vaud sont soumises à la loi cantonale sur la protection des données personnelles (LPrD). Ses dispositions sont régies par un cadre international contraignant pour la Suisse. Cela requiert, pour tout traitement de données personnelles, le respect des principes-clés suivants : la légalité, la finalité, la proportionnalité, la transparence, l'exactitude, la sécurité, la conservation et le consentement. En découle également le droit pour tout individu de maîtriser ses données personnelles et de pouvoir y accéder. Enfin, cette loi instaure une autorité indépendante – le·la préposé·e à la protection des données – en charge de la surveillance de l'application et de la promotion de cette législation.

Quel intérêt d'examiner l'application de la loi dans l'Administration cantonale ?

Si les principes de la loi sont simples, leur application est complexe. La définition précise de ce qui est requis ou de ce qui est interdit ne figure souvent pas clairement dans les textes législatifs et demande une bonne connaissance du métier concerné voire une pesée des intérêts.

En outre, les enjeux et les problèmes liés à la sécurité des données, en particulier informatiques, sont d'une actualité brûlante :

- les cyberattaques, dont sont victimes un certain nombre d'entités publiques et privées, illustrent les conséquences qu'un déficit de sécurité peut causer : dégât d'image, coûts de récupération des données, demande et versement de rançons, paralysie temporaire du fonctionnement de l'entité, atteinte à la personnalité ;
- le boom du télétravail, notamment consécutif à la pandémie de COVID-19 implique de nouveaux outils qui suscitent des interrogations au niveau de leur sécurité.

Dans le contexte actuel de risques et de menaces accrus, auquel s'ajoute celui des difficultés d'application de la législation sur la protection des données, la Cour a jugé opportun de réaliser un état des lieux en matière de protection des données afin de vérifier que ce droit fondamental des citoyen·ne·s est respecté dans le cadre des actions publiques. Pour cet audit consacré à ce thème, la Cour a choisi de centrer son analyse sur la principale collectivité publique vaudoise, soit l'Administration cantonale.

OBJECTIF ET PÉRIMÈTRE DE L'AUDIT

L'audit a pour objectif de répondre à la question suivante :

La protection et la sécurité des données personnelles sont-elles assurées dans un contexte de développement du télétravail à l'ACV ?

L'approche d'audit consiste en l'examen des conditions cadres permettant l'application de la LPrD et des bonnes pratiques de sécurité :

- cadre des responsabilités défini et connu des différentes parties ;
- connaissances suffisantes des collaborateur·trice·s ;
- mesures de sécurité physiques et numériques adéquates ;
- organisation des systèmes d'information et processus de gestion des données adaptés et documentés ;
- dispositif de contrôle de l'application de la législation efficace ;
- cadre légal autorisant le traitement et la communication des données personnelles.

Pour ce faire, la Cour a analysé la situation prévalant dans huit entités-métiers, que l'on peut regrouper en deux catégories :

1. les entités « services » qui bénéficient d'une certaine autonomie ou gèrent une diversité importante de données personnelles : la Direction générale de l'enseignement obligatoire (DGEO), le Service des automobiles et de la navigation (SAN), l'Office du médecin cantonal (OMC), la Direction de l'insertion et des solidarités (DIRIS) et le Service de l'éducation physique et du sport (SEPS) ;
2. les entités « offices » qui dépendent d'une entité supérieure ou gèrent un nombre restreint de données personnelles différentes : l'Office de psychologie scolaire (OPS), l'Office cantonal des bourses d'études et d'apprentissage (OCBE), la Direction finances et affaire juridiques de la direction générale de la santé (DFAJ).

Des cas concrets de traitement de données personnelles par ces entités ont fait l'objet d'un examen sommaire. C'est à la lumière des constats établis dans les entités-métiers, qu'ont ensuite été analysées les conditions cadres mises en place par les trois entités transversales compétentes en matière de protection et sécurité des données (ci-après les entités-cadres) : l'Autorité de protection des données et de droit à l'information (APDI), la Direction générale du numérique et des systèmes d'information (DGNSI) et le Service du personnel de l'Etat de Vaud (SPEV). L'audit a été centré sur les données à protéger spécifiquement soit les données personnelles sensibles et les profils de personnalité.

La LPrD définit les données personnelles sensibles comme celles ayant trait aux opinions ou activités religieuses, philosophiques, politiques ou syndicales, ainsi qu'à une origine ethnique, à la sphère intime de la personne, en particulier à son état psychique, mental ou physique, aux mesures et aides individuelles découlant des législations sociales, aux poursuites ou sanctions pénales et administratives. Les profils de personnalité sont des assemblages de données qui permettent d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique (art. 4 al. 1 chiffres 2 et 3 LPrD).

LES PRINCIPAUX CONSTATS

1. LES ENTITÉS-MÉTIERS

Déficit d'analyse des données personnelles traitées

Le cadre légal et réglementaire assigne la responsabilité principale de la mise en œuvre des dispositions en matière de protection des données au responsable du traitement, à savoir l'entité-métier. Elle doit tout d'abord disposer d'une connaissance complète et précise des données personnelles traitées et de leurs flux. Une fois cet état des lieux réalisé, elle doit adopter des mesures pour respecter les principes de la législation.

L'examen réalisé auprès des huit entités-métiers auditées a révélé des situations inégales à cet égard.

Parmi les cinq entités « services », en charge de plusieurs activités :

- Certaines n'ont entamé aucune analyse pour identifier et catégoriser toutes les données personnelles traitées. Elles accumulent souvent les données sans les trier ni les anonymiser et n'ont pas entrepris de réflexion sur le besoin d'adopter des mesures de sécurisation particulière. Les démarches d'application des principes de protection des données relèvent de l'exception et sont notamment réalisées dans le cadre d'un changement d'applicatif informatique.
- D'autres ont intégré quelques principes de protection des données et mis en œuvre certaines mesures, mais de manière plutôt réactive et au coup par coup. Certaines directives ont été émises, mais elles ne couvrent pas l'ensemble des activités.

Parmi les trois entités « offices » gérant un nombre plus restreint d'activités :

- Certaines disposent, ou sont en voie de le faire, d'une application informatique intégrant des principes de protection des données, tels que la gestion segmentée des accès.
- Une seule entité, gérant un nombre limité d'applications, applique des mesures adéquates (anonymisation des données, gestion des accès, etc.).

Certaines entités n'ont pas complété le registre des fichiers requis par la LPrD depuis 2008 et géré par l'APDI. Aucune n'a poursuivi la démarche permettant d'avoir une vision exhaustive et documentée de toutes les données personnelles traitées et des mesures appliquées afin de se conformer à la LPrD. Les réflexions relatives au principe de conservation font particulièrement défaut, les données personnelles étant généralement stockées indéfiniment.

Sous-traitance et délégation de tâches insuffisamment cadrées

Dans les entités « services », il n'existe pas de politique de protection des données visant un traitement uniforme et conforme des données personnelles. En cas de délégation d'une tâche publique impliquant la communication de données personnelles, aucune mesure n'est adoptée pour contrôler la bonne application de la LPrD par les délégataires. Les conventions ou contrats sont souvent incomplets.

Si les entités « offices » ont adopté des mesures généralement plus appropriées en matière de protection des données, elles n'ont toutefois pas reçu d'instruction à ce sujet de la part de leur hiérarchie, signifiant que cette dernière n'a, à l'instar des entités « services » auditées, pas non plus adopté de politique adéquate y relative.

Exemples de lacunes constatées

L'examen d'applications ou d'activités impliquant le traitement de données personnelles a révélé des manquements dans l'application de la LPrD par les entités-métiers auditées sur des points précis :

- gestion des accès insuffisamment contrôlée pour une application informatique contenant des données personnelles sensibles ;
- clauses contractuelles insuffisantes en cas de sous-traitance ou de délégation de traitement de données : risques d'hébergement de données sensibles à l'étranger (non soumis au droit suisse) et absence de mention sur la nécessité de respecter la LPrD ;
- cas de violation de la confidentialité des données par des collaborateur·trice·s ACV (accès et consultation de fichiers contenant des données sensibles à des fins personnelles) ;
- application informatique traitant de données sensibles non gérée par la DGNSI, cette dernière ne pouvant donc pas surveiller son niveau de sécurité ;
- absence de traçabilité de l'accord donné par les représentants légaux (accord oral) pour transmettre des données sensibles relatives à des enfants mineurs à d'autres entités de l'ACV ;
- communication régulière par une entité d'adresses courriels de collaborateur·trice·s à des partenaires externes à l'ACV, sans accord ni analyse des risques de cette pratique.

Méconnaissance des dispositions LPrD et des règles de sécurité

Les lacunes constatées dans l'application de la LPrD et le manque d'implication des entités-métiers pour conformer leurs processus métier à ses dispositions témoignent tout d'abord d'un déficit de connaissances des collaborateur·trice·s en la matière, et ce, quel que soit leur niveau hiérarchique. Les représentant·e·s des entités auditées ont d'ailleurs été unanimes à le reconnaître. Seule une minorité a déclaré disposer d'un·e collaborateur·trice formé·e dans ce domaine.

Le personnel de l'ACV n'est pas non plus suffisamment formé et sensibilisé sur les bonnes pratiques de sécurité informatique. Les tests de faux phishing via courriels (hameçonnage) réalisés par le DGNSI ont montré que le besoin de formation et d'information est encore important dans ce domaine.

En outre, si le cadre des responsabilités en matière de protection des données est bien défini par la LPrD, il est généralement méconnu des entités-métiers, comme en témoigne l'absence de politique et de cadre concret défini en matière de protection des données.

Les entités-métiers ne sont pas non plus conscientes de leur responsabilité en matière de sécurité informatique. Elles doivent définir leurs besoins avant d'en faire part à la DGNSI conformément au Règlement sur l'informatique cantonale (RIC). Plusieurs d'entre elles auraient besoin d'outils ou de mesures de sécurité spécifiques, par exemple pour échanger des messages avec l'extérieur ou pour journaliser les opérations réalisées. Mais elles n'ont jamais exprimé ces besoins.

Culture du secret de fonction et du secret professionnel bien ancrée

Si les dispositions en matière de protection des données sont souvent méconnues, il faut néanmoins relever que le personnel est généralement rompu aux questions de confidentialité des informations traitées dans le cadre professionnel. Ces dernières sont en effet couvertes par le secret de fonction, notion qui, même si elle mériterait d'être mieux définie par chaque entité, est bien connue. Le secret professionnel, qui comprend le secret médical, est quant à lui bien intégré par le personnel concerné.

LES PRINCIPAUX CONSTATS

2. LES ENTITÉS-CADRES

Les lacunes en matière de respect des dispositions relatives à la législation sur la protection des données et des règles de bonnes pratiques sécuritaires proviennent essentiellement du manque de connaissance du personnel des entités-métiers dans ces domaines. Elles révèlent en outre l'insuffisance des conditions cadres nécessaires à leur mise en œuvre par les entités-métiers.

APDI : haut niveau d'expertise juridique mais activité de surveillance insuffisante

Le spectre des missions de l'APDI est très large (surveillance, promotion, conseil, traitement des recours, examen des projets de loi, etc.), tout comme celui des entités sous sa surveillance (l'ACV, les communes et toutes les entités auxquelles le canton et les communes délèguent une tâche publique).

La Cour constate que l'APDI bénéficie d'excellentes compétences juridiques. Elle relève sa disponibilité et son efficacité pour conseiller les entités qui sont généralement dépourvues de compétences en interne. Ce constat est partagé tant par les entités-métiers que par les autres entités-cadres auditées.

La Cour estime néanmoins que treize ans après l'entrée en vigueur de la LPrD, l'APDI doit renforcer sa mission de surveillance, qui représente moins de 2% de son activité depuis 2009, alors qu'elle en consacre près des deux tiers aux tâches de conseil et de promotion de la LPrD. La Cour relève également que l'absence de compétences pointues en matière informatique à l'APDI est problématique, les questions techniques étant de plus en plus centrales en matière de protection des données.

La Cour relève en outre que l'APDI n'est pas systématiquement informée en cas de violation de la sécurité des données personnelles. Cette situation ne lui permet pas de remplir pleinement son rôle de surveillance qui nécessite de cibler les actions sur les problèmes existants.

DGNSI : politique de sécurité en cours d'implémentation

Le point fort du dispositif de protection des données à l'ACV est le système de sécurité informatique mis en œuvre par la DGNSI. Toutefois l'intégration des enjeux de protection et de sécurité des données est relativement récente : c'est depuis 2011 qu'un important travail de rattrapage a été effectué. La politique générale de sécurité informatique mise en place est en voie de certification ISO 27001 et présente un bon niveau de sécurité selon des audits réalisés, notamment par le Contrôle cantonal des finances (CCF). La Cour recommande toutefois des améliorations ainsi que la poursuite des mesures menant à la certification ISO.

La DGNSI a bien intégré les principes de protection des données dans le cadre de la gestion des projets de renouvellement des applicatifs. Mais d'autres outils demandent à être adaptés. Le modèle du schéma directeur métier ne comporte en effet pas d'étape spécifique relative à la protection des données. De même, les contrats-types ne comprennent pas toutes les clauses requises.

Des outils de connexion à distance garantissant un bon niveau de sécurité ont été mis à disposition du personnel en télétravail. La Cour note toutefois que certaines pratiques autorisées peuvent présenter des risques : utilisation non cadrée de périphériques de stockage privés, possibilité d'imprimer sur n'importe quelle imprimante interne à l'Etat, sauvegarde dans le cloud de pièces jointes contenant des données personnelles professionnelles reçues sur un smartphone privé, etc.

La DGNSI met à disposition des tutoriels et effectue des campagnes de sensibilisation des collaborateur·trice·s. Courant 2021 elle a redoublé d'efforts en la matière (information via la Gazette, campagne de faux phishing, etc.), mais le niveau de connaissance du personnel est toutefois toujours insuffisant, comme en témoignent les tests réalisés par la DGNSI elle-même. La Cour relève qu'il manque en outre une liste exhaustive et centralisée de bonnes pratiques à appliquer par le personnel de l'ACV.

SPEV : directive obsolète sur les règles de sécurité à respecter par le personnel

Dans les domaines de la protection et de la sécurité des données, le SPEV est uniquement responsable des clauses y relatives figurant dans le cadre normatif lié au personnel de l'ACV. Il a en particulier émis la directive LPers 50.1 sur l'utilisation d'Internet, de la messagerie électronique, de la téléphonie et du poste de travail. Cette directive, qui contient les devoirs du personnel de l'ACV en matière de sécurité informatique et qui date des années 2000, n'est cependant ni complète, ni à jour. Elle nécessite une révision et devra être liée avec la liste des bonnes pratiques à établir par la DGNSI.

En charge des dispositions encadrant le télétravail, le SPEV a émis une directive sur les obligations du personnel y relative (directive DT 48.8). La première version de la directive en vigueur jusqu'à fin 2020 contenait des ambiguïtés sur la notion de responsabilité de la protection des données s'appliquant en télétravail et ne détaillait pas les exigences principales en matière de sécurité. La nouvelle version, entrée en vigueur durant l'exécution de l'audit a cependant clarifié ces notions et a été complétée.

LES PRINCIPAUX CONSTATS

3. LE CADRE LÉGAL

Conformité du cadre légal des activités métiers insuffisamment examinée

Le principe de la légalité est un des piliers de la législation sur la protection des données. La LPrD offre plusieurs alternatives : soit il existe un article de loi autorisant le traitement de données personnelles (et/ou personnelles et sensibles), soit le traitement est jugé nécessaire à l'accomplissement d'une tâche publique. Dans le cas de données sensibles, la LPrD exige que la collecte soit absolument nécessaire à l'accomplissement d'une tâche clairement définie dans une loi.

Si la première option, soit l'existence d'une base légale formelle, est idéale, la seconde demande une démarche analytique afin de définir les notions de « nécessaire » et « absolument nécessaire », ce qui implique de bien connaître la tâche publique en question et peut laisser place à une marge d'interprétation.

Les lois postérieures à la LPrD contiennent bien des clauses relatives au traitement des données personnelles, mais tel n'est pas le cas des lois antérieures. Compte tenu du fait que le Tribunal fédéral se montre plutôt exigeant en matière de base légale formelle un examen global de la conformité des traitements de données réalisés à l'ACV est nécessaire pour, le cas échéant, adapter les lois s'appliquant aux entités-métiers.

Base légale lacunaire pour traiter les données personnelles à des fins policières

La LPrD exclut de son périmètre les données traitées dans le cadre des procédures civiles, pénales et administratives (art. 3 al. 2 lettre b LPrD). Or le traitement des données à des fins policières dans les Etats signataires des Accords Schengen dont la Suisse fait partie, doit être régi par une transposition en droit interne de la directive (UE) 2016/680. Si la Confédération a procédé à cette transposition, tel n'est pas le cas du canton de Vaud, dont la législation est donc lacunaire.

LES CONCLUSIONS

Le secret de fonction et la sécurité informatique assurent une certaine protection…

La culture du secret de fonction, largement répandue parmi le personnel de l'ACV, ainsi que les mesures de sécurité informatique mises en place par la DGNSI permettent d'assurer un certain niveau de protection des données personnelles des administré·e·s traitées à l'ACV. Les principes de confidentialité et de sécurité sont ainsi en partie pris en compte dans le dispositif de protection en place.

… insuffisante toutefois en regard des exigences de la LPrD

Cette couche de protection présente toutefois des failles dues essentiellement à la méconnaissance des employé·e·s de l'ACV des dispositions sur la protection des données et des bonnes pratiques en matière de sécurité, ainsi qu'au manque d'implication des entités-métiers pour les faire appliquer. Même s'ils sont rares et jusqu'ici de peu d'ampleur, des cas de fuites de données se sont déjà produits à l'ACV. Si les principes de confidentialité et de sécurité sont des piliers importants de la protection des données, ils ne suffisent toutefois pas à assurer le respect de tous ses impératifs.

Les entités-métiers n'ont pas adopté de politique de gestion des données personnelles adéquate et adaptée à leurs activités permettant de minimiser les risques. Les données personnelles traitées sont insuffisamment tracées et maîtrisées, étant généralement dispersées et duplifiées dans plusieurs applications, fichiers ou supports qui n'ont pas fait l'objet d'analyse de besoin de sécurisation spécifique. Les données sont gérées essentiellement, voire uniquement en fonction des besoins du métier, sans tenir compte des exigences en matière de protection des données.

Aussi sécuritaire soit-il dans son architecture, tout système informatique présente des vulnérabilités face à des cyberattaques ou d'autres actes illicites internes ou externes pouvant générer des fuites de données ou leur destruction ou altération. Si de tels cas se produisent, les dégâts sont bien plus importants lorsque les données ne sont pas gérées selon les principes de la LPrD et sont par exemple conservées au-delà de période d'utilité ou n'ont pas fait l'objet de mesures de sécurisation nécessaire (anonymisation, pseudonymisation, gestion des accès, etc.).

Le dispositif de contrôle est lacunaire

Au déficit de gestion par les entités-métiers, s'ajoute un dispositif de contrôle insuffisant. L'APDI consacre une partie marginale de son activité à la surveillance des entités soumises à la LPrD. Ces dernières sont donc peu incitées à entreprendre des démarches pour se conformer à ces dispositions.

Les entités responsables du traitement, qui gèrent déjà insuffisamment leurs propres données, n'opèrent pas non plus de contrôle adéquat en cas de sous-traitance de données personnelles ou de délégation de tâches publiques impliquant le traitement de telles données.

L'implication des entités-métiers est l'élément pivot de la mise en œuvre de la LPrD

L'amélioration de l'application des dispositions de la LPrD passe par le renforcement des conditions cadres favorisant une réelle implication des entités-métiers dans la mise en œuvre de la protection des données dont elles ont la responsabilité. Cette démarche, qui doit émaner de la base, est indispensable pour compléter les mesures de sécurisation informatique adoptées en amont par la DGNSI. Ce n'est en effet qu'à cette condition que l'accompagnement de la transition numérique prévue au programme de législature du Conseil d'Etat pourra être réalisée. Cet objectif ne peut en effet être atteint qu'avec l'adhésion des citoyen·ne·s, ce qui nécessite de gagner leur confiance dans les missions étatiques requérant le traitement de leurs données.

Une réelle prise en main par les entités-métiers de la gestion des données personnelles traitées selon les principes de la LPrD contribuera en outre à poser les jalons d'une véritable politique de la donnée que l'ACV ambitionne d'élaborer. Celle-ci se doit en effet d'être cohérente dans toute l'ACV et garantir le droit à la protection des données des citoyen·ne·s que leur confère la Constitution.

LES RECOMMANDATIONS

Sur la base des constats et des conclusions d'audit, la Cour a émis 20 recommandations visant à ancrer une véritable culture de la protection des données à l'ACV.

- 13 recommandations visent l'amélioration des conditions cadres et s'adressent :
  - Au Conseil d'Etat qui les accepte toutes :
    - Instituer la fonction de délégué·e 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 :
    - 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).
  - A l'ensemble des entités-métiers auditées qui l'acceptent :
    - Documenter les données personnelles gérées et leurs mesures de protection.
- 7 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.