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

Rapport N°74

du 23.12.2021

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

Illustration de couverture © Darwin Laganzon de Pixabay

TABLE DES MATIÈRES

1. INTRODUCTION

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

La thématique de la protection des données suscite des questions nombreuses et complexes. Elle concerne les pouvoirs publics qui collectent bon nombre de données personnelles relatives à leurs administré·e·s. Quelles données sont-ils en droit de collecter ? Quel usage peuvent-ils en faire ? Sont-ils en droit de les transmettre ? Et si oui, à qui ? La confidentialité et la sécurité des données personnelles traitées sont-elles assurées ?

Droit fondamental reconnu depuis près de 70 ans

Bien que n'occupant l'actualité que depuis peu, la protection des données n'est pas un concept nouveau : c'est en effet en 1953 que la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH) a été édictée. Ratifiée par la Suisse en 1974, la CEDH ancre les principes du droit au respect de la vie privée et familiale (art. 8) pour la première fois dans un traité international. La déclinaison de ces principes figure dans la Convention STE n°108[1] (ci-après « Convention 108 ») adoptée par le Conseil de l'Europe en 1981. Cette Convention, à caractère obligatoire, a été ratifiée par 55 Etats, dont la Suisse en 1997. Elle a fait l'objet d'une révision complète et son protocole d'amendement (STE 223) a été adopté le 18 mai 2018.

Au plan constitutionnel, la protection de la sphère privée a été inscrite comme droit fondamental dans la Constitution fédérale de la Confédération suisse du 18 avril 1999 et dans la Constitution du Canton de Vaud du 14 avril 2003. La liberté personnelle avait déjà été reconnue comme un droit constitutionnel non-écrit par le Tribunal fédéral en 1963[2].

La loi fédérale sur la protection des données (LPD), qui s'applique tant à l'administration fédérale qu'au secteur privé, a été adoptée en 1992. Ce n'est que plus tardivement, soit en 2007, que le Canton de Vaud a légiféré sur la base de la Convention 108, avec la loi sur la protection des données personnelles (LPrD), dont les dispositions s'appliquent aux administrations cantonale et communales, ainsi qu'aux entités délégataires d'une tâche publique.

Cadre international contraignant et évolutif

La Convention 108 révisée, communément appelée Convention 108+, le nouveau règlement général européen sur la protection des données (RGPD)[3] et la Directive Justice-Police[4] avec lesquels le droit suisse doit assurer une compatibilité adéquate en vertu des accords de Schengen, ont sensiblement renforcé les principes de protection des données.

[1] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, conclue à Strasbourg le 28 janvier 1981 ; entrée en vigueur pour la Suisse le 1er février 1998. Série des traités européens N°108.
[2] ATF 89 I 92.
[3] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.
[4] Directive (EU) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

La loi fédérale vient d'être entièrement révisée dans ce sens le 25 septembre 2020 et devrait entrer en vigueur en principe le 1er janvier 2023 (nLPD). Un projet de refonte de la loi vaudoise est en cours, avec un renforcement probable de ces mêmes principes.

Objectifs de protection de la personnalité et de maîtrise de ses propres données

Les dispositions sur la protection des données, telles que figurant dans la loi vaudoise actuellement en vigueur, visent à prévenir le traitement abusif des données relatives aux personnes et à protéger leur personnalité ainsi que leur sphère privée. Elles concrétisent en outre le droit à l'autodétermination informationnelle, qui permet à tout individu de maîtriser ses données personnelles. Cela implique que les collectivités publiques qui détiennent des informations, doivent être en mesure de garantir leur accès à toute personne qui en formule la demande.

Parmi les autres éléments-clés des dispositions, figure l'institution d'un·e préposé·e à la protection des données, autorité indépendante chargée de la surveillance de l'application et de la promotion de la loi. Elle a également pour mission de recenser tous les fichiers contenant des données personnelles (le « registre des fichiers », dans la loi vaudoise).

Cette loi reprend également la distinction communément admise entre deux types de données personnelles : les données personnelles sensibles et les profils de personnalité d'une part, et les données personnelles non sensibles d'autre part. Celles de la première catégorie doivent bénéficier de mesures de protection renforcées.

Des principes complexes à appliquer

Tout traitement de données personnelles doit respecter les principes de légalité, de finalité, de proportionnalité, de transparence, d'exactitude, de sécurité, de conservation et de consentement[5]. Si, au plan théorique, les principes de la protection des données sont relativement simples à appréhender, leur application est plus complexe. Elle demande en effet un cadre bien défini, une très bonne connaissance de ces principes par les collaborateur·trice·s qui l'appliquent, ainsi qu'une maîtrise des besoins du domaine métier concerné.

Risques accrus générés par les nouvelles technologies et le télétravail

Avec le développement des nouvelles technologies, la problématique de la protection des données a encore acquis une nouvelle dimension, s'ajoutant à la complexité du domaine. Le volet de la sécurité des données y occupe en effet désormais une place prépondérante. A l'époque du « tout papier », il suffisait aux pouvoirs publics de disposer de locaux sécurisés et fermés à clé avec des fonctionnaires rompus au secret de fonction, pour assurer une sécurité des données suffisante. De nos jours, avec la numérisation et la dématérialisation des données[6], ce n'est qu'avec un arsenal de mesures techniques et de cyber-compétences que les informations personnelles des administré·e·s peuvent être protégées contre les diverses menaces qui les touchent. Parmi ces dernières, figurent les tentatives de cyberattaques ciblant de plus en plus les systèmes informatiques des collectivités publiques.

[5] Ces principes seront explicités au chapitre 3.1.2.

[6] La numérisation est la transformation d'un document physique en copie numérique. Elle fait partie des actions de gestion électronique de documents (GED). Tandis que la dématérialisation est un processus complet de transformation digitale qui permet de produire un document directement au format numérique, à partir d'un système d'information.

Le basculement forcé de l'ensemble des collaborateur·trice·s de l'Etat de Vaud en télétravail, suite aux mesures de lutte contre la pandémie de COVID-19 dès mars 2020, a multiplié les questions liées à la protection et la sécurité des données, amenant la Cour des comptes à s'intéresser à cette thématique. A ces interrogations, s'ajoutent les constats posés lors de précédents audits de la Cour. Des manquements en matière de protection des données avaient en effet été pointés dans l'audit sur le contrôle des habitants (N°33, 2015) ainsi que dans celui sur l'Office cantonal d'orientation scolaire et pédagogique (N°57, 2019).

La Cour a donc estimé le moment opportun pour lancer un audit centré sur l'application des dispositions en matière de protection des données. Dans ce contexte, il est en effet apparu nécessaire de vérifier que ce droit fondamental des citoyen·ne·s garanti par la Constitution est assuré et respecté dans le cadre de toute action de l'Etat.

2. DESCRIPTIF ET APPROCHE DE L'AUDIT

2.1 OBJECTIF, AXES ET CRITÈRES D'AUDIT

L'audit réalisé 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'audit comprend ainsi deux axes, la protection et la sécurité des données :

Axe 1 – Concernant *la protection des données*, les critères d'audit se réfèrent donc aux dispositions de la LPrD et à son contexte légal complexe. L'audit cible prioritairement les conditions cadres permettant d'assurer le respect de ces dispositions et par là, à en vérifier l'existence et l'adéquation (formation, information, organisation et documentation des processus, dispositif de contrôle). L'audit examine également les mesures entreprises par les entités-métiers[7] pour se conformer aux principes de base requis par cette législation[8].

Axe 2 – Quant à *la sécurité des données*, bien que faisant partie intégrante des principes de la LPrD, il forme un axe d'audit séparé, en tant que volet sécurité informatique, principal aspect de sécurité traité dans cet audit[9]. Néanmoins, il est important de préciser ici que la Cour n'a pas procédé à un audit informatique en tant que tel. Cet audit, centré sur la protection des données, se limite à vérifier si des mesures techniques et organisationnelles correspondant aux bonnes pratiques de sécurité ont été mises en œuvre, sans auditer leur qualité technique.

Au niveau de l'organisation et des rôles et responsabilités en matière de sécurité (sur le site et en télétravail), l'analyse a été réalisée sur la base :

- des dispositions du Règlement relatif à l'informatique cantonale (RIC) ;
- de la directive DT 48.8 sur le télétravail, émise par le Service du personnel pour ce qui relève de la sécurité des données en télétravail ;
- et de la législation sur le personnel de l'Etat de Vaud, pour les aspects de formation.

[7] Pour cet audit, on considère les « entités-métiers » et non les « services-métiers ». En effet selon la LPrD, le responsable du traitement n'est pas forcément le service, soit l'unité administrative qui fait office d'autorité d'engagement ou d'unité budgétaire. Il peut s'agir d'une entité plus petite.

[8] Il a été tenu compte indirectement de la révision de la LPrD en cours. Il est en effet d'autant plus nécessaire de respecter les dispositions actuelles, que celles-ci seront probablement amenées à se renforcer en s'alignant sur le cadre légal fédéral et européen.

[9] Comme le précise le message concernant la révision totale de la loi fédérale sur la protection des données du 15 septembre 2017 : « *Il existe une interaction entre la protection des données et leur sécurité, mais ces deux aspects doivent être traités séparément. La protection des données relève de la protection de la personnalité de l'individu. Quant à la sécurité des données, elle vise généralement les données présentes chez un responsable du traitement ou chez un sous-traitant et englobe le cadre organisationnel et technique général du traitement des données. Par conséquent, la protection de l'individu n'est possible que si des mesures techniques générales ont été prises pour la sécurité des données le concernant. D'où la distinction opérée … »*

2.2 APPROCHE DE L'AUDIT

La Cour s'est saisie elle-même du sujet de l'audit et a conduit ses travaux conformément à sa méthodologie, à sa Charte éthique et son Code de déontologie. L'audit a été réalisé conformément aux normes internationales sur les audits de performance établies par l'Organisation Internationale des Institutions Supérieures de Contrôle des Finances Publiques (INTOSAI).

Pour cet audit, une double approche est choisie, la première étant la principale :

- Une approche *système* (ou indirecte) pour l'examen des conditions cadres permettant d'assurer le respect des principes des dispositions sur la protection des données.
- Une approche *résultats* (ou directe) pour l'examen de la mise en œuvre de l'application de la LPrD (et respect du secret de fonction) dans une sélection de services ou entités de l'ACV.

Des éléments de conformité ont également été étudiés dans le cadre de l'approche *résultats*.

En optant pour un périmètre d'audit large, transversal à toute l'administration et en ciblant l'approche *système* avec l'examen des conditions cadres pour principal volet, l'objectif était également d'éviter d'axer l'analyse sous un angle exclusivement juridique, domaine qui relève de la compétence de l' Autorité de protection des données. En effet, c'est cette dernière qui est habilitée, de par la LPrD, à réaliser des audits détaillés portant sur des entités spécifiques et à émettre des recommandations en cas de constats de non-conformités.

2.3 LES ENTITÉS AUDITÉES

Trois entités-cadres

Les entités auditées pour l'examen des conditions cadres, sont trois entités transversales de l'Administration cantonale vaudoise (ACV) :

Entité		Aspects audités
APDI	Autorité de protection des données et de droit à l'information	LPrD
DGNSI	Direction générale de l'informatique et du numérique	Sécurité informatique
SPEV	Service du personnel de l'Etat de Vaud	Télétravail et formation du personnel

A noter que l'audit étant principalement centré sur les données numériques, les archives cantonales dont les dispositions, selon la loi vaudoise sur les archives (LArch), s'appliquent pour l'heure essentiellement aux données papier, n'ont pas été incluses.

Huit entités-métiers

A ces trois entités transversales ont été adjoints huit services[10] dans le but de vérifier l'application des principes de protection et sécurité des données. Ces entités-métiers ont été sélectionnées sur la base des critères suivants : elles traitent de données personnelles sensibles ; elles sont de tailles différentes ; certaines ont déclaré leurs fichiers au Registre des fichiers tenu par l'APDI, d'autres non ; plusieurs départements sont représentés ; elles gèrent des données personnelles numérisées.

Entité-métier		Département	Applications numériques	Registre des fichiers	Nbre de collab.	ETP
DGEO	Direction générale de l'enseignement obligatoire (Etat-major et administration)	DFJC Formation, jeunesse et culture	• *LAGAPEO données personnelles de l'élève et données relatives à la scolarisation de l'élève*	Oui	1186	661
OPS[11]	Office de psychologie scolaire	DFJC Formation, jeunesse et culture	• *Dossier de l'enfant suivi par un psychologue, psychomotricien ou logopédiste en milieu scolaire*	Oui	280	190
SAN	Service des automobiles et de la navigation	DIT Institutions et territoire	• *Application Viacar (conducteurs-véhicules-sanctions)* • *Gestion électronique des documents (GED) des données Viacar*	Oui	241	217.4
DIRIS	Direction de l'insertion et des solidarités	DSAS Santé et action sociale	• *Fichier FORJAD (formation pour les jeunes en difficulté)*	Non	106	73.9
OMC	Office du médecin cantonal	DSAS Santé et action sociale	• *Plateforme de gestion des traitements agonistes opioïdes* • *Autorisations d'exploiter et de pratiquer (Progrès)*	Oui	42	23.6
OCBE	Office cantonal des bourses d'études et d'apprentissage	DSAS Santé et action sociale	• *Fichiers des bénéficiaires de bourses d'étude*	Non	30	19.1
DFAJ	Direction des finances et des affaires juridiques	DSAS Santé et action sociale	• *Cliniques privées VD - Bordereaux pour paiement de la part cantonale*	Oui	23	17.2
SEPS	Service d'éducation physique et des sports	DEIS Économie, innovation et sport	• *Préavis pour les élèves des classes spéciales (sport-études)*	Oui	22	19.8

Pour chaque entité, une ou deux applications informatiques ont été sélectionnées pour un examen plus approfondi.

[10] Dans ce document et pour en faciliter sa lecture, la dénomination « service » désigne toutes les entités de l'ACV telles que les directions, directions générales, services, offices, centres etc.

[11] Suite à une restructuration de la DGEO, l'Office de psychologie scolaire est devenu la Direction psychologie, psychomotricité, logopédie en milieu scolaire (DPPLS) dès le 1er août 2021.

2.4 PÉRIMÈTRE DE L'AUDIT

L'audit porte sur la protection des données dans l'Administration cantonale vaudoise (ACV), telle que définie par la loi vaudoise sur la protection des données (LPrD). Comme mentionné dans l'introduction, cette législation est complexe et comporte de multiples aspects. Le périmètre a donc été restreint aux éléments jugés comme prioritaires, particulièrement en regard des risques présentés par le télétravail, soit la protection des données des administré·e·s.

Protection des données des administré·e·s

L'analyse s'est tout d'abord concentrée sur la protection des données des administré·e·s, excluant la protection des données des collaborateur·trice·s en tant qu'employé·e·s de l'Etat, même si la LPrD s'applique également à leurs données. Ce thème constituerait en effet un sujet d'audit en soi, car il ne porte pas uniquement sur le cadre de la LPrD, mais aussi sur l'ensemble des dispositions régissant le personnel de l'Etat.

Focus sur les risques liés au télétravail et les données numériques

Du fait des risques importants liés au traitement et au transfert informatique des données, l'audit porte principalement sur la protection des données numériques.

Envisagé d'abord dans le contexte du développement du télétravail, l'audit s'est centré sur l'étude des risques liés au transport des données, à la connexion informatique à distance et au traitement des données à domicile. Les conditions de sécurité et de protection des données en télétravail ne pouvant être assurées que si elles le sont de manière générale et indépendamment du lieu de traitement des données, l'audit a également porté sur certains éléments généraux liés à la sécurité et la protection des données explicités ci-après.

Examen centré sur les conditions cadres assurant le respect des principes-clés de la LPrD

L'examen a porté sur les principes de la législation vaudoise sur la protection des données (LPrD), qui figurent dans le chapitre II section I de la loi, en se focalisant sur les conditions cadres. Parmi celles qui permettent d'assurer la bonne application des principes de protection des données, on peut citer :

- une désignation claire des responsabilités en matière de protection et de sécurité des données ainsi qu'une connaissance de ces dispositions par les différentes parties (entités-cadres, responsables d'entités, collaborateur·trice·s, etc.) ;
- une bonne connaissance des collaborateur·trice·s des principes de la LPrD, ainsi que des bonnes pratiques de sécurité informatique ;
- la mise en place de mesures de sécurité physiques et numériques ;
- l'organisation des systèmes d'information et le processus de gestion des données permettant d'identifier les données à protéger et d'assurer le respect de la LPrD ;
- la mise en place du dispositif de contrôle de l'application de la législation ;
- le cadre légal assurant la licéité du traitement et du transfert des données personnelles.

Principe de sécurité au cœur de l'analyse

Les principes de la législation sélectionnés pour l'analyse, sont ceux qui présentent à la fois le plus de risques, en lien notamment avec le télétravail, et dont le non-respect est susceptible de porter les préjudices les plus graves tant aux administré·e·s qu'à l'Etat : atteinte à la personnalité, dégât d'image ou perte financière. Des questions de faisabilité d'audit ont également pesé dans le choix des éléments analysés.

Le premier principe retenu est celui de la sécurité des données, incluant la confidentialité. Il vise à prévenir les risques de fuite, de vol, de perte, d'altération et de divulgation volontaire ou non de données personnelles. Ce principe est primordial, du fait de l'importance de la confidentialité des données traitées par l'ACV et des risques que sa violation implique : la dématérialisation rend en effet les données vulnérables à des cyberattaques, dont les conséquences peuvent être dévastatrices. De plus, le cercle des intervenant·e·s qui ont la mission d'assurer le respect de cette confidentialité est l'ensemble des collaborateur·trice·s qui y ont accès et est donc très large, ce qui multiplie d'autant les risques. Le principe de sécurité a également pour particularité qu'il doit être réévalué et adapté en tout temps.

Autres principes retenus

La question du respect des principes de légalité, finalité, proportionnalité, ainsi que de conservation des données personnelles traitées a également été abordée en particulier lors de l'examen des cas concrets dans les entités de l'ACV auditées.
A noter que les risques liés à ces principes se cumulent avec ceux liés à la sécurité : plus il y a de données, plus celles-ci sont conservées longtemps, plus les risques de sécurité augmentent.

Principes et aspects de la législation non examinés

Les principes de transparence, d'exactitude et de liberté du consentement n'ont pas été abordés, car leur examen aurait nécessité la collecte d'informations directement auprès d'administré·e·s, ce qui n'entrait pas dans le périmètre de l'audit. De même, l'accès des individus à leurs propres données détenues par l'ACV et la question des recours déposés en la matière n'ont pas été traités.

Ainsi, le registre des fichiers[12] géré par l'Autorité de protection des données n'a pas fait l'objet d'un examen spécifique donnant lieu à des recommandations générales, car il a pour objectif de faciliter cet accès.

Ainsi, la Cour a choisi de se concentrer sur la manière dont les services de l'administration organisent, documentent en interne et protègent les données personnelles qu'ils gèrent.

[12] En effet, l'objectif du Registre des fichiers tel que défini dans la loi actuelle est de renseigner les citoyen·ne·s sur les données traitées pour faciliter l'accès à leurs propres données. De plus, il est possible que ce Registre soit amené à être structuré de manière différente dans la nouvelle loi cantonale, à l'instar du RGPD et de la nLPD où cette notion disparaît pour faire place au « Registre des activités de traitement ». Cela nécessitera alors une description plus détaillée des différents traitements et flux de données. Il paraissait ainsi peu approprié de formuler des recommandations générales pour un outil amené à être modifié. Par contre dans le cadre de l'examen des cas concrets dans les entités-métiers, les lacunes constatées en matière d'annonce au Registre des fichiers actuel ont fait l'objet d'une recommandation.

Protection prioritaire des données personnelles sensibles

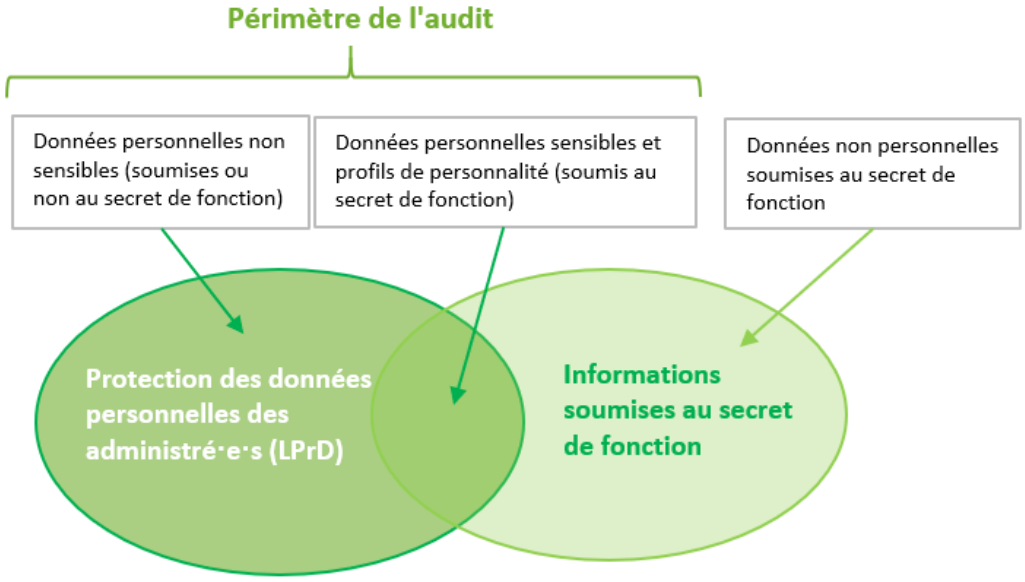
La législation sur la protection des données distingue deux types de données personnelles : les données personnelles sensibles et non sensibles. Les données personnelles sensibles sont celles qui se rapportent (art. 4 LPrD) :

- 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.

Selon la LPrD, les données personnelles sensibles, ainsi que les informations constituant un profil de la personnalité défini comme « *un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique* » (art. 4 LPrD) doivent bénéficier de mesures de protection renforcées. C'est pourquoi l'audit a également été centré sur la protection de ce type de données.

Secret de fonction intégré à la thématique

La notion de protection des données personnelles a également été envisagée sous l'angle des informations soumises au secret de fonction que tout·e employé·e de la fonction publique se doit de respecter et dont la définition sera développée au chapitre 3.



©Cour des comptes 2021

Les deux notions se recoupent en effet en partie, toutes les données personnelles sensibles, de même que les profils de personnalité ou toute donnée ou combinaison de données personnelles devant rester confidentielles étant soumis au secret de fonction.

En outre, les sanctions en cas de violation de la protection de données personnelles sensibles sont beaucoup plus sévères sous l'angle du secret de fonction (Code pénal) que de celui de la LPrD. C'est pourquoi cette notion a été intégrée à la thématique d'audit, le périmètre d'audit restant toutefois les données soumises à la LPrD.

2.5 COLLECTE D'INFORMATIONS

Collecte minimale réalisée auprès des entités-métiers

Les entretiens d'audit et la collecte d'information se sont déroulés entre septembre et décembre 2020, soit en pleine période de pandémie COVID-19. Cette dernière a généré une forte surcharge de travail dans de nombreux services de l'Etat, y compris parmi des entités auditées (notamment l'Office du Médecin Cantonal). C'est pourquoi l'équipe d'audit s'est efforcée de réduire la sollicitation des services au strict minimum, nécessitant tout de même l'organisation d'une voire deux séances par entité, ainsi que la collecte de documents.

De plus, la généralisation du télétravail a compliqué la tenue de séances en présentiel. Néanmoins, les séances d'audit ont été consacrées à l'examen des conditions mises en place pour assurer la protection et la sécurité des données d'une part et d'autre part, à l'examen des applications informatiques sélectionnées. Ce dernier n'a pu être que sommaire. Les constats et recommandations qui leur sont liés ne portent donc que sur les éléments analysés. Ils n'ont pas pour ambition de résulter d'une analyse exhaustive, telle que celle réalisée par l'APDI dans le cadre de ses audits.

Un questionnaire standard sur les conditions cadres (voir annexe I) a été adressé aux entités auditées quelques jours précédant l'entretien.

Plusieurs entretiens avec les entités-cadres

Quant aux entités-cadres, elles ont été sollicitées à divers degrés : deux entretiens ont suffi pour les questions liées au personnel et au télétravail. La question de la sécurité informatique a nécessité plusieurs sollicitations de la DGNSI, dont plusieurs demandes d'information auprès de spécialistes de la sécurité du numérique. Quant à l'APDI, deux séances et de nombreux contacts ont été nécessaires.

2.6 ORGANISATION DE L'AUDIT ET RAPPORT

L'équipe d'audit était composée de Mme Valérie Schwaar, magistrate responsable et de Mme Christina Maier, cheffe de mandat d'audit. La fonction de chef de mandat d'audit support a été assurée par M. Allister Keane, puis par M. Philippe Zahnd. L'équipe d'audit a été assistée par un expert spécialiste en protection des données.

L'audit a démarré par l'annonce officielle de l'audit consécutive à l'adoption de la stratégie d'audit le 23 septembre 2020.

Le projet de rapport a été adressé aux entités auditées afin qu'elles puissent formuler leurs observations durant le délai de consultation de 21 jours.

La Cour délibérant en séance plénière en date du 23 décembre 2021 a adopté le présent rapport public en présence de M. Guy-Philippe Bolay, président, et de Mmes Nathalie Jaquerod et Valérie Schwaar, vice-présidentes.

2.7 REMERCIEMENTS

La Cour des comptes tient à remercier toutes les personnes qui lui ont permis de réaliser cet audit. Elle souligne la disponibilité de ses interlocuteur·trice·s, la qualité des échanges de même que la diligence et le suivi mis à la préparation et à la fourniture des documents et des données requis.

Une synthèse de ce rapport et une capsule vidéo de présentation des travaux d'audit sont librement accessibles sur la page Internet de la Cour des comptes du canton de Vaud : www.vd.ch/cdc.

La Cour formule les réserves d'usage pour le cas où des documents, des éléments ou des faits ne lui auraient pas été communiqués, ou l'auraient été de manière incomplète ou inappropriée, éléments qui auraient pu avoir pour conséquence des constatations et/ou des recommandations inadéquates.

3. CADRE JURIDIQUE ET TECHNIQUE

Ce chapitre a pour but de développer les critères d'audit, basés sur :

- le cadre et le contexte juridique de la protection des données ;
- la définition de la notion de secret de fonction et de ses implications ;
- les grandes lignes des bonnes pratiques en matière de sécurité informatique.

3.1 PROTECTION DES DONNÉES PERSONNELLES

3.1.1 UN CONTEXTE JURIDIQUE COMPLEXE

Pour être en mesure de juger la performance de la mise en œuvre des exigences requises en matière de protection des données à l'ACV, il est important de bien comprendre les dispositions qui s'y appliquent et qui l'impactent, ainsi que d'appréhender leurs perspectives d'évolution.

Cette démarche implique d'identifier les éléments du contexte international, européen et suisse en matière de protection des données qui conditionnent directement ou indirectement celles qui s'appliquent au niveau de la législation vaudoise à laquelle l'ACV est soumise.

Ce cadre juridique, brièvement résumé dans l'introduction, est composé de plusieurs textes légaux dont les principaux[13] sont :

- la Convention de sauvegarde des droits de l'homme et des libertés fondamentales de 1953 ;
- la Convention 108 du Conseil de l'Europe de 1981 (et révisée en 2018) ;
- le Règlement européen sur la protection des données de 2016 ;
- la Constitution fédérale de 1999 ;
- la Constitution vaudoise de 2003 ;
- les lois fédérale (1992) et vaudoise (2007) sur la protection des données.

A noter que, comme dans tout domaine juridique, les lois doivent être interprétées à la lecture de la jurisprudence et la doctrine, les textes légaux ne fournissant pas toutes les réponses aux interrogations qui se posent.

3.1.2 CONTEXTE VAUDOIS

La Constitution du Canton de Vaud du 13 avril 2003 (BLV 101.01)

La Constitution du Canton de Vaud du 13 avril 2003 (BLV 101.01) contient un article relatif à la protection des données qui correspond à l'article de la Constitution fédérale sur la protection de la sphère privée (art. 13 Cst. CH). Il ajoute toutefois davantage de poids à la notion de protection des données en la citant nommément dans le titre de l'article (art. 15 Cst-VD).

De plus, l'article constitutionnel vaudois aborde le principe fondamental de la protection des données soit le droit à l'autodétermination informationnelle, qui est le droit des individus à disposer de leurs données personnelles et d'être protégés contre toute utilisation abusive.

[13] Afin de ne pas alourdir la lecture du rapport, les explications concernant le contexte international, européen et suisse figurent dans l'annexe II et le schéma illustrant l'historique de ces dispositions dans l'annexe III.

Les principes concrets qui en découlent et qui sont cités dans la Constitution vaudoise sont l'accès à ses données pour la personne concernée, l'exactitude et la conservation des données personnelles. Leur élévation au rang constitutionnel au titre de droit fondamental leur confère ainsi une portée d'emblée plus importante que s'ils étaient uniquement de niveau légal[14].

Protection de la sphère privée et des données personnelles (Art. 15 Cst-VD)

1. Toute personne a droit au respect et à la protection de sa vie privée et familiale, de son domicile, de sa correspondance et des relations établies par les télécommunications.

2. Toute personne a le droit d'être protégée contre l'utilisation abusive de données qui la concernent. Ce droit comprend :
a. la consultation de ces données ;
b. la rectification de celles qui sont inexactes ;
c. la destruction de celles qui sont inadéquates ou inutiles.

Loi sur les fichiers informatiques et la protection des données (LIPD)

En comparaison intercantonale, le Canton de Vaud a été parmi l'un des premiers à légiférer en matière de protection des données avec la loi sur les fichiers informatiques et la protection des données (LIPD) entrée en vigueur en 1981, peu après Genève (1976). La LIPD traitait des fichiers informatiques que l'Etat, les communes, les établissements et les corporations de droit public exploitaient directement ou par l'intermédiaire de tiers.

Cette loi ne correspondait toutefois pas à la Convention 108, qui prévoyait déjà l'instauration d'une autorité indépendante de surveillance et non une simple gestion interne à l'Etat, sans réel pouvoir de surveillance (par le Secrétariat général du Département des finances).

La LIPD comprenait cependant bon nombre de principes-clés de protection des données, comme le droit d'accès des individus aux données les concernant, la nécessité de disposer de bases légales pour traiter des données personnelles et les transférer entre entités étatiques.

Loi sur la protection des données personnelles (LPrD ; BLV 172.65)

Première loi vaudoise relativement tardive

C'est en 2008 qu'est entrée en vigueur la première loi vaudoise basée sur le modèle de la Convention 108. Dès lors, le périmètre d'application de la LPrD ne couvre pas uniquement les fichiers informatiques comme pour la LIPD, mais tout traitement de données personnelles quel que soit le support, y compris papier. Un chapitre entier est par ailleurs consacré à la vidéosurveillance.

Elargissement du champ des assujettis

Les entités soumises à la LPrD sont l'ACV, l'Ordre judiciaire et son administration, le Conseil d'Etat, le Grand Conseil, la Cour des comptes, les communes et les associations de communes, ainsi que les entités délégataires d'une tâche publique[15] (art. 2 al. 2 LPrD).

[14] La jurisprudence a fini par consacrer ces principes au rang constitutionnel, alors qu'ils ne sont pas cités dans la Constitution fédérale. Un arrêt du Tribunal fédéral de 2012 a en effet précisé : « Le *droit à l'autodétermination en matière de données personnelles est un droit constitutionnel qui garantit à chacun la maîtrise de ses données personnelles* » (ATF 138 II 346, 359 s.).
[15] Le spectre des assujettis est plus large que celui de la LIPD puisque, hors collectivités publiques au sens strict, il ne comprend plus seulement les établissements et corporations de droit public, mais toutes les entités délégataires d'une tâche publique.

De plus, la LPrD encadre le traitement des données par des sous-traitants en le conditionnant à une base légale ou à un contrat (art. 18 LPrD) et en leur conférant la responsabilité de la sécurité des données[16].

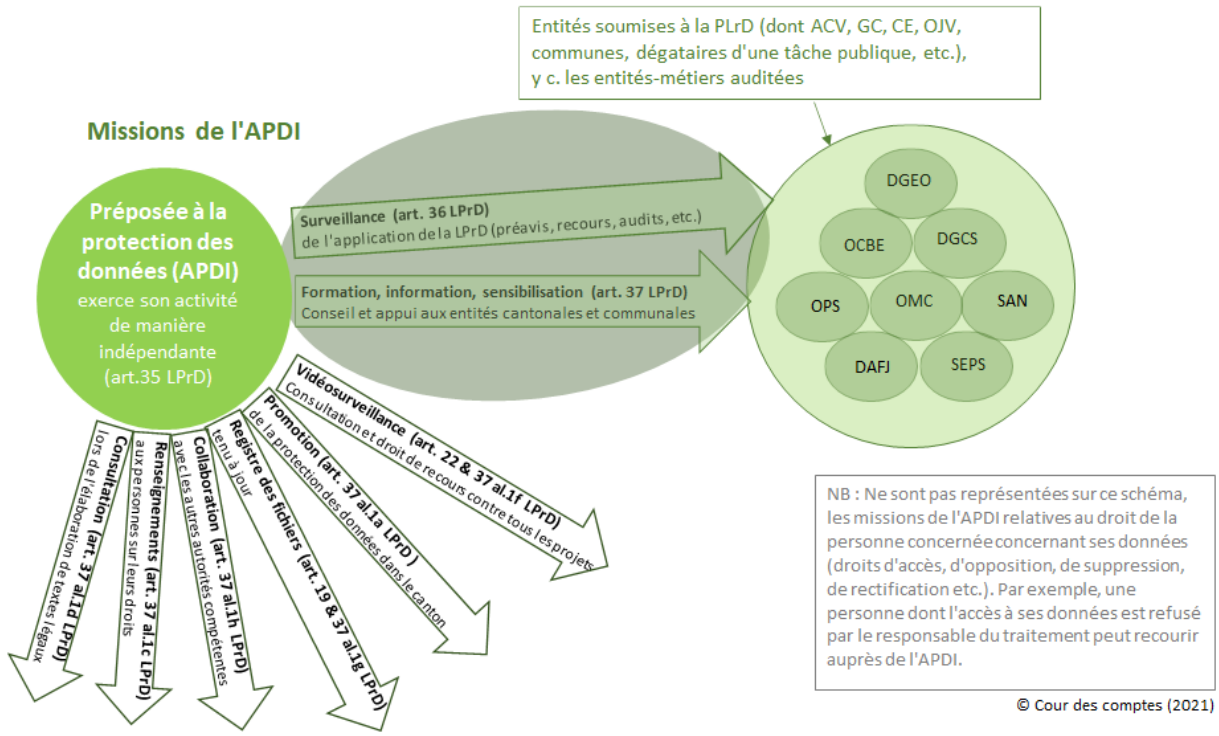
Notion de responsable du traitement précisée

Alors que la LIPD attribuait la responsabilité au service de l'Etat dans lequel les données étaient traitées, la LPrD a affiné la notion de responsable du traitement en la définissant comme la « *… personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine le contenu, ainsi que les finalités du fichier* » (art. 4 al. 1 chiffre 8). Cela signifie que le responsable du traitement n'est donc plus forcément le service ou la direction, mais peut être une entité qui lui est hiérarchiquement subordonnée dans la mesure où le contenu et la finalité du fichier sont définis par ses soins. Compte tenu des responsabilités qui lui sont attribuées, il est donc important d'identifier précisément qui est le responsable du traitement.

Changement culturel important avec l'instauration d'une autorité de surveillance

La grande nouveauté instaurée par la LPrD est la mise en place d'une autorité indépendante chargée de surveiller l'application de la loi.

Cette autorité, représentée par le·la préposé·e à la protection des données, est en effet non seulement habilitée à conseiller les entités soumises à la législation, mais également à y mener des investigations et audits et à leur formuler des recommandations. Elle est également instance de recours, par exemple dans le cadre de la procédure d'accès des personnes à leurs propres données (dès qu'une décision est rendue) et peut obliger les départements à prendre des mesures en cas de traitement illicite par un service.



[16] La formulation de la LPrD dans l'art. 18 al. 2 consacré au traitement des données par un tiers : « *Le tiers est responsable de la sécurité des données qu'il traite*», ne doit toutefois pas laisser conclure que le responsable du traitement est déchargé de toute responsabilité quant à la sécurité des données personnelles dont il a la charge et qui sont traitées par des sous-traitants ; il est tenu de s'assurer, notamment par contrat, que le sous-traitant sécurise les données confiées de manière adéquate dans le sens de la LPD « *Le responsable du traitement doit en particulier s'assurer que le sous-traitant est en mesure de garantir la sécurité des données* » (art 9 al. 2 LPD).

Autodétermination informationnelle renforcée

La LPrD renforce le dispositif, déjà existant sous la LIPD, permettant aux individus d'accéder à leurs données personnelles et d'en assurer la maîtrise. La notion d'autodétermination informationnelle y est déclinée conformément aux exigences de la Convention 108 et selon l'article 15 de la Constitution vaudoise. Elle comprend le droit d'accès des individus à leurs propres données, leur droit d'opposition ainsi que le droit d'exiger l'arrêt d'un éventuel traitement illicite des données. En cas de refus de l'autorité sollicitée, la possibilité de déposer un recours est prévue.

Cela implique que les responsables de traitement de données personnelles sont désormais tenus de structurer leurs systèmes d'information et de les sécuriser en fonction de ces nouvelles exigences.

Principes de la Convention 108 respectés

Tout comme la LPD fédérale, la LPrD reprend tous les éléments fondamentaux de la Convention 108 du Conseil de l'Europe, notamment les définitions et les principes de base qui forment le cœur de la protection des données[17] :

- **La légalité** (art. 5 LPrD) : Il s'agit du principe cardinal de la protection des données qui exige que le traitement des données personnelles, qui est une restriction de la sphère privée, soit autorisé par une base légale ou serve à l'accomplissement d'une tâche publique. Pour les données non sensibles, une base légale formelle ou matérielle est suffisante. En revanche, les conditions sont plus strictes pour le traitement de données personnelles sensibles qui doit être prévu par une loi formelle, être absolument exigé par l'accomplissement d'une tâche clairement définie dans une loi ou reposer sur le consentement de la personne concernée ou encore ne porter que sur des données qu'elle a rendues accessibles à tout un chacun (art. 5 al. 2 let. b LPrD).
- **La finalité** (art. 6 LPrD) : Les données ne peuvent être traitées que dans les buts figurant dans une loi ou annoncés lors de leur collecte. Il convient également d'être attentif à ce principe en cas de transfert à des tiers.
- **La proportionnalité** (art. 7 LPrD) : Ce principe impose de ne traiter que les données nécessaires et aptes à atteindre le but visé.
- **La transparence** (art. 8 LPrD) : Ce principe reconnaît le droit de la personne concernée à être informée du traitement des données la concernant. L'EMPL de 2007 relatif à la LPrD précise que les renseignements suivants doivent être fournis : entité responsable du traitement, finalité, destinataires, etc.
- **L'exactitude** (art. 9 LPrD) : Ce principe figurait déjà dans la LIPD. Il implique que les données traitées soient correctes et donne le droit à la personne concernée d'obtenir la correction ou la destruction des données inexactes.
- **La sécurité** (art. 10 LPrD) : Ce principe-clé concerne les mesures techniques et organisationnelles à mettre en place pour garantir la disponibilité, l'intégralité et la confidentialité des données traitées.

[17] Source : Exposé des motifs et projet de loi sur la protection des données personnelles, mars 2007

- **La conservation** (art. 11 LPrD) : C'est un aspect du principe de proportionnalité (temporelle). Les données ne doivent être conservées que tant qu'elles sont nécessaires au but de la collecte. Sinon elles doivent être détruites, ou anonymisées. La loi vaudoise sur les archives (LArch) demeure réservée, en particulier lorsqu'elle impose des obligations de conservation.
- **Le consentement** de la personne (art. 12 LPrD) : si un consentement est requis, il ne peut être valable que si la personne concernée s'est exprimée librement après avoir été dûment informée. De plus, si des données sensibles sont concernées, le consentement doit être explicite.

Le registre des fichiers : un outil destiné à garantir la transparence des données traitées

Dans le but d'assurer la transparence des traitements et de faciliter l'accès des individus à leurs propres données, la loi vaudoise prévoit, tout comme la loi fédérale, la tenue par le·la préposé·e à la protection des données d'un registre des fichiers (art. 19 à 21a LPrD). Celui-ci est alimenté par le responsable du traitement qui doit informer le·la préposé·e de tout projet visant à constituer un fichier contenant des données personnelles[18].

Le règlement d'application de la LPrD (RLPrD) décrit le contenu du registre des fichiers et les modalités de transmission : *nature et but du fichier, existence de données sensibles et/ou de profils de la personnalité, provenance des données, co-exploitation, modalités d'accès au fichier, nombre approximatif des personnes concernées, durée de conservation (archivage ou destruction), nom des tiers au bénéfice de la transmission, disposition légale autorisant la transmission, périodicité et modalités de la transmission (accès au fichier).*

Transfert des données personnelles réglementé

La LPrD (art. 15) réglemente la communication de données personnelles par les entités soumises à la législation. Les transferts peuvent soit s'effectuer entre une entité soumise à la LPrD et une personne physique ou morale, soit entre plusieurs entités soumises à la LPrD. Les transferts intraétatiques sont donc également soumis à cette disposition. Celle-ci précise notamment que le transfert de données personnelles doit se fonder sur une disposition légale, ou être nécessaire pour remplir une tâche légale ou encore répondre à un intérêt prépondérant du requérant privé[19].

Ces règles sont également valables en cas de procédure d'appel[20], c'est-à-dire concernant les données qui sont accessibles en ligne en « libre-service ». Toutefois s'il s'agit de données sensibles ou de profils de personnalités accessibles par procédure d'appel, une base légale formelle ou un règlement sont exigés dans le cas d'un transfert entre entités soumises à la LPrD ; s'il s'agit d'un transfert vers une entité privée, il est nécessaire que « *…une loi au sens formel le prévoit expressément…* » (art. 16 LPrD).

[18] Font exception à l'obligation de déclaration : fichiers renfermant uniquement des informations accessibles au public, fichiers d'enregistrement de la correspondance, fichiers d'adresses, fichiers éphémères dont la durée de vie n'excède pas un an (art. 21a LPrD).
[19] L'article 5 LPrD mentionne encore d'autres motifs, moins fréquents dans le cadre de transfert entre entités publiques : la personne concernée a exprimé expressément son consentement ; le transfert fait l'objet d'un consentement exprès des personnes concernées ; la personne concernée a rendu les données personnelles accessibles à tout un chacun et ne s'est pas formellement opposée à leur communication ; etc. En outre, les autorités peuvent communiquer spontanément des données personnelles dans le cadre de l'information au public, en vertu de la loi sur l'information, à condition que la communication réponde à un intérêt public ou privé prévalant sur celui de la personne concernée.
[20] Cette notion désigne le mode de communication automatisé des données par lequel les destinataires, en vertu d'une autorisation du responsable du fichier, décident de leur propre chef, sans contrôle préalable, du moment et de l'étendue de la communication. C'est en fait une communication régulière qui prend la forme d'une autorisation générale d'accéder aux données (on line). Dans un tel cas, c'est l'impossibilité pour l'organe communiquant de vérifier de cas en cas si les principes généraux sont respectés qui fonde la nécessité d'une base légale autorisant expressément une telle procédure.

Communications transfrontières soumises à restrictions supplémentaires

La LPrD réglemente également la communication transfrontière en posant l'exigence que le pays de destination de ces données dispose d'un *niveau de protection adéquat* en matière de protection des données. Des exceptions sont toutefois prévues dans la loi (par exemple en cas de consentement de la personne concernée, si la sauvegarde d'un intérêt public en dépend, si les garanties contractuelles sont suffisantes, etc.).

Cette question se pose par exemple lorsque le fournisseur d'hébergement des données se trouve à l'étranger où les lois locales en matière de protection des données s'appliquent. Si les pays de l'Union européenne, soumis au RGPD, offrent un niveau adéquat de protection, tel n'est pas le cas des Etats-Unis, de l'Inde ou de la Chine par exemple [21].

La LPrD autorise le recours à des sous-traitants …

L'article 18 alinéa. 1 de la LPrD prévoit que le traitement de données peut être confié à un sous-traitant[22] aux trois conditions cumulatives suivantes :

- le traitement par le sous-traitant est prévu par la loi ou par un contrat ;
- le responsable du traitement est légitimé à traiter lui-même les données concernées ;
- et aucune obligation légale ou contractuelle de garder le secret ne l'interdit.

… mais en cas de contrat, il est nécessaire de préciser leur assujettissement

Si le traitement par un sous-traitant n'est pas prévu par une loi, un contrat avec celui-ci doit être conclu. Si le sous-traitant est considéré comme délégataire d'une tâche publique, il est soumis automatiquement à la LPrD. Ainsi le contrat (ou la convention) devrait rappeler qu'il doit se conformer à la LPrD, voire en rappeler certains principes.

S'il s'agit d'un sous-traitant privé, œuvrant par exemple dans le domaine informatique, il n'est pas considéré comme délégataire d'une tâche publique et sera, s'il est basé en Suisse, soumis à la loi fédérale sur la protection des données. Or si le·la préposé·e cantonal·e est l'autorité de surveillance et de recours pour la loi cantonale, pour la loi fédérale, il s'agit du·de la préposé·e fédéral·e à la protection des données et à la transparence. En conséquence et afin que l'ensemble de l'activité des collectivités publiques vaudoises soit conforme à la LPrD, il faut que le contrat de sous-traitance prévoie une clause imposant au sous-traitant de respecter la LPrD.

De surcroît, le sous-traitant doit également être contractuellement soumis au secret de fonction (voir chapitre 3.2.3)

[21] « *Aux USA par exemple, le Foreign Intelligence Surveillance Act américain (FISA) permet au Gouvernement américain d'obtenir facilement des informations concernant des personnes qui ne sont pas des résidents U.S. lorsque les données sont hébergées sur sol américain ou traitées par des entreprises américaines. Le FISA avait initialement pour but de surveiller les espions étrangers, mais au gré des modifications cette loi vise désormais les pouvoirs étrangers et les agents de pouvoirs étrangers, une notion sujette à une interprétation large. L'ACLU, une organisation américaine de défense des libertés individuelles, considère que les avocats, journalistes, chercheurs et universitaires étrangers sont également inclus dans cette notion. Comme les non-résidents U.S. sont exclus de la protection offerte par le IVe Amendement, ils ne bénéficient même pas de la possibilité de saisir une autorité judiciaire ou d'être informés une fois la transmission de leurs données intervenue. Il existe dès lors un risque réel que des données de ressortissants suisses ou européens puissent être obtenues par les autorités américaines.* » Source : « Confier ses données à une société étrangère n'est pas sans risque », Sylvain Métille, Medialex 2013, Stämpfli Verlag AG.

[22] La LPrD, comme la LPD parle improprement de tiers.

Lien entre la LPrD et la loi sur l'information (LInfo)

A l'image de la Confédération et de plusieurs cantons, Vaud a opté pour l'institution d'une autorité à la fois responsable de la protection des données et de l'application de la loi sur l'information (LInfo)[23]. Cette dernière, entrée en vigueur en juillet 2003, lui est en effet partiellement liée : par exemple, un document susceptible d'être rendu public selon la LInfo, peut contenir des données personnelles qui, au vu de la LPrD, doivent rester confidentielles. Il est ainsi essentiel que les principes de transparence et de protection des données soient appliqués de manière cohérente d'où l'intérêt que l'application et la surveillance de ces deux dispositions soient traitées par la même instance.

Nécessité de réviser la LPrD

Comme mentionné en introduction et détaillé dans l'annexe III, le cadre juridique international et national impactant les dispositions vaudoises a évolué, nécessitant de réviser ces dernières en profondeur. En effet, la LPrD n'est plus alignée sur la Convention 108+ ni sur les éléments du RGPD et n'assure donc plus un niveau de protection adéquat en regard des exigences des pays de l'Union européenne.

D'autre part, à l'instar de la plupart des cantons, le Canton de Vaud n'a pas encore transposé dans sa législation les éléments de la directive « Police-Justice » du Parlement Européen[24], contrairement aux exigences liées aux accords de Schengen.

3.1.3 DIFFICULTÉS LIÉES À L'APPLICATION DE LA LÉGISLATION SUR LA PROTECTION DES DONNÉES

Besoin d'interprétation des dispositions

La difficulté d'application de la loi réside tout d'abord dans le besoin et la marge d'interprétation conférée aux différentes notions qui fondent les dispositions. La définition précise de ce qui est requis ou de ce qui est interdit ne découle pas clairement des textes législatifs et demande une analyse fine voire une pesée des intérêts. En outre, une bonne application de cette législation nécessite une connaissance approfondie du domaine métier auquel elle s'applique.

Par exemple pour que le principe de légalité soit respecté, la loi prévoit plusieurs possibilités pour le traitement de données personnelles sensibles. Si la première constitue un critère clair, soit l'existence d'une base légale formelle, la deuxième nécessite une appréciation. Elle stipule que le traitement des données personnelles sensibles doit être « absolument exigé » pour l'accomplissement d'une tâche « clairement définie » par une base légale formelle. L'absolue nécessité du traitement est donc à démontrer, comme la définition claire de la tâche.

[23] La loi sur l'information a pour but de garantir la transparence des activités des autorités afin de favoriser la libre formation de l'opinion publique et réglemente de ce fait l'accès aux informations qu'elles détiennent en posant le principe que « … *les renseignements, informations et documents officiels détenus par les organismes soumis à la présente loi sont accessibles au public* » (art. 8 al. 1 LInfo). Des exceptions à ce principe peuvent être accordées « … *si des intérêts publics ou privés prépondérants s'y opposent.* » (art 16 al. 1 LInfo).

[24] Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données (Directive EU 2016/680).

L'application des principes de finalité, de proportionnalité et de conservation demande également une connaissance approfondie de la tâche publique concernée. Il n'est en effet pas toujours aisé de déterminer si le but dans lequel sont utilisées les données est lié au but initial du traitement, si le traitement de telles ou telles données personnelles est effectivement nécessaire ou si les données ne sont pas conservées plus longtemps que nécessaire.

Référence à la notion d'«intérêt prépondérant»

La loi se réfère aussi largement à la notion d'intérêt prépondérant :

- l'existence d'un intérêt prépondérant limite le devoir d'informer les individus d'un traitement de données les concernant (art 14, al 1 lettre b) ;
- l'intérêt prépondérant d'un requérant privé peut justifier la communication de données personnelles relatives à un autre individu (art 15, al 1 lettre c) ;
- en cas d'intérêt prépondérant, le responsable du traitement peut refuser l'accès d'un individu à ses données personnelles (art 27, al 1 lettre b).

Si la doctrine fournit une définition de base de la notion d'intérêt prépondérant[25], l'appréciation finale requiert une analyse souvent approfondie, basée sur une bonne connaissance du domaine en question et une interprétation de la situation. Il faut en effet d'abord identifier l'intérêt privé ou public en question et le mettre en balance, dans chaque cas, avec l'intérêt présumé de la personne à ce que ses données ne soient pas traitées. Ce n'est que si le premier prime sur le second qu'il sera prépondérant.

3.2 LE SECRET DE FONCTION

3.2.1 OBJECTIF, DÉFINITION ET PÉRIMÈTRE

Notion et portée précisées par la doctrine

Si la législation fournit une définition générale du secret de fonction et le Code pénal suisse précise les sanctions en cas de violation, son objectif et sa portée sont définis par la doctrine. Les éléments figurant dans ce chapitre sont directement issus d'un avis de droit sollicité par la Cour des comptes (dans le cadre d'un autre audit)[26].

Double objectif du secret de fonction

Le secret de fonction a pour premier objectif de protéger le bon fonctionnement des institutions et l'accomplissement des tâches de l'État. Il permet d'assurer la confidentialité des informations confiées et de conserver la confiance des citoyen·ne·s qui sans cela seraient plus réticents à fournir les renseignements dont les services étatiques ont besoin pour assurer leurs tâches.

Le secret de fonction protège d'autre part la sphère privée des particuliers qui ne souhaitent pas que les renseignements qu'ils fournissent à l'Etat puissent être divulgués à tout un chacun. Ainsi, le champ couvert par le secret de fonction et la protection des données personnelles se recouvre partiellement (voir point 2.4).

[25] « *Les intérêts publics prépondérants visent à assurer le bon fonctionnement des autorités et du processus de décision, ainsi que la sécurité et l'ordre publics alors que les intérêts privés prépondérants assurent principalement la protection contre une atteinte notable à la sphère privée ou d'autres secrets (…).* » Sylvain Métille, « L'utilisation de l'informatique en nuage par l'administration publique », PJA 2019.

[26] Avis de droit pour la Cour des comptes VD, décembre 2018 « Avis de droit sur la portée du secret de fonction dans le cadre de prestations informatiques et les risques particuliers liés aux contrats informatiques ».

La définition du secret de fonction se réfère à l'existence d'un intérêt prépondérant

La définition du secret de fonction figure à l'art. 18 de la loi vaudoise sur l'information (LInfo) :

> **Secret de fonction (Art 18 LInfo)**
>
> *Il est interdit aux collaborateurs de la fonction publique ainsi qu'aux délégataires d'une tâche publique de divulguer des informations ou des documents officiels dont ils ont eu connaissance dans l'exercice de leur fonction, et qui doivent rester secrets en raison de la loi ou d'un intérêt public ou privé prépondérant.*

Avant son entrée en vigueur en 2003, la définition du secret de fonction était beaucoup plus simple à appliquer, puisque la culture du secret primait sur la transparence : toute information obtenue dans le cadre professionnel devait par défaut être tenue secrète par les employé·e·s de la fonction publique.

Depuis lors, le périmètre de la notion de secret de fonction est plus difficile à déterminer, sa définition faisant désormais référence à la notion d'intérêt prépondérant mentionnée plus haut. Dans les cas de données personnelles sensibles ou de profils de personnalité, les données sont presque toujours couvertes par le secret de fonction[27].

3.2.2 VIOLATION DU SECRET DE FONCTION

La violation du secret de fonction est pénalement répressible

La violation du secret de fonction est un délit sanctionné pénalement par le Code pénal suisse :

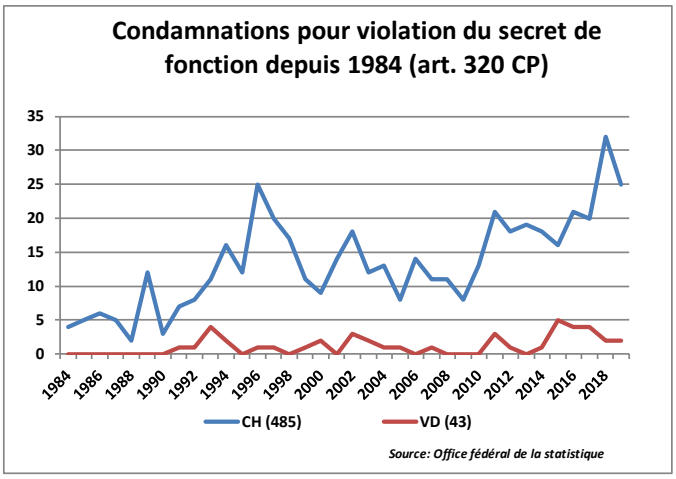
> **Violation du secret de fonction (Art. 320 CP)**
>
> 1. *Celui qui aura révélé un secret à lui confié en sa qualité de membre d'une autorité ou de fonctionnaire, ou dont il avait eu connaissance à raison de sa charge ou de son emploi, sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. La révélation demeure punissable alors même que la charge ou l'emploi a pris fin.*
> 2. *La révélation ne sera pas punissable si elle a été faite avec le consentement écrit de l'autorité supérieure.*

Il y a violation du secret de fonction lorsqu'un·e membre d'une autorité ou un·e fonctionnaire divulgue une information officielle relevant d'un fait secret au sens du Code pénal et ne pouvant pas être accessible selon la LInfo. C'est la personne individuelle qui est condamnée et non l'État.

[27] L'exception principale concerne le cas où les personnes concernées ont déjà rendu public les données personnelles sensibles les concernant, ce qui enlèverait tout intérêt à garder l'information secrète.

Peu de condamnations …

Le nombre de condamnations pénales pour violation du secret de fonction est assez faible : de 1984 à 2019, seules 43 condamnations ont été prononcées pour le canton de Vaud et 485 pour toute la Suisse. Cela représente moins de 2 cas par année pour Vaud et moins de 14 cas pour l'ensemble de la Suisse.



… mais des sanctions beaucoup plus sévères que celles liées au non-respect de la LPrD

La LPrD contient certes une disposition sanctionnant la violation du droit de discrétion : « *Toute personne ayant révélé intentionnellement, d'une manière illicite, des données personnelles ou sensibles qui ont été portées à sa connaissance dans l'exercice de sa fonction, sera punie d'une amende* » (art. 41 al. 1 LPrD). Cependant dans les faits, la violation du devoir de discrétion concernant des données personnelles soumises au secret est généralement sanctionnée par l'art. 320 du Code pénal suisse qui prévoit une peine plus lourde.

3.2.3 CONDITIONS DE DÉLÉGATION DE TRAITEMENT DE DONNÉES PERSONNELLES SOUMISES AU SECRET DE FONCTION

Nécessité de régler les conditions de sous-traitance de données personnelles par un contrat

Le chapitre précédent a précisé les conditions de traitement de données personnelles par des sous-traitants, nécessitant une clause contractuelle les obligeant au respect de la LPrD.

Dans la même logique, celui qui confie une information soumise au secret de fonction à un sous-traitant ou à un délégataire d'une tâche publique doit s'assurer que ce dernier est soumis au secret par la loi ou par un engagement exprès, notamment dans un contrat écrit. Même si on accorde au sous-traitant la qualité d'auxiliaire[28] impliquant une application automatique de l'art. 320 CP, il est nécessaire de le préciser dans le contrat de délégation de traitement.

[28] Dans son acception large, la notion de sous-traitant peut être assimilée à celle d'auxiliaire. Or selon la doctrine admise, on peut appliquer la notion d'auxiliaire de l'art. 321 CP (qui sanctionne la violation du secret professionnel concernant notamment les médecins, avocats, etc. et leurs auxiliaires) à l'art. 320 CP par analogie, en ce sens que les auxiliaires sont également soumis au secret de fonction. La notion d'auxiliaire a d'ailleurs été ajoutée à l'art. 320 CP dans le cadre de l'adoption de la loi fédérale sur la sécurité de l'information au sein de la Confédération (LSI) du 18 décembre 2020. La modification n'est pas encore entrée en vigueur.

Les conditions de délégation de données soumises au secret

Si un engagement à respecter le secret de fonction semble suffisant lorsque l'auxiliaire est basé en Suisse, il en va différemment si celui-ci est soumis au droit étranger. Le sous-traitant pourrait ainsi être obligé, en vertu du droit étranger, de transmettre des informations protégées au sens du droit suisse[29]. De surcroît, il sera difficile de le sanctionner s'il a agi à l'étranger.

Les conditions de délégation de traitement de données personnelles soumises au secret de fonction sont donc en principe les suivantes :

- le sous-traitant est en Suisse et soumis au droit suisse ;
- les données sont traitées (y compris l'hébergement) en Suisse.

Une exception à ces conditions peut toutefois être admise dans les cas où les données sont chiffrées et que le prestataire n'a ni la clé, ni raisonnablement la possibilité de déchiffrer les données. En effet ces données chiffrées ne sont pas considérées comme des données personnelles et ne sont pas non plus soumises au secret de fonction.

[29] Voir exemple décrit sous note 21 page 21.

3.3 LA SÉCURITÉ INFORMATIQUE

Comme précisé au chapitre 2, l'examen de la sécurité informatique dans le cadre de cet audit vise à s'assurer que des mesures techniques conformes aux bonnes pratiques ont été adoptées pour garantir la sécurité, l'intégrité, la disponibilité ainsi que la traçabilité des données au sens de l'art. 10 LPrD. La qualité technique des mesures n'a pas été examinée.

3.3.1 LE CADRE RÉGLEMENTAIRE DE LA SÉCURITÉ INFORMATIQUE À L'ACV

Règlement et directives liés au personnel

Le cadre réglementaire sur le personnel et les directives émises par le SPEV définissent également les responsabilités des collaborateur·trice·s ACV en matière de sécurité informatique :

- le RLPers « Les collaborateurs utilisent le matériel confié à des fins professionnelles conformément aux directives émises » (art. 125 al. 1) ;
- la directive LPers 50.1 « Utilisation d'Internet, de la messagerie électronique, de la téléphonie et du poste de travail », fixe un certain nombre de règles de sécurité à respecter par les collaborateur·trice·s ;
- la directive DT 48.8 sur le télétravail fixe les règles de sécurité à respecter spécifiquement en télétravail.

Règlement sur l'informatique cantonale (RIC)

Le règlement sur l'informatique cantonale (RIC) décrit les missions et les responsabilités des différents acteurs étatiques en matière de sécurité informatique.

Pilotage stratégique informatique et politique de sécurité des systèmes d'information sous la responsabilité du Conseil d'Etat

Le pilotage stratégique général des systèmes d'information est sous la responsabilité du Conseil d'Etat qui établit tous les cinq ans un Plan directeur cantonal informatique (art. 4 al. 2 RIC). Le plan actuel porte sur la période 2018-2023.

Le volet de la sécurité des systèmes d'information est également du ressort du Conseil d'Etat qui, dans le cadre de sa mission consistant à « *définir les orientations stratégiques en matière d'évolution des systèmes d'information* » (art. 4 al. 1 RIC), « *adopte la politique de sécurité des systèmes d'information* » (art. 4 al. 2 RIC).

Il est encore précisé qu' « *à travers la politique générale de sécurité des SI, le Conseil d'Etat définit les objectifs généraux et les principes de mise en œuvre de la protection des informations, en particulier des données personnelles, afin de garantir en tout temps leur disponibilité, leur intégrité et leur confidentialité.* » (art 15 al. 1 RIC).

La DGNSI chargée de la mise en œuvre de la politique de sécurité

La mission générale de la DGNSI consiste à assurer « *la disponibilité des moyens informatiques et de télécommunications nécessaires quotidiennement au bon fonctionnement de l'Administration et mettre en œuvre, avec les services bénéficiaires, des solutions contribuant à rendre les processus de l'Administration plus simples et plus efficients, pour elle-même et pour les usagers* » (art. 6 RIC).

Avec l'acceptation par le Grand Conseil de la loi sur la cyberadministration entrée en vigueur au 1er décembre 2020, la DGNSI a vu son périmètre d'action s'étendre et inclure le déploiement des prestations et échanges électroniques entre l'Etat et les usagers, entreprises et autres collectivités publiques, via un portail électronique.

Le devoir d'assurer la sécurité entre dans le cadre de la mission générale de la DGNSI ; il est mentionné en effet qu'elle est chargée spécifiquement de la « *mise en œuvre de la sécurité des systèmes d'information (…) sous la conduite d'un responsable de la sécurité des systèmes d'information* » (art. 7 RIC).

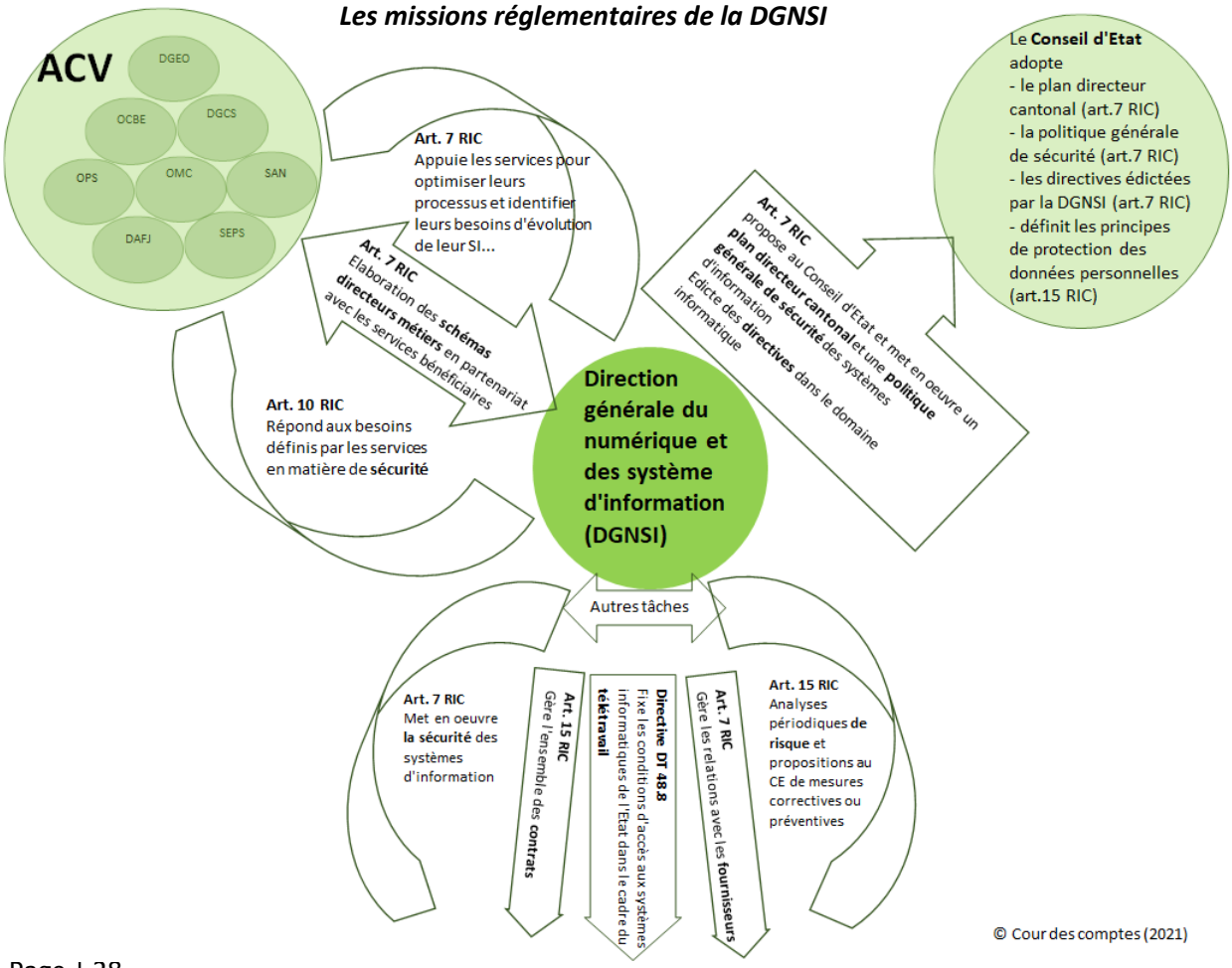
La DGNSI est l'entité charnière entre l'instance de pilotage stratégique et les services-métiers : elle est chargée à la fois de mettre en œuvre les orientations stratégiques fixées par le Conseil d'Etat et de répondre à leurs besoins de manière générale et en matière de sécurité.

Le schéma directeur sectoriel du système d'information (SI), un outil pour le présent et le futur

En partenariat avec les services-métiers, elle établit leur schéma directeur sectoriel du SI (ou schéma directeur métier). Ce dernier définit, pour un ensemble de services ou un service en particulier, les principes, les étapes et les projets d'évolution du système d'information métier pour les 5 à 10 ans à venir, en adéquation avec les orientations stratégiques d'un service.

Dans ce cadre, la DGNSI a la charge de « *documenter et analyser les systèmes informatiques et leurs fonctionnalités afin de permettre l'élaboration de schémas directeurs métiers en partenariat avec les services bénéficiaires* », « *élaborer des solutions propres à chaque métier* » et de « *gérer les relations avec les fournisseurs de biens et services en matière de technologies de l'information et de la communication* », étant donc seule habilitée à gérer les contrats. En outre elle est chargée « *d'édicter des directives dans le domaine informatique* » (art.7 al. 1).

Les missions réglementaires de la DGNSI



Définition des besoins en sécurité par les services-métiers

La mise en œuvre des mesures de sécurité informatique implique une étroite collaboration entre la DGNSI et les services-métiers. Ces derniers, en tant que propriétaires des données, « *définissent les besoins en matière de sécurité (disponibilité, intégrité, confidentialité)* » et sont « *responsables de la qualité, de l'harmonisation et de l'optimisation de leurs processus en vue notamment de leur informatisation* » (art. 10 a. 1 RIC), ainsi que de « *documenter et d'analyser leur stratégie, leurs processus, leur organisation et leurs besoins fonctionnels afin de permettre l'élaboration de leur schéma directeur sectoriel (métier)* » (art. 10 al. 2 RIC).

La sécurité dans la loi sur la protection des données

La sécurité des données personnelles assurée par le responsable du traitement

La LPrD comprend une disposition sur la sécurité des données personnelles : « *le responsable du traitement prend les mesures appropriées pour garantir la sécurité des fichiers et des données personnelles, soit notamment contre leur perte, leur destruction, ainsi que tout traitement illicite*. »

La responsabilité de la sécurité incombe donc prioritairement au responsable du traitement. Au niveau informatique, ce dernier doit donc, selon le RIC, définir ses besoins en la matière auprès de la DGNSI qui est chargée d'y pourvoir.

Les éléments ci-après ont permis de corroborer les résultats de l'audit de la Cour des comptes :

- la conformité aux démarches de sécurité recommandées par les normes ISO 27001 et 27002[30];
- les recommandations du préposé fédéral à la protection des données et à la transparence (PFPDT) ;
- les mesures recommandées par la CNIL[31] pour sécuriser, y compris les données soumises à la législation sur la protection des données personnelles ;
- l'analyse des conclusions d'autres audits, notamment sur la sécurité informatique à l'ACV.

3.3.2 LES NORMES ISO 27001 ET 27002

Norme ISO 27001 : système de management de la sécurité de l'information (SMSI)

La norme 27001 fixe les exigences pour la mise en place d'un système de management de la sécurité de l'information (SMSI). Le SMSI recense les mesures de sécurité pour garantir la protection des actifs d'un organisme contre toute perte, vol ou altération, et les systèmes informatiques contre toute intrusion et sinistre. La démarche prévoit quatre grandes phases : la phase d'établissement (Plan), la phase d'implémentation (Do), la phase de maintien (Check), la phase d'amélioration (Act) des mesures qui doivent être proportionnées aux risques encourus. L'application de cette norme dépend avant tout de l'analyse des risques et des objectifs fixés par l'entité, lui laissant ainsi une marge de manœuvre importante.

[30] L'ISO (Organisation internationale de normalisation) est une organisation internationale non gouvernementale, indépendante, dont les 166 membres sont les organismes nationaux de normalisation. www.iso.org.

[31] La CNIL (Commission Nationale de l'Informatique et des Libertés) a été créée en France en 1978. Elle est chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, aussi bien publics que privés. De par ses nombreuses publications, elle est devenue une Autorité dans le domaine de la protection et la sécurité des données. L'équipe d'audit a choisi de se baser également sur ses recommandations car plus actuelles que celles du Préposé fédéral à la protection des données qui datent de 2015.

Norme ISO 27002 : codes de bonnes pratiques pour la sécurité de l'information

La Norme ISO 27002 ressemble à un code de pratiques et ne fait pas l'objet d'une certification. Elle prévoit plusieurs volets dont notamment, l'évaluation des risques de traitement, les politiques et l'organisation de la sécurité de l'information, la sécurité des ressources humaines, le contrôle d'accès, la sécurité physique et environnementale, la sécurité des communications, les relations avec les fournisseurs, la gestion des incidents et de la continuité de l'activité.

3.3.3 LES RECOMMANDATIONS DU PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT)

Le « Guide relatif aux mesures techniques et organisationnelles de la protection des données » émis par le PFPDT en août 2015 contient des recommandations relatives à la sécurité physique et technique des données. Les mesures préconisées concernent quatre axes :

- l'accès aux données : sécurité des locaux, des serveurs et des places de travail, assurance de l'identification et de l'authentification des utilisateur·trice·s, sécurisation de l'accès ;
- le cycle de vie des données : introduction, journalisation, pseudonymisation/anonymisation, chiffrement, sécurité des supports, sauvegarde, destruction, sous-traitance, sécurité et protection ;
- le transfert des données : sécurité du réseau, chiffrement des messages, signature des messages, transmission des supports de données, journalisation des transferts ;
- le droit d'accès : droit des personnes concernées, reproductibilité des procédures.

3.3.4 LES MESURES RECOMMANDÉES PAR LA CNIL

Institution de référence au plan international en matière de protection des données, la Commission nationale informatique et libertés (CNIL) a publié en 2018 un guide « La sécurité des données personnelles ». Si une partie des thèmes sont repris de la norme ISO 27002, le guide consacre des chapitres à la protection des données : sensibilisation des utilisateur·trice·s, sécurisation de l'informatique mobile, traçage des accès, gestion des incidents et de la sous-traitance.

3.3.5 AUDITS SUR LA SÉCURITÉ INFORMATIQUE À L'ACV

Audits du Contrôle cantonal des finances (CCF)

Depuis la mise en place de la politique de sécurité informatique à l'ACV en 2011, le Contrôle cantonal des finances (CCF) réalise des audits en matière de sécurité informatique conformément à l'art. 10 de la loi sur le Contrôle cantonal des finances et assure le suivi des recommandations émises. Les constats de plusieurs d'entre eux sont utilisés dans le cadre de cet audit.

Audits de protection et sécurité des données de l'APDI

Conformément à sa mission de surveillance définie par la loi, l' Autorité de protection des données (APDI) peut, par autosaisine, réaliser des audits et émettre des recommandations. Elle a notamment mandaté un audit de sécurité sur l'application SI-RDU (système d'information du revenu déterminant unifié). Réalisé par un mandataire externe et publié en 2015, l'audit traite également de la sécurité générale de l'informatique à l'ACV.

4. RÉSULTATS : UNE CULTURE DE PROTECTION ET DE SÉCURITÉ INSUFFISAMMENT ANCRÉE À L'ACV

Les résultats des travaux d'audit sont présentés en trois sections :

- La première (chapitre 4.1) concerne à la fois la protection des données (axe 1) et la sécurité des données (axe 2) ; elle contient des constats et recommandations communs aux deux axes, destinés aux entités-cadres en matière de protection des données (APDI, DGNSI, SPEV).
- La deuxième (chapitre 4.2) porte spécifiquement sur l'application de la législation sur la protection des données par les entités-métiers et par les entités-cadres (axe 1).
- La troisième (chapitre 4.3) traite des mesures de sécurité informatique assurées par la DGNSI et du cadre réglementaire mis en œuvre par le SPEV pour les collaborateurs·trice·s (axe 2).

4.1 CLARIFIER LES RESPONSABILITÉS ET RENFORCER LA FORMATION

4.1.1 UN CADRE RÉGLEMENTAIRE DES RESPONSABILITÉS MAL CONNU

La mise en œuvre des dispositions de la législation sur la protection des données et des bonnes pratiques en matière de sécurité informatique implique divers intervenants, à différents niveaux. Il est dès lors essentiel que les rôles et responsabilités soient très clairement définis et que ce cadre soit connu. Ainsi, avant même d'examiner si les dispositions sont appliquées et de quelle manière, il convient de regarder si le cadre réglementaire définissant ces responsabilités est clair et si les différentes entités sont conscientes des tâches et obligations qui leur incombent.

Plusieurs niveaux de responsabilité bien définis

Il ressort du cadre réglementaire que les responsabilités sont effectivement définies de manière claire et cohérente, même s'il est nécessaire de procéder à une analyse et à une compilation des différentes lois, règlements et directives pour avoir une vision précise de la situation.

Pilote, entités-cadres, entités-métiers et collaborateurs·trice·s

Les responsabilités sont réparties sur quatre niveaux telles que décrites au précédent chapitre :

1. Le Conseil d'Etat : est chargé du pilotage stratégique en matière de :
    - Protection des données[32]
    - Sécurité des données[33]
    - Formation continue des collaborateur·trice·s[34].

[32] Le Conseil d'Etat est chargé de l'exécution de LPrD (art. 45 LPrD) et de sa révision.
[33] Le Conseil d'Etat définit les objectifs généraux et les principes de mise en œuvre de la protection des informations, en particulier des données personnelles afin de garantir en tout temps leur disponibilité, leur intégrité et leur confidentialité (art. 15 RIC). Il adopte la Politique générale de sécurité des systèmes d'information (art. 4 al. 2 RIC). Il valide le plan directeur cantonal informatique 2018-2023 (art. 4 al. 2 RIC), à noter que ce dernier contient parmi ses 2 axes prioritaires, la sécurité et la protection des données. Il adopte la Politique générale de sécurité des systèmes d'information (art. 4 al. 2 RIC).
[34] Le Conseil d'Etat promeut (art. 5 LPers) et met en œuvre sa politique de formation continue (art. 6 RForm).

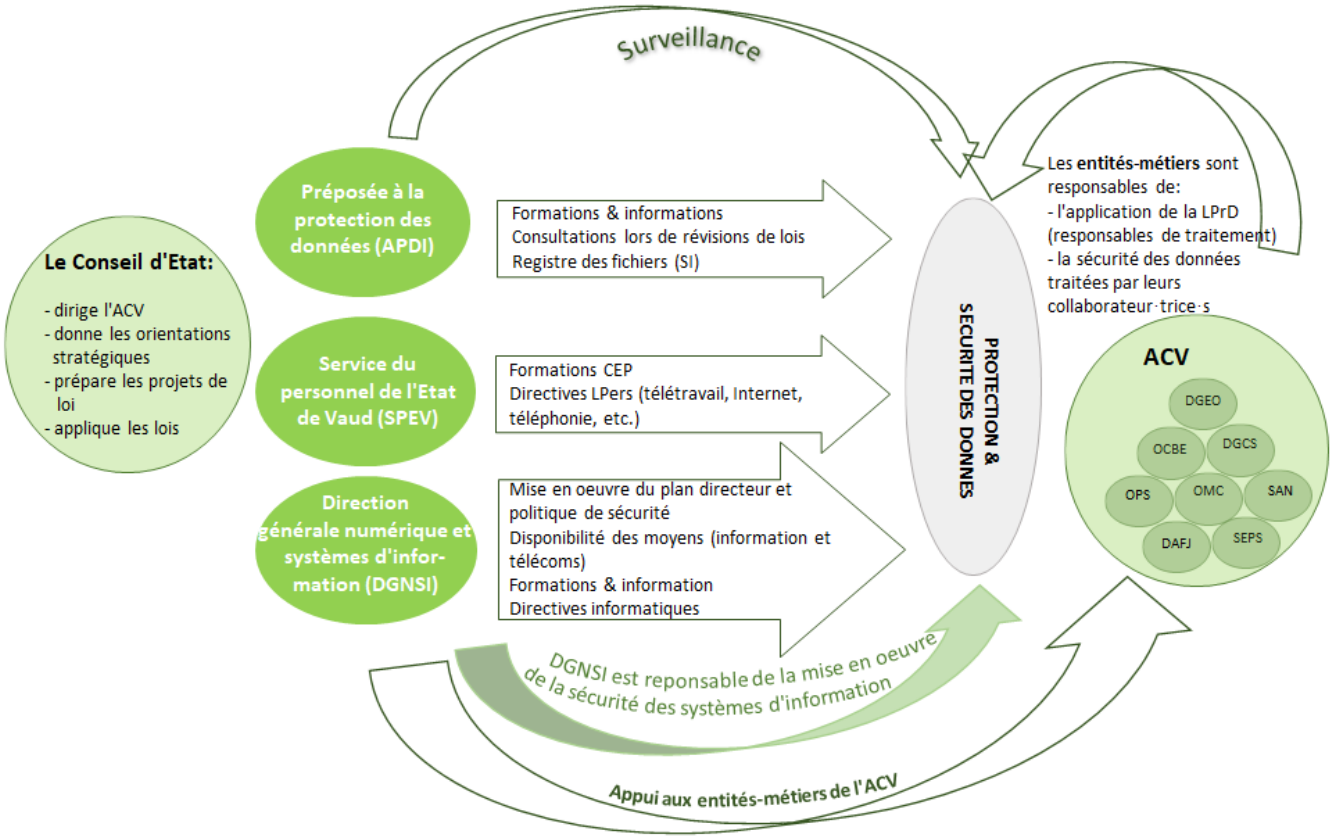
2. Les entités-cadres mettent en place les conditions pour assurer la protection et la sécurité des données :
   - L'APDI organise des formations, conseille les entités soumises à la LPrD, diffuse des informations sur la protection des données, notamment sur son site internet (recueil de jurisprudence, guides, etc.)[35].
   - Le SPEV est chargé d'édicter les directives pour le personnel (directives sur le télétravail DT 48.8 ou sur l'utilisation d'internet LPers 50.1, etc.) et de consolider les besoins en formation (art. 7 RForm).
   - La DGNSI a pour mission de répondre aux besoins en sécurité définis par les entités-métiers[36]. Elle se charge en outre des directives informatiques et des conseils de bonnes pratiques à l'intention des collaborateur·trice·s.
3. Les entités-métiers ont la charge de la protection et de la sécurité des données lorsqu'elles sont responsables du traitement et doivent définir leurs besoins en sécurité informatique : les entités-métiers sont « … *responsables de la qualité, de l'harmonisation et de l'optimisation de leurs processus en vue notamment de leur informatisation* … » (art. 10 al. 1 RIC) et sont chargées « … *de documenter et d'analyser leur stratégie, leurs processus, leur organisation et leurs besoins fonctionnels afin de permettre l'élaboration de leur schéma directeur sectoriel du système d'information en partenariat avec la DSI* … » (art. 10 al. 2 RIC). En matière de formation, elles ont la responsabilité d'identifier les besoins pour leurs collaborateur·trice·s et d'en faire part au SPEV (art. 7 RForm)[37]. Elles ont également le pouvoir de leur imposer des formations (art. 17 RForm).
4. Le·la collaborateur·trice doit, dans le cadre de ses fonctions « … *agir, en toutes circonstances, de manière professionnelle et conformément aux intérêts de l'Etat et du service public, dans le respect des normes en vigueur, des missions et des directives de son supérieur …* » (art. 50 al. 2 LPers). Il·elle est donc responsable de respecter la LPrD ainsi que les directives DT 48.8 et LPers 50.1 ainsi que les autres consignes de sécurité qui lui sont destinées. Il·elle est soumis·e au secret de fonction.

[35] Si la mission de l'APDI est centrée sur les conditions cadres, elle est également chargée du contrôle de l'application.

[36] En matière de sécurité informatique, la responsabilité de la DGNSI va bien au-delà de la mise en place des conditions cadres, puisqu'elle a la charge de la « *mise en œuvre de la sécurité des systèmes d'information* » (art. 7 RIC). Par contre sous l'angle de la protection des données, la responsabilité de la sécurité informatique incombe aux entités-métiers qui doivent définir leurs besoins en sécurité, la DGNSI étant chargée d'en assurer la mise en œuvre.

[37] L'article 7 RForm stipule que « *Les services définissent les formations nécessaires en fonction des besoins identifiés, notamment au moyen de l'entretien d'appréciation. Les services en informent le SPEV qui consolide les besoins.* »

Illustration des niveaux de responsabilités en matière de protection et sécurité des données des différents intervenants et tâches y relatives



Besoin de clarification des responsabilités pour les entités-métiers

S'il est apparu lors des entretiens avec les entités auditées que les entités-cadres, soit l'APDI, la DGNSI et le SPEV connaissaient leurs responsabilités, tel n'était généralement pas le cas pour les entités-métiers. En effet, le cadre réglementaire en vigueur à l'ACV leur délègue une large partie de la responsabilité en matière de protection et sécurité des données. Elles doivent également être proactives en matière de formation de leur personnel, y compris dans les domaines non directement liés à leur activité-métier, comme la protection des données ou la sécurité informatique.

Les réponses à la question posée aux entités auditées[38] à propos des responsabilités, montrent que ces dernières ne sont ni suffisamment connues, ni claires, que ce soit en matière de protection des données, de sécurité informatique ou de formation des collaborateur·trice·s. Une recommandation sur la nécessité de mieux informer les services sur leurs responsabilités est ainsi adressée aux trois entités-cadres.

[38] Question d'entretien n°46 « *Estimez-vous que les responsabilités en matière de protection et de sécurité des données traitées sont clairement définies pour les différents acteurs : entité responsable du traitement, entité utilisatrice, collaborateur·trice·s, DGNSI, Autorité de protection des données, SPEV, etc.* ? »

Dispositions de la LPrD et responsabilité des entités-métiers insuffisamment connues

Dans le domaine de la protection des données, les entités-métiers ont certes conscience que la responsabilité de mettre en œuvre les dispositions de la LPrD pour les données dont elles ont la charge leur incombe. Par contre, elles n'ont pas suffisamment pris la mesure de toutes leurs obligations et de toutes les dispositions auxquelles elles sont astreintes. Il appartient ainsi à l'APDI, dans le cadre de sa mission de support et conseil aux entités soumises à la LPrD, d'informer les services de l'ACV à ce propos.

Informer les services de leur responsabilité en matière de protection des données
Constatation n°1
Les services ont de nombreuses responsabilités. Or l'audit a montré que ces responsabilités étaient insuffisamment connues des entités auditées. Pour la protection des données personnelles, les services, en tant que responsables du traitement, sont chargés, selon la LPrD, de prendre « *les mesures appropriées pour garantir la sécurité des fichiers et des données personnelles* » (art. 10 LPrD). Ils sont en outre chargés d'appliquer l'ensemble des dispositions LPrD pour les données personnelles qu'ils traitent. La LPrD prévoit que le préposé à la protection des données « *informe les responsables de traitement sur les exigences posées en matière de protection des données* » (art. 37 LPrD).
Recommandation n°1 à l'APDI
Rappeler formellement aux responsables de traitement leur responsabilité en matière de respect des dispositions LPrD (en accord avec l'art. 37 LPrD, al. 1 lettre b).

Services-métiers insuffisamment proactifs pour définir leurs besoins en sécurité informatique

Les entretiens avec les entités-métiers ont révélé que la plupart d'entre elles ignorent qu'elles sont chargées de définir leurs besoins en sécurité, estimant, à tort, que la mission de sécurité relève uniquement de la compétence de la DGNSI. Certains services traitant de données très sensibles, comme les données médicales, sont toutefois conscients de la spécificité de leurs besoins, comme la mise à disposition d'une plateforme sécurisée pour les échanges de courriers électroniques ou la nécessité de tracer les accès, les opérations, etc. Mais aucun n'en a formellement fait part à la DGNSI.

De plus, les entités-métiers sont insuffisamment proactives en matière d'analyse et de documentation de leurs processus, essentiellement par méconnaissance de leurs obligations en la matière. Or cette démarche analytique et documentaire est une condition préalable à l'identification des besoins en sécurité. A noter aussi que les entités-métiers en tant que responsables de traitement doivent également s'assurer que leurs sous-traitants adoptent des mesures de sécurité appropriées. Cette responsabilité est également insuffisamment connue.

Informer les services de leur responsabilité en matière de sécurité informatique et gestion de leurs processus	
Constatation n°2	
Les services ont de nombreuses responsabilités. Or l'audit a montré que ces responsabilités étaient insuffisamment connues des entités auditées. Dans le domaine informatique, les services-métiers, en tant que propriétaires des données, « *définissent les besoins en matière de sécurité (disponibilité, intégrité, confidentialité)* » et sont « *responsables de la qualité, de l'harmonisation et de l'optimisation de leurs processus en vue notamment de leur informatisation* » (art. 10 a. 1 RIC), ainsi que de « *documenter et d'analyser leur stratégie, leurs processus, leur organisation et leurs besoins fonctionnels afin de permettre l'élaboration de leur schéma directeur sectoriel (métier)* » (art. 10 al. 2 RIC). En outre et selon la Politique générale de sécurité des systèmes d'information (PGSSI), fixée par le Conseil d'Etat, les services doivent assurer l'application de la politique générale de sécurité auprès des usager·ère·s, fournisseurs internes et externes.	
Recommandation n°2	**à la DGNSI**
Rappeler formellement aux chef·fe·s de service leur responsabilité découlant du Règlement sur l'informatique cantonale (RIC) et de la Politique générale de sécurité des systèmes d'information (PGSSI), en matière de définition de leurs besoins en sécurité informatique, d'optimisation de leurs processus et de documentation de leur activité. Les services doivent en outre s'assurer que leurs collaborateur·trice·s et leurs sous-traitants appliquent la politique générale de sécurité.	

A noter que le problème concerne surtout les domaines qui n'ont pas été dotés d'une application informatique récente ou qui n'ont pas collaboré étroitement avec la DGNSI récemment. En effet les services-métiers et la DGNSI collaborent étroitement lors de la mise en place d'un nouvel applicatif métier et il a été constaté que les besoins en sécurité étaient alors bien pris en compte.

Services-métiers insuffisamment impliqués en matière de formation continue

Selon la loi sur le personnel de l'Etat de Vaud : « *L'Etat et les collaborateur·trice·s partagent la responsabilité du maintien d'une formation suffisante* » (art. 37 LPers). En matière de protection et sécurité des données, il appartient cependant à l'entité-métier d'identifier les besoins en formation continue de son personnel et de faire part de ses besoins au SPEV.

Insuffisamment conscientes de leur responsabilité en matière d'application des dispositions sur la protection et la sécurité des données, les entités-métiers n'ont pas intégré qu'elles sont également responsables de l'identification des besoins en formation en la matière.

Ces besoins sont variables selon les services. Les besoins s'avèrent plus importants dans les entités traitant quotidiennement de données personnelles sensibles ou de profils de personnalité que pour les services traitant occasionnellement de telles données.

Or la Cour constate que la majorité des services-métiers audités, même ceux traitant de données qualifiées de très sensibles, n'avaient pas entrepris des démarches en la matière, en dépit du règlement sur la formation continue applicable aux services de l'ACV[39].

Informer les services de leur responsabilité en matière de formation (en sécurité et en protection des données)	
Constatation n°3	
Les services ont de nombreuses responsabilités. Or l'audit a montré que ces responsabilités étaient insuffisamment connues des entités auditées. En tant qu'autorité d'engagement, les services ont la charge d'identifier les besoins en formation de leur personnel afin de garantir qu'ils disposent des compétences nécessaires, y compris en matière de protection et de sécurité des données personnelles. La LPers précise que « *l'autorité d'engagement peut imposer une formation qu'elle juge nécessaire au maintien du niveau des prestations du collaborateur* » (art. 38 al. 1 LPers).	
Recommandation n°3	**au SPEV**
Rappeler formellement aux chef·fe·s de service leur responsabilité de garantir un niveau adéquat des compétences des collaborateur·trice·s en matière de protection et sécurité des données et, le cas échéant, appuyer les entités-métiers dans la mise en œuvre d'une formation pour les collaborateur·trice·s en fonction du besoin nécessité par leur fonction (art. 38 al. 1 LPers).	

4.1.2 FORMATION : UN BESOIN RECONNU PAR LES ENTITÉS-MÉTIERS

Protection des données : connaissances lacunaires déjà constatées lors de précédents audits

A l'instar des constats établis par les deux précédents audits de la Cour ayant abordé la question de la protection des données, à savoir celui consacré au contrôle des habitants du canton de Vaud[40], ainsi que celui portant sur les prestations d'orientation professionnelle pour adultes[41], le présent audit a mis en évidence un déficit de connaissances, parfois même de base, relatif aux dispositions en matière de protection des données.

Le besoin de formation s'est fait clairement sentir d'une part du fait des lacunes en matière de respect des dispositions qui seront détaillées au point 4.2. D'autre part, les représentant·e·s des entités auditées ont été unanimes à reconnaître que leurs connaissances en matière de protection des données ou celles de leurs collaborateur·trice·s étaient lacunaires en regard des dispositions en vigueur[42]. Seule une minorité d'entités-métiers ont déclaré avoir parmi leur personnel un·e collaborateur·trice ayant suivi une formation dans ce domaine[43].

[39] Règlement sur la formation continue du 9 décembre 2002 (RForm)
[40] « Audit du contrôle des habitants dans le canton de Vaud », CdC, rapport n°33 (2015) et « Audit de la performance des prestations d'orientation professionnelle pour adultes », CdC, rapport n°57 (2019). Si la recommandation de la Cour a débouché sur la mise en place avec succès d'une formation en matière de protection des données à l'intention des préposé·e·s au contrôle des habitants, l'audit sur les prestations d'orientation professionnelle, plus récent, est encore en cours de suivi.
[41] « Audit de la performance des prestations d'orientation professionnelle pour adultes », CdC, rapport n°57 (2019)
[42] La majorité des représentants n'a pas pu fournir de réponse précise sur le niveau de connaissance de leur personnel, si ce n'est qu'il n'était vraisemblablement pas suffisant.
[43] Une collaboratrice d'un Etat-major avait suivi la formation organisée par le Centre d'éducation permanente de l'Etat de Vaud (CEP) (2 heures) et un responsable de section avait suivi une formation plus poussée.

Le besoin est évidemment variable selon si les collaborateur·trice·s traitent régulièrement ou occasionnellement des données personnelles sensibles ou des profils de personnalités[44]. Néanmoins, comme le traitement de données personnelles d'administré·e·s concerne tous les secteurs de l'action étatique, il apparaît nécessaire que l'ensemble du personnel de l'Etat soit au bénéfice d'un socle de connaissances de base en la matière, ce qui n'est pas le cas actuellement.

Cas de divulgations de données personnelles sensibles avérés à l'ACV

Même s'ils sont relativement rares, des cas divers de violation de la confidentialité, du secret de fonction et de la LPrD se sont produites à l'ACV[45] :

- consultation d'un registre contenant des données personnelles à des fins d'investigation privée ;
- divulgation d'informations relatives à des données personnelles sensibles d'un autre membre du personnel figurant dans un registre ;
- consultation du Journal des événements de police (JEP) pour fournir des informations confidentielles sur les infractions commises par une personne à une proche.

Bien que les auteurs aient été sanctionnés, ces cas démontrent la nécessité de former les collaborateur·trice·s de l'ACV en matière de protection des données et de mieux les informer des conséquences en cas de non-respect.

Sécurité informatique : part non négligeable des employé·e·s non informé·e·s des risques

Malgré les informations dispensées par la DGNSI[46], les opérations de « faux phishing[47] » menées par la DGNSI depuis 2018 auprès des collaborateur·trice·s de l'ACV, ont révélé qu'une partie d'entre eux·elles avaient été piégé·e·s et n'étaient pas informé·e·s que certaines de leurs actions présentaient des risques de sécurité pour le système informatique de l'Etat. En effet, lors du premier test de « faux phishing » en 2018, près du quart des destinataires avait cliqué sur le lien suspect permettant de bénéficier d'un abonnement de fitness offert par l'Etat de Vaud. Deux ans plus tard seuls 12% de collaborateur·trice·s se sont laissé « hameçonner » par une pseudo-offre liée au Black Friday. En septembre 2021, un nouveau test a été réalisé, à l'aide d'un courriel demandant la mise à jour de l'application de connexion à distance VPN[48], permettant au personnel de se connecter au réseau informatique ACV à distance (notamment en télétravail). Cette fois 27% des collaborateur·trice·s se sont fait piéger par ce test, qui avait toutefois la caractéristique de concerner tous les membres du personnel contrairement aux deux autres. A noter également que sur les 3'748 personnes qui ont cliqué sur le lien suspect, 3'314 ont fourni leur identifiant et leur mot de passe.

En conclusion, bien que la DGNSI sensibilise régulièrement le personnel de l'Etat de Vaud depuis cinq ans, ces résultats témoignent d'un besoin d'information dans ce domaine.

[44] Le personnel employé dans des entités telles que l'Office du médecin cantonal (OMC) ou la Direction de l'insertion et des solidarités (DIRIS) traite beaucoup plus fréquemment de données sensibles que le personnel du SEPS par exemple.
[45] Deux entités-métiers auditées ont signalé un cas lors des entretiens et d'autres cas ont été relayés par la presse.
[46] Plusieurs informations sont mises à disposition par la DGNSI dont ESUSI, formation e-learning en matière de sécurité, élaborée en collaboration avec plusieurs cantons, à l'attention des collaborateur·trice·s de l'ACV et du public : https://www.esusi.vd.ch/esusi_menu_web/story.html.
[47] Le « phishing » (hameçonnage) désigne une tentative de fraude réalisée par courriel dans lequel les pirates insèrent un lien malveillant ou un document infecté et sur lesquels l'utilisateur·trice est invité·e à cliquer ou qui les invite à fournir des données personnelles.
[48] Virtual Private Network

Une clarification de la notion de secret de fonction depuis l'entrée en vigueur du principe de transparence est nécessaire

Avant l'entrée en vigueur de la loi sur l'information (LInfo) en juillet 2003, le périmètre des informations soumises au secret de fonction était simple à délimiter, le principe du secret étant à appliquer par défaut. Depuis lors, c'est le principe de transparence qui s'applique. Il reste toutefois actuellement encore beaucoup d'informations que les collaborateur·trice·s de l'Etat doivent garder secrètes, sous réserve de s'exposer aux sanctions prévues par l'article 320 du Code pénal relatives à la violation du secret de fonction.

Si une définition sommaire du secret de fonction figure sur le site intranet de l'ACV[49], elle n'est cependant pas suffisamment détaillée pour rendre compte de sa portée. Les sanctions encourues en cas de non-respect n'y sont notamment pas mentionnées. Dans le cadre de cet audit, nous constatons qu'aucun des services audités n'avait entamé de réflexion sur le périmètre des informations soumises au secret de fonction, ni n'avait informé son personnel de l'existence des dispositions légales y relatives. La délimitation des données soumises au secret de fonction et de celles soumises au principe de transparence n'est pas évidente.

Contrairement à la Confédération, l'Etat de Vaud n'impose pas d'obligation à son administration de classifier les informations selon leur degré de confidentialité. En effet, les services de l'administration fédérale[50] sont tenus de classifier toutes les informations « dignes de protection » selon trois catégories : secret, confidentiel et interne. Ainsi toutes les informations qualifiées de secrètes, confidentielles ou internes entrent par définition dans le périmètre du secret de fonction.

La Cour ne recommande pas la mise en place d'une telle systématique, qui représenterait pour l'administration un travail conséquent et qui devrait reposer sur une volonté politique, pour l'heure non exprimée. Il apparaît toutefois raisonnable d'intégrer dans le cadre d'une formation minimale sur la protection des données, un volet consacré au secret de fonction. Cela se justifie d'autant plus que, comme expliqué auparavant, ces deux notions ne se recouvrent que partiellement, ce qui nécessite une clarification.

Formation minimale pour tous les collaborateur·trice·s ACV

Plusieurs formations en protection et sécurité des données existent sans qu'il y ait d'obligation pour les collaborateurs·trice·s de l'ACV de les suivre. Si les besoins sont variables selon les secteurs d'activité, il apparaît que tou·te·s les employé·e·s devraient posséder des connaissances minimales dans ces domaines (y compris relatives au secret de fonction).

[49] https://intranet.etat-de-vaud.ch/themes/personnel/droits-et-devoirs/secret-de-fonction
[50] Selon l'Ordonnance concernant la protection des informations de la Confédération (OPrI) du 4 juillet 2007

Mettre en place une formation minimale et obligatoire en matière de protection des données, de secret de fonction et de sécurité informatique	
Constatation n°4	
Les responsables des services et leurs collaborateur·trice·s n'ont qu'une connaissance incomplète des dispositions de la législation sur la protection des données personnelles (LPrD). Ces lacunes concernent par exemple les règles de conservation et de communication des données personnelles, la définition précise des données personnelles sensibles, les bonnes pratiques à adopter etc. Aucun service n'a défini la notion de « secret de fonction » auquel est soumis tout le personnel de l'ACV : les informations sur la portée du secret de fonction et les sanctions encourues en cas de non-respect n'ont notamment jamais été clairement transmises aux collaborateur·trice·s. Ces dernier·ère·s sont en outre insuffisamment formé·e·s en matière de bonnes pratiques de sécurité informatique.	
Recommandation n°4	**au SPEV**
Instaurer une formation basique minimale obligatoire sur les devoirs et obligations du personnel de l'Etat dans les trois domaines que sont la protection des données (au sens de la LPrD), la sécurité informatique et le secret de fonction. Cette formation est destinée aux collaborateur·trice·s n'ayant pas eu de formation spécifique au préalable dans ces domaines.	

4.2 PROTECTION DES DONNÉES : RENFORCER L'IMPLICATION DES ENTITÉS-MÉTIERS ET LE CONTRÔLE PAR L'APDI

4.2.1 MISE EN CONFORMITÉ NÉCESSAIRE DU CADRE LÉGAL DES MÉTIERS

Le principe de la légalité est un des piliers de la législation sur la protection des données. Un précédent audit de la Cour des comptes[51] avait révélé une collecte de données sans base légale. Dans ce cas, il est nécessaire d'interrompre la collecte illégale ou de compléter la législation en question. Mais l'analyse du principe de légalité n'est pas aisée, la LPrD offrant plusieurs alternatives (voir chapitre 3.1.3). La communication de données personnelles repose sur des exigences similaires à la collecte tandis que la communication par procédure d'appel[52] de données personnelles sensibles ou de profils de personnalité entre entités soumises à la LPrD doit reposer sur une base légale ou sur un règlement.

[51] « Audit du contrôle des habitants dans le canton de Vaud » (n°33, 2015)

[52] Art. 4. al. 1 chiffre 10 LPrD : « *Procédure d'appel, mode de communication automatisé des données par lequel les destinataires décident eux-mêmes de la communication des données, moyennant une autorisation du responsable du traitement* ».

Le principe de légalité généralement respecté mais densité normative à examiner

Dans le cadre de cet audit, un examen des bases légales de l'activité des entités-métiers auditées a été effectué. S'il n'a pas été constaté de non-conformité évidente aux dispositions LPrD, il convient de s'interroger sur la suffisance de la densité normative dans les cas où la collecte et la communication de données ne reposent pas sur une base légale formelle. En effet, le Tribunal fédéral applique cette notion de manière restrictive (cf. ATF 6B_908/2018)[53], estimant qu'il faut disposer d'une base légale formelle pour traiter ou communiquer des données, et ce d'autant si celles-ci sont sensibles.

Les lois postérieures à la LPrD contiennent des clauses relatives à la protection des données

Certaines législations examinées, postérieures à la LPrD, contiennent une clause spécifique :

- la loi sur l'enseignement obligatoire (LEO) du 7 juin 2011[54], base légale pour la DGEO ;
- la loi sur la pédagogie spécialisée (LPS) du 1 septembre 2015[55], base légale pour l'OPS ;
- la loi sur l'aide aux études et à la formation professionnelle (LAEF) du 1 juillet 2014[56], base légale pour l'OCBE.

Les lois antérieures à la LPrD n'ont généralement pas été adaptées

La Cour relève que les lois examinées, antérieures à la LPrD ne contiennent pas de dispositions sur la collecte et la communication de données personnelles telles que la loi vaudoise sur l'action sociale du 2 décembre 2003 (LASV)[57] ou la loi sur la santé publique (LSP)[58] du 29 mai 1985.

Néanmoins, il paraît évident que pour accomplir les tâches décrites dans ces dernières, des données personnelles relatives au recours aux régimes sociaux ou des données médicales doivent être collectées. La Cour s'interroge toutefois sur l'opportunité d'introduire une disposition ad hoc, pour éviter toute ambiguïté laissant la porte ouverte à des recours et des procédures[59].

Néanmoins, deux cas de communication de données entre entités de l'ACV relevés dans le cadre de cet audit suscitent des interrogations de la Cour[60]. Leur non-conformité n'est pas avérée car ils visent l'accomplissement d'une tâche publique. Il serait néanmoins préférable d'examiner si la densité normative des dispositions sur lesquelles ils se basent est suffisante et au besoin la compléter.

---

[53] Cet arrêt a mis en évidence que le canton de Thurgovie ne disposait pas d'une base légale suffisante pour utiliser les enregistrements effectués par un système automatisé de recherche de véhicules et de surveillance du trafic (RSV), qui avait permis de détecter qu'une personne qui faisait l'objet d'un retrait de permis avait néanmoins conduit un véhicule. Le Tribunal fédéral estime que la réalisation et le stockage d'enregistrements RSV constituait une atteinte aux droits fondamentaux des personnes concernées. L'atteinte à la sphère privée liée à cette surveillance viole l'art. 13. al 2 Cst. et les preuves de l'infraction obtenues par ce biais, sans base légale spécifique, ne sont pas valables (pour autant que l'infraction ne soit pas reconnue comme grave).

[54] Art 44 LEO : « *Données personnelles des élèves* »

[55] Art. 61 LPS : *« Données collectées »*

[56] Art. 44 LAEF *« Traitement de données »* et art. 45 LAEF *« Communication de données »*

[57] La LASV s'applique aux prestations de la DIRIS.

[58] La LPS s'applique aux prestations de l'OMC.

[59] Par exemple la collecte de données sur la situation financière d'un requérant de mesure d'aide sociale, tâche nécessaire à son octroi a fait l'objet d'un recours. Ce dernier a certes été perdu par le requérant, mais a tout de même généré du travail de la part de l'autorité (source : affaire PS.2013.0068, CDAP 28.10.2013).

[60] Le premier concerne l'accès du SAN à l'application informatique des Offices des poursuites « Themis ». Il s'agit de la communication de données via une procédure d'appel. Si les informations figurant dans le registre des poursuites ne sont pas considérées comme sensibles au sens de la LPrD, elles sont toutefois plus délicates que de simples données d'identité. L'accès au registre repose sur une décision du Conseil d'Etat et non sur une base légale formelle ou un règlement. Chaque collaborateur·trice qui détient un accès doit signer un formulaire, également validé par la direction du SAN et le secrétaire de l'ordre judiciaire.
Le deuxième cas concerne la communication d'informations du Service de protection de la jeunesse (SPJ) à l'OCBE lorsque le mineur suivi par le SPJ atteint sa majorité et demande une bourse d'étude. La LAEF prévoit que les Centres sociaux régionaux, le service en charge de l'aide sociale et les établissements de formation peuvent échanger des données personnelles avec l'OCBE, mais le SPJ n'est pas mentionné, alors que certaines données sont sensibles. Les deux services ont toutefois signé un protocole de collaboration qui cadre et conditionne strictement l'échange de données entre eux.

Les services et entités-métiers sont d'ailleurs invités dans le cadre du travail d'analyse et de documentation demandé (voir recommandation n°7), à identifier les lacunes de leurs bases légales.

La Cour propose de revoir et d'adapter l'ensemble des bases légales dans le cadre de la révision de la LPrD et adresse donc cette recommandation au Conseil d'Etat.

Créer une base légale vaudoise pour le traitement des 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) et 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 (voir Annexe II). Si la Confédération a procédé à cette transposition, tel n'est pas le cas d'une partie des cantons, dont Vaud. Il convient dès lors de combler cette lacune.

Actualiser les bases légales indispensables à la collecte, au traitement et à la communication des données personnelles comme requis par la LPrD
Constatation n°5
Toutes les bases légales ne sont pas à jour en matière de collecte et de communication de données personnelles sensibles à l'ACV. La LPrD exige généralement l'existence d'une base formelle pour leur collecte, leur traitement et leur communication (y compris les communications de données entre services de l'ACV). La Cour a constaté que les législations antérieures à la date d'entrée en vigueur de la LPrD, soit 2007, n'ont généralement pas été adaptées à ces dispositions. Les bases légales relatives à la protection des données dans les domaines de la police et de la justice, en partie exclus du périmètre LPrD, ne respectent pas les exigences du développement des acquis Schengen auquel le canton de Vaud doit se conformer.
Recommandation n°5 **au Conseil d'Etat**
Dans le cadre de la révision de la LPrD et sur la base du travail d'analyse et de documentation à réaliser par les entités-métiers (voir recommandation n°7), proposer au législateur une adaptation des bases légales « métier » lacunaires en matière de traitement des données personnelles afin de légaliser la collecte, le traitement et la communication de toutes les données personnelles traitées par l'ACV. Cette mise à jour des bases légales doit également concerner les domaines de la police et de la justice afin de se conformer aux exigences du développement des acquis Schengen.

4.2.2 ENTITÉS-MÉTIERS EN GÉNÉRAL : FAVORISER LEUR IMPLICATION DANS LA MISE EN ŒUVRE DE LA LPRD

L'entrée en vigueur de la LPrD a remis en cause des pratiques parfois répandues

Comme expliqué précédemment, l'entrée en vigueur de la LPrD en 2008 a signifié un changement culturel important dans le mode de gestion des données personnelles. De nombreuses pratiques répandues et politiquement admises, ont été remises en cause. Le cas des certaines communes qui fournissaient régulièrement les adresses de leurs nouveaux·elles habitant·e·s à une entité externe chargée d'effectuer des envois publicitaires ciblés sur mandat de sociétés privées avait alors été révélé par la presse et avait fait grand bruit. Ce n'est qu'en juin 2017, et suite à de fortes pressions, qu'il a été mis fin à cette pratique qui reposait sur une base légale dont la portée était très débattue, mais qui dans son fondement n'était pas en phase avec les principes de protection des données.

Ce cas illustre la complexité de l'intégration des principes de protection des données. Il révèle également qu'il est parfois long de modifier des pratiques controversées en regard de la loi.

Une mise en œuvre organisationnelle parfois compliquée à réaliser …

Outre la connaissance insuffisante des dispositions de la LPrD que l'on peut constater dans les entités qui y sont soumises, des obstacles concrets se posent à leur mise en œuvre. Certains sont d'ordre organisationnel. En effet, pour les entités traitant un volume important de données personnelles sensibles dans des documents papiers ou des fichiers informatiques qui n'avaient pas été structurés selon les exigences de la LPrD, la mise en conformité des dossiers établis antérieurement à la LPrD représente un travail colossal. Cette tâche a souvent été repoussée faute de moyens. C'est le cas en particulier de l'Office du médecin cantonal (OMC), dépositaire d'un grand nombre de documents et d'archives médicales « papier » de diverses provenances.

… ou techniquement impossible

Des obstacles techniques existent également. C'est le cas des applications ou systèmes informatiques antérieurs à la LPrD qui n'ont pas été conçus pour respecter ces dispositions et qui ne sont pas suffisamment flexibles ou paramétrables pour être modifiés à cette fin[61] :

Tout d'abord, une politique de gestion des accès conforme aux règles de protection des données peut être compliquée à mettre en œuvre pour des applications informatiques anciennes ne permettant pas la segmentation des accès. En outre, les serveurs de base de l'Etat permettent une gestion des accès sur trois niveaux seulement. Ainsi, au sein d'une même entité, la limitation des accès à certaines données pour les seul·e·s collaborateur·trice·s en ayant réellement besoin s'avère parfois techniquement impossible.

De plus, les règles de bonnes pratiques en matière de protection des données traitées informatiquement requièrent, selon le type de données traitées, une journalisation des opérations[62]. Or si les applications informatiques récentes sont dotées de cette fonctionnalité, comme l'application de gestion électronique des documents (GED) utilisée à l'Etat, tel n'est pas le

[61] C'est le cas d'un certain nombre d'applications à l'ACV. L'audit « *Gouvernance des projets de système d'information métier de l'Etat de Vaud* » (n°67, août 2021) a mis en lumière que les systèmes d'information à l'ACV étaient remplacés souvent dans l'urgence, après avoir atteint un stade d'obsolescence avancé.

[62] L'enregistrement automatique et séquentiel de tous les accès au système d'information et de toutes les opérations effectuées.

cas des plus anciennes. Les opérations effectuées sur des documents à l'aide de logiciels de bureautique (Word, Excel, PDF, etc.) directement enregistrés sur le serveur ne sont que partiellement traçables[63].

De même, il n'existe pas toujours de solution sécurisée pratique pour l'envoi de courriers électroniques confidentiels[64].

Principes de la LPrD parfois perçus comme une entrave à réaliser une tâche publique

Lors des entretiens d'audit, la Cour note que les dispositions sur la protection des données sont perçues par certain·e·s comme une entrave à la réalisation de leur mission, générant des « complications » ou de la « paperasse » inutiles. Convaincu·e·s que le secret de fonction (ou médical ou professionnel) auquel le personnel de l'ACV est soumis est suffisant pour garantir la protection des données personnelles des administré·e·s, il·elle·s ne perçoivent parfois pas la plus-value de la mise en œuvre des exigences de la LPrD. La Cour regrette que certaines entités, sans le reconnaître ouvertement, manifestent une certaine résistance à empoigner la thématique de la protection des données.

Culture de la protection des données insuffisamment implantée

Changement culturel nécessaire à la mise en œuvre de la LPrD

L'accomplissement des missions des différentes entités de l'ACV n'étant pas tributaire de l'application des dispositions de la LPrD, cela explique également le peu d'entrain avec lequel certains services traitent de la question.

La situation s'avère toutefois inégale entre les entités auditées, certaines ayant été davantage proactives que d'autres comme cela sera détaillé ci-après (chapitre 4.2.3). Des constats généraux concernant l'ensemble d'entre elles peuvent toutefois être au préalable établis.

Manque d'analyse globale orientée protection des données

Comme vu précédemment, l'intérêt du respect de la sphère privée et les principes de la législation ne sont pas suffisamment connus des entités-métiers. Il n'est donc pas étonnant de constater que, faute de connaissances suffisantes, les entités-métiers auditées n'aient pas procédé à une analyse globale de toutes les données personnelles qu'elles traitent, permettant d'élaborer un concept de traitement qui respecte tous les principes de la législation sur la protection des données[65]. Si certaines ont certes intégré quelques principes, leur démarche relève davantage du « coup par coup », par exemple en cas de renouvellement d'une application informatique ou pour donner suite à une intervention externe (APDI, public, média, etc.), que d'une approche globale, cohérente et transversale à tous les domaines traités par l'entité-métier[66].

[63] Un « journal » des opérations est certes enregistré, mais le système ne permet pas de garantir que l'enregistrement n'a pas été modifié par la suite.

[64] La solution proposée à l'ACV pour les envois de courriers hors plateforme sécurisée, n'est en effet pas praticable pour les entités émettant ou recevant un grand nombre de messages, puisqu'elle consiste à compacter le fichier (zip) à envoyer en lui assignant un mot de passe qui doit être communiqué par un autre canal que le courrier électronique (par téléphone ou par SMS). Cette solution est beaucoup trop lourde et impraticable pour certaines entités communiquant quotidiennement avec l'extérieur.

[65] Ce constat concerne les entités traitant un grand nombre de données personnelles différentes et pour lesquelles une telle démarche analytique est nécessaire. Ce besoin est moindre pour les entités traitant un nombre limité de données personnelles.

[66] Seules deux entités ont fourni des réponses écrites et développées au questionnaire soumis : le SAN et l'OMC, témoignant qu'une réflexion avait eu lieu sur la thématique abordée.

Ainsi, la recommandation émise dans le rapport d'audit sur les prestations d'orientation professionnelle pour adultes[67], qui a conclu pour l'entité auditée, qu' « *Il est indispensable que l'Office* (*ndlr* Office cantonal d'orientation scolaire et professionnelle (OCOSP)) *développe une stratégie spécifique en lien avec la collecte, la conservation et la destruction des données personnelles des bénéficiaires* »[68], pourrait s'appliquer aux entités sollicitées dans le cadre du présent audit.

Lacunes en matière de directives internes

La Cour relève qu'aucune entité auditée n'a émis de directive interne couvrant l'ensemble de ses activités ou n'a élaboré de charte à l'intention de son personnel. Cette lacune, déjà pointée lors de précédents audits de la Cour, est la conséquence logique du manque de réflexion et de stratégie globale en matière de protection des données.

Si l'une des entités auditées a émis une directive ciblée[69], d'autres entités de l'ACV – mais non auditées - ont déjà effectué une telle démarche globale. Par exemple l'unité en charge du Système d'information sur le revenu déterminant unifié (SI-RDU), qui contient des informations sensibles relatives aux mesures sociales des bénéficiaires, a établi une déclaration de confidentialité détaillant les pratiques interdites pour les collaborateur·trice·s ayant accès aux données à protéger. Cette pratique, qui relève de l'exception à l'ACV, est un exemple à citer, car non seulement elle permet d'informer clairement le personnel concerné de ses obligations et des sanctions en cas de non-respect, mais elle constitue également un acte d'engagement pour les collaborateur·trice·s (le document figure dans l'annexe IV).

Manque de réflexion sur la conservation des données …

La majorité des entités n'ont pas non plus entamé de réflexion sur les règles de conservation et d'archivage à appliquer pour leurs données sous l'angle des dispositions en matière de protection des données. Elles n'ont généralement appliqué que les dispositions en matière d'archivage selon la loi vaudoise sur les archives (LArch), notamment pour établir le calendrier de conservation requis par la loi. Mais elles n'incluent pas automatiquement d'analyse en lien avec les dispositions de la LPrD[70]. Certaines entités ont même déclaré conserver les données personnelles, y compris les données sensibles, « aussi longtemps que possible », dans le cas où elles s'avéreraient utiles un jour. Cette pratique contrevient très clairement au principe de proportionnalité.

… ainsi que sur les mesures de sécurité

Comme relevé plus haut, la plupart des entités estiment que les mesures de sécurité informatique sont du seul ressort de la DGNSI et ne s'impliquent pas dans l'analyse et la définition de leurs besoins dans ce domaine[71]. A contrario, si certaines entités ont identifié des besoins, elles n'en ont pas informé la DGNSI (voir recommandation n°2).

[67] Rapport n°57 « Audit de la performance des prestations d'orientation professionnelle pour adultes »
[68] Il convient également d'intégrer le principe de sécurité à cette stratégie.
[69] Il s'agit de la DGEO (voir page 49).
[70] Seul l'OPS a élaboré un calendrier de conservation des archives en distinguant les dossiers actifs et inactifs pour les documents papier. La réflexion mériterait d'être poursuivie sous l'angle de la protection des données et devrait englober les données numérisées.
[71] L'audit « *Gouvernance des projets de système d'information métier de l'Etat de Vaud* » (n°73, août 2021) parvenait à un constat similaire : les services-métiers ne sont pas suffisamment impliqués dans la gestion de projets SI métiers qui leur sont destinés.

Contrats de sous-traitance ou de délégation de tâches souvent incomplets

Les entités auditées peuvent sous-traiter certaines de leurs tâches, confier des mandats spéciaux à des externes ou déléguer certaines missions. Sept documents relatifs à des contrats ou conventions, conclus par les entités auditées avec des sous-traitants ou mandataires externes ont été collectés dans le cadre de l'audit. La majorité des documents, soit six sur sept étaient lacunaires sur une des clauses mentionnées dans le chapitre précédent[72]. Une recommandation spécifique à chaque entité concernée sera détaillée au chapitre 4.2.3.

Gestion des accès analysée, mais la mise en œuvre se heurte parfois à des limites techniques

Les entités auditées ont toutes mené, à des degrés divers, des réflexions sur la gestion des accès pour assurer la protection de leurs données[73]. On relève toutefois que la mise en œuvre d'une gestion appropriée des accès aux données numériques est fortement dépendante des modalités techniques des applications informatiques. Ainsi, seules les entités équipées d'applications informatiques ayant été conçues dès le départ avec cette fonctionnalité ont pu mettre en place une gestion ciblée de ces accès. Les entités traitant leurs données sur le serveur de l'Etat sont, elles, limitées dans leurs possibilités de segmentation des accès.

Conditions à mettre en place pour opérer le changement culturel nécessaire

Ces constats généraux illustrent la nécessité de mettre en place des mesures de formation du personnel à tous les niveaux hiérarchiques (recommandations n°3 et n°4) : les objectifs et la finalité de la législation sur la protection des données doivent y être clairement explicités, de même que les bonnes pratiques minimales en la matière.

Ces constats dénotent également le besoin de rappeler aux entités leurs responsabilités en matière de protection et de sécurité des données (recommandations n°1 et n°2).

Cela témoigne aussi de la nécessité de créer, au sein des entités-métiers, les conditions nécessaires au changement culturel exigé par la législation sur la protection des données.

Cadre à mettre en place au sein des entités-métiers

Responsabiliser les entités-métiers

Les conditions cadres à implémenter passent par la mise en place de compétences internes visant à responsabiliser les entités. Elles consistent également à établir un cadre analytique et documentaire permettant de gérer les données conformément à la LPrD et aux besoins métiers. Le cadre légal est parfois également à adapter pour respecter les principes de légalité et de finalité.

[72] Pour rappel, il est tout d'abord nécessaire de soumettre contractuellement le sous-traitant ou le délégataire à la fois à la LPrD et au secret de fonction. Ensuite, il convient de s'assurer que le sous-traitant ou le délégataire soit basé en Suisse tout comme, contractuellement, que le traitement et l'hébergement des données sous-traitées le soient également.

[73] Lors des audits sur le contrôle des habitants et sur les prestations d'orientation professionnelle, cet aspect était alors apparu comme insuffisamment traité par les entités auditées.

Fonction de référent·e interne à l'entité-métier à mettre en place

La responsabilisation des entités-métiers en matière de protection des données passe par la nécessité de renforcer les compétences en interne. La désignation d'une personne parmi les employé·e·s d'une entité qui endosserait la fonction de délégué·e est une solution à même de répondre à ce besoin. Cette solution offre l'avantage pour l'entité de disposer d'un·e référent·e au fait de la législation en matière de protection des données (formé·e en la matière) tout en ayant les connaissances métier nécessaires à sa bonne application. Cela permet également de mieux filtrer les demandes adressées à l'APDI.

A relever que le Règlement européen sur la protection des données (RGPD) a introduit l'obligation d'instaurer la fonction de Délégué·e à la protection des données (DPO). Une disposition analogue figure également depuis 1993 dans la législation fédérale[74] qui prévoit au minimum un·e référent·e par département.

Au vu de la situation constatée dans le cadre de cet audit et de l'hétérogénéité des activités des services dans un même département, il paraît toutefois que la désignation d'un·e délégué·e au seul niveau départemental, par exemple au sein du secrétariat général, est insuffisant. Pour amener une réelle amélioration et garantir l'efficacité de la mission, il est nécessaire de disposer de compétence de proximité et au fait du métier en question.

En outre, les questions liées au droit d'accès des administré·e·s à leurs propres données conféré par la LPrD pourraient également être traitées par ce·tte délégué·e.

Désigner un·e délégué·e à la protection des données dans chaque entité-métier responsable de traitement.
Constatation n°6
Si pour l'ensemble des collaborateur·trice·s, une formation minimale basique en matière de protection et de sécurité des données (recommandation n°4) suffit à leurs besoins, la plupart des entités-métiers qui gèrent des applications complexes contenant des données sensibles, nécessitent des compétences internes spécifiques plus pointues en matière de protection des données. Or, dans la plupart des services audités, ces compétences sont insuffisantes.
Recommandation n°6 **au Conseil d'Etat**
Prévoir l'obligation pour chaque entité-métier responsable de traitement, de désigner parmi les membres de leur personnel, un·e délégué·e à la protection des données, au bénéfice d'une formation spécifique (ou à former), chargé·e de régler les questions courantes de protection des données internes au service et d'être le point de contact pour l'APDI et les administré·e·s.

[74] Ordonnance relative à la loi fédérale sur la protection des données (OLPD) du 14 juin 1993, art. 23 al. 1 :
« *La Chancellerie fédérale et chaque département désignent respectivement et au minimum un conseiller à la protection des données. Ce conseiller a pour tâches de :*
a. conseiller les organes responsables et les utilisateurs ;
b. promouvoir l'information et la formation des collaborateurs ;
c. concourir à l'application des prescriptions relatives à la protection des données. »

Effectuer la démarche d'identification et de classification des données

Le respect des dispositions en matière de protection des données implique pour les responsables de traitement, généralement les entités-métiers, une réflexion approfondie sur leur manière de gérer leurs données et d'organiser leurs systèmes d'informations. Il s'agit d'une part de pouvoir répondre aisément aux demandes des citoyen·ne·s d'accéder à leurs données et d'autre part d'avoir une vision consolidée des données pour garantir les principes de légalité, de finalité, de proportionnalité et de sécurité requis. Cela nécessite un travail important de documentation.

La première étape de cette démarche est l'identification et la classification de tous les types de données personnelles traitées par l'entité. Il s'agit également de mettre en évidence les flux et d'identifier les bases légales permettant leur traitement et leur éventuelle communication. Il s'agit d'élaborer ensuite l'analyse des principes de légalité, de finalité, de proportionnalité, de conservation et de sécurité qu'il conviendra de documenter. Cette démarche s'apparente à celle que les services doivent mener pour la sécurité informatique « *de documenter et d'analyser leur stratégie, leurs processus, leur organisation et leurs besoins fonctionnels* » (art. 12 al. 2 RIC).

Si une partie des éléments sont déjà inclus dans les fiches du registre des fichiers[75], ils sont présentés de manière trop synthétique pour permettre d'identifier clairement le type de données, les variables traitées et leurs flux. En effet, il est essentiel de décrire précisément les données traitées dans chaque fichier ou pour chaque activité, ainsi que de documenter les mesures adoptées pour garantir leur protection.

Identifier toutes les données personnelles ainsi que celles soumises au secret de fonction traitées au sein de l'entité ainsi que leurs flux et documenter les mesures de protection
Constatation n°7
La Cour a constaté que les responsables des huit entités-métiers auditées ont généralement une bonne connaissance « de tête » des différents types de données (personnelles, sensibles et profils de personnalité) ainsi que celles soumises au secret de fonction qu'ils gèrent. Cependant, leur système d'information ne permet pas de les identifier clairement. De plus, il a été constaté que des mesures visant à sécuriser ces données n'ont pas toujours été mises en place et que si elles existent, elles n'ont fait l'objet d'aucune documentation. Aucun des services n'a adopté de politique ou de directives formelles en matière de protection des données.

[75] Voir page 20 pour plus de détails sur le Registre des fichiers.

Recommandation n°7	aux entités-métiers

- Identifier toutes les données (personnelles, sensibles ainsi que les profils de personnalité) traitées dans les fichiers informatiques ou dans les registres papier puis établir, notamment à partir du registre des fichiers selon l'art. 19 LPrD, une cartographie de celles-ci ainsi que de leur flux. Cela s'inscrit dans l'obligation des services de documenter leurs processus (art. 10 al 2 RIC).
- Faire de même avec les données personnelles soumises au secret de fonction, qui sont à définir au préalable.
- Une fois la cartographie des applicatifs et registres contenant ces types de données réalisée, documenter les mesures adoptées pour se conformer à la LPrD (art. 10) et pour assurer la sécurité de ces données en général.
- Vérifier et documenter les bases légales du traitement des données personnelles identifiées.
- Au besoin, compléter le registre des fichiers, si la démarche de documentation a révélé que ce dernier n'était pas complet.

4.2.3 ENTITÉS-MÉTIERS AUDITÉES : DES SITUATIONS INÉGALES CONSTATÉES

Situations non comparables entre entités

Il n'est pas pertinent de comparer les différentes entités auditées entre elles, chaque situation devant être analysée pour elle-même. En effet, toutes ne sont pas de même niveau : directions générales, directions, services et offices dont les responsables n'ont pas le même niveau hiérarchique. De plus, certaines entités ne gèrent qu'un nombre limité de types de données personnelles[76].

Entités dotées d'applications informatiques récentes

On relève de manière générale, que les entités dont la gestion de l'activité est au bénéfice d'une application informatique relativement récente (moins de six ans) ont intégré certains principes de protection des données, comme la gestion des accès. Ceci s'explique par le fait que les principes de protection des données ont été progressivement intégrés à la gestion des projets informatiques de la DGNSI (voir chapitre 4.2.4). En outre, l'APDI est de plus en plus souvent consultée en amont dans le cadre des projets informatiques.

[76] On distingue deux types d'entités : les entités assimilées à des services (les entités « service ») qui disposent d'une certaine autonomie et qui gèrent des activités d'envergure ou un nombre important d'activités (DGEO, OMC, DIRIS, SAN et SEPS) et les entités « office » (constituant un office, une section etc.) qui dépendent d'une entité supérieure (entité « service ») et/ou qui ne gèrent qu'un nombre restreint d'activités ou de tâches (OPS, OCBE, DFAJ).

1. DGEO : bonne intégration des principes de base de protection des données mais formation à renforcer

Les projets de modernisation informatique ont intégré certains impératifs de protection des données

La DGEO est l'entité auditée la plus importante en termes d'effectifs, puisqu'elle comprend 1'186 collaborateur·trice·s employé·e·s au secteur administratif du secrétariat général et des 93 établissements d'enseignement. L'informatique de la DGEO a la particularité d'être gérée par deux entités : la DGNSI pour l'informatique administrative et le Centre de l'informatique pédagogique de l'enseignement obligatoire (CIPEO) pour l'informatique pédagogique.

Les applications informatiques de l'entité ont été modernisées en 2015 pour former le système d'information GIS-EO (Gestion informatisée scolaire pour l'enseignement obligatoire)[77]. Dans le cadre de ce projet informatique transversal à toutes les applications de la DGEO, il a été constaté que les questions de sécurité et de protection des données selon la LPrD ont fait l'objet d'un examen régulier. Ainsi, parmi les entités auditées, la DGEO fait partie de celles qui ont mieux intégré les éléments de protection des données à son activité :

- Gestion ciblée des accès à l'application informatique administrative et pédagogique LAGAPEO (application sous revue pour l'audit)[78].
- Analyses documentées et instructions sur :
  - la gestion des accès aux données LAGAPEO et leur communication par les divers intervenants internes ;
  - la communication aux communes des données LAGAPEO (document communiqué aux établissements afin d'harmoniser les pratiques) ;
  - le type de données pouvant être communiquées en procédure d'appel entre la DGNSI et le CIPEO.
- Suppression de la collecte de données non utiles (comme la religion) dans le système.
- Charte d'utilisation d'Office 365 détaillant les pratiques autorisées et interdites en matière de protection des données.
- Instructions concernant les champs libres de LAGAPEO rendant attentif sur la nécessité de respecter la LPrD et de ne pas y intégrer de données sensibles.

[77] Exposé des motifs et projet de décret accordant au Conseil d'Etat un crédit de CHF 9'369'900.- pour financer la modernisation du système d'information de la Direction générale de l'enseignement obligatoire (DGEO) dans le cadre du programme de Gestion Informatique Scolaire (GIS-EO), décembre 2014.

[78] LAGAPEO - Logiciel d'aide à la gestion administrative et pédagogique de l'enseignement obligatoire - est un des modules de GIS-EO. Mis en place en 2015, il est à disposition des administrations des établissements (directeur·trice·s, doyen·ne·s et secrétaires) pour l'organisation de l'établissement scolaire (classes, groupes, répartition de l'enseignement), le suivi administratif des élèves (enclassement, congés et événements particuliers) et la gestion de l'activité des enseignant·e·s (charge de travail, remplacements). La gestion de l'archivage permettra d'accéder aisément aux éléments du dossier élève archivés. LAGAPEO est une application disponible en ligne par le biais du portail IAM (plateforme de gestion des identités de l'Etat). Cette application peut être utilisée via l'intranet ou par internet, avec une sécurisation renforcée (i.e., authentification forte). Cette application a été développée par un prestataire externe en collaboration avec la DGNSI et des expert·e·s métiers.

Pas de recommandation spécifique autre que les recommandations transversales

Si aucune recommandation spécifique n'est adressée à la DGEO, les recommandations générales sur la formation et la documentation des données la concernent. En effet les représentants de la DGEO ayant participé aux entretiens d'audit, soit le Directeur général et le responsable de l'informatique CIPEO bénéficiaient d'une bonne connaissance des principes de protection des données et affirmaient les intégrer à leur réflexion lors de nouveaux traitements de données. Cependant, de l'avis même de ces derniers, il paraît vraisemblable que tous les collaborateur·trice·s ne soient pas au bénéfice de connaissances suffisantes et qu'un effort de formation serait souhaitable tant pour le personnel administratif que pour le personnel enseignant (recommandation n°1).

En outre, la documentation des applications informatiques, déjà en partie existante, doit être complétée, notamment en indiquant le type de données personnelles traitées, leur flux et la base légale applicable (recommandation n°7).

Nouvelles dispositions relatives au traitement des numéros AVS à respecter

Les nouvelles dispositions de la loi fédérale sur l'assurance-vieillesse et survivants (LAVS) qui devraient entrer en vigueur fin 2021, posent de nouvelles exigences aux services administratifs qui utilisent le numéro AVS pour leurs activités. La loi modifiée en décembre 2020 (pas encore entrée en vigueur à fin 2021), permet aux unités administratives cantonales et communales l'utilisation systématique du numéro AVS, dans la mesure où l'exécution de leurs tâches légales le requiert (art. 153c LAVS). A noter toutefois que les nouvelles dispositions ne permettent pas son utilisation comme code d'authentification.

Mais elle exige la mise en place de mesures organisationnelles et techniques précisées à l'art. 153d LAVS[79]. Des entités telles la DGEO qui collectent le numéro AVS sont soumises à ces dispositions et doivent entreprendre les démarches pour s'y conformer.

Respect des principes de protection des données par les entités externes délégataires

La DGEO délègue certaines tâches publiques à des entités externes à l'administration, comme les mesures MATAS (Modules d'activités temporaires et alternatives à la scolarité)[80]. Bien que ces mesures n'aient pas été retenues pour l'examen de cas concrets dans le cadre de cet audit, la DGEO doit néanmoins s'assurer que les entités délégataires (fondations, associations etc.), respectent les principes de protection dans le traitement des données des élèves qui leur sont confiées et que les contrats ou conventions conclus contiennent bien les clauses adéquates.

[79] Art. 153d de la LAVS « *Mesures techniques et organisationnelles* » (pas encore entré en vigueur) :
« *Les autorités, organisations et personnes habilitées à utiliser le numéro AVS de manière systématique ne peuvent l'utiliser que si elles ont pris les mesures techniques et organisationnelles suivantes :*

a. limiter l'accès aux banques de données qui contiennent le numéro AVS aux personnes qui ont besoin de ce numéro pour accomplir leurs tâches et restreindre en conséquence les droits de lecture et d'écriture dans les banques de données électroniques contenant ce numéro ;

b. désigner une personne responsable de l'utilisation systématique du numéro AVS ;

c. veiller à ce que les personnes autorisées à accéder aux données soient informées, dans le cadre de formations et de perfectionnements, que le numéro AVS ne peut être utilisé qu'en rapport avec leurs tâches et ne peut être communiqué que conformément aux prescriptions légales ;

d. garantir la sécurité de l'information et la protection des données en fonction des risques encourus et conformément à l'état de la technique ; veiller en particulier à ce que les fichiers de données qui comprennent le numéro AVS et qui transitent par un réseau public soient cryptés conformément à l'état de la technique ;

e. définir la manière de procéder en cas d'accès non autorisé aux banques de données ou d'utilisation abusive de celles-ci. »

[80] Les mesures MATAS visent à prendre en charge des élèves présentant des difficultés durables de comportement, associées la plupart du temps à un risque de rupture scolaire. Le but de la mesure, prévu par le cadre légal, est de favoriser la poursuite de la scolarité de l'élève, en principe dans la classe et l'établissement d'origine de l'élève. Le nombre de ces structures a rapidement augmenté dans le canton. On en compte aujourd'hui 21, réparties entre les huit régions scolaires.

2. OPS : culture de la confidentialité bien intégrée mais formalisation nécessaire de l'accord parental pour la communication de données

Le personnel de l'OPS bien sensibilisé à la confidentialité des données

Deuxième entité auditée en termes d'effectifs (450 collaborateur·trice·s), l'Office de psychologie scolaire (OPS) a pour mission principale d'assurer une offre cantonale en matière de psychologie, psychomotricité et logopédie en milieu scolaire (PPLS) pour les élèves de l'école obligatoire[81].

Les données traitées par l'OPS concernent la situation thérapeutique des élèves recourant aux prestations PPLS et sont donc sensibles. Les dossiers individuels PPLS sont enregistrés actuellement sous forme papier (journal des interventions) et sont stockés dans des armoires fermées à clé situées dans les locaux des établissements scolaires spécifiquement dédiés aux activités PPLS.

La Cour relève que la culture de la confidentialité des données sensibles est bien implantée dans les milieux PPLS. Ces professionnel·le·s sont soumis·e·s au secret professionnel au sens de l'art. 321 CP au même titre que les médecins notamment[82] et ont été sensibilisé·e·s à cette thématique au cours de leur formation.

Par ailleurs les codes de déontologie des psychologues, psychomotriciens et logopédistes intègrent les principes de protection des données et du secret de fonction.

De plus, la protection des données personnelles fait l'objet d'un chapitre spécifique dans la loi sur la pédagogie spécialisée, qui contient des articles sur la collecte, les accès, la transmission ainsi que sur la conservation des données (articles 63 à 65 LPS) ; tout comme le calendrier de conservation des archives de cette entité intègre une réflexion liée à la protection des données.

Nouvelle application informatique en cours

L'application informatique actuelle de l'OPS est obsolète. Le futur système d'information, commun à tout le Service de l'enseignement spécialisé et de l'appui à la formation (SESAF), le GI-PSAF[83] vise à intégrer les impératifs de protection des données selon la LPrD. En particulier, déterminer et organiser la gestion des accès des différents intervenants aux informations PPLS. Cette mesure fait l'objet d'une recommandation de la Cour, formulée dans le cadre de l'audit sur l'Office cantonal d'orientation scolaire et professionnelle (OCOSP)[84], concerné par le projet[85].

---

[81] Les autres missions de l'OPS sont : autoriser et administrer les prestations de logopédie indépendante (0-20 ans) ; appuyer la mission de formation de l'école et soutenir les établissements scolaires dans leurs missions ; et collaborer avec les partenaires externes dans la recherche de solutions d'aide aux enfants et adolescents.

[82] L'article 321 du Code pénal stipule que les professionnels (des domaines cités dans l'article dont les psychologues et ergothérapeutes ainsi que leurs auxiliaires) qui « *auront révélé un secret à eux confié en vertu de leur profession ou dont ils avaient eu connaissance dans l'exercice de celle-ci, seront, sur plainte, punis d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire* ».

[83] Exposé des motifs et projet de décret accordant au Conseil d'Etat un crédit d'investissement de CHF 8'705'000 pour financer la Gestion Informatisée de la Pédagogie Spécialisée et de l'Appui à la Formation (GI-PSAF), avril 2019

[84] Audit de la Cour des comptes n°57 de 2019

[85] Recommandation n°8 de l'audit n°57 « *a) Développer un concept de sûreté de l'information et de protection des données qui devrait notamment comprendre les éléments suivants :*

1. *Harmonisation de la collecte d'informations personnelles sur l'ensemble du territoire ;*
2. *Harmonisation de la procédure de conservation et de destruction des données personnelles ;*
3. *Réalisation d'un audit périodique sur le contenu des dossiers et des notes personnelles ;*
4. *Formation des collaborateurs aux exigences de la LPrD et du règlement y relative ;*
5. *Conformément à l'art. 20 LOPro, détermination des catégories de données que le Service est habilité à traiter dans le système d'information, ainsi que des règles et limites d'accès (Département).* »

Autorisation pour la communication de données à formaliser par écrit

La Cour formule néanmoins une recommandation à l'OPS concernant la transmission des informations liées au dossier PPLS des élèves. L'article 63 de la LPS relatif à la transmission des données précise en effet que « *la transmission de données sensibles au sens de la loi du 11 septembre 2007 sur la protection des données personnelles (LPrD) ne peut se faire entre professionnels impliqués dans la prise en charge en principe qu'avec l'accord des parents, voire de l'élève* ».

Or la traçabilité de l'accord n'est pas assurée, ce dernier étant recueilli oralement. La Cour estime que la communication de ces données sensibles devrait être cadrée par un document écrit et signé au moins par les parents ou par l'élève si ce dernier a la capacité de discernement suffisante. L'existence d'un tel document aurait également pour avantage d'expliquer précisément aux parents l'usage effectué des informations obtenues et d'exposer les mesures qui les sécurisent.

Recueillir l'accord par écrit en cas de communication de données sensibles entre professionnel·le·s impliqué·e·s dans la prise en charge de l'élève
Constatation n°8
La loi sur la pédagogie spécialisée exige que toute communication de données personnelles sensibles traitées dans le cadre de la prise en charge des élèves en matière de pédagogie spécialisée, à d'autres professionnel·le·s impliqué·e·s dans le processus, se base sur l'accord parental, voire de l'élève. L'accord est cependant demandé oralement ce qui ne permet pas d'en assurer la preuve.
Recommandation n°8 à l'Office de psychologie scolaire (OPS)
En cas de communication de données personnelles sensibles entre professionnel·le·s impliqué·e·s dans la prise en charge de l'élève en matière de pédagogie spécialisée, recueillir l'accord par écrit des parents, voire de l'élève, pour assurer une traçabilité des dispositions prévues à l'art 63 al. 1 LPS.

De surcroît, les recommandations générales sur la formation et la documentation en matière de LPrD s'appliquent également à l'Office de psychologie scolaire (OPS).

3. SAN : questions de protection des données régulièrement abordées, mais adaptation nécessaire des documents contractuels

Système d'information complexe mais processus hautement informatisés et bien documentés

Troisième entité auditée en termes d'effectifs (241 collaborateur·trice·s), le Service des automobiles et de la navigation (SAN) exerce différentes missions[86]. Pour gérer toutes les informations relatives à l'admission des véhicules et des personnes à la circulation routière et à la navigation, aux sanctions, à la perception des taxes et redevances et à la gestion des finances du service, le SAN utilise l'application centrale VIACAR. Il gère ainsi des données personnelles sensibles que sont les données médicales, celles relatives aux sanctions et au contentieux. L'application VIACAR, commune à plusieurs cantons est gérée par une société externe, basée en Suisse, avec laquelle les services des automobiles cantonaux signent un contrat.

Le système d'information du SAN, centré autour de VIACAR, est complexe et a déjà fait l'objet de différentes modernisations depuis 2013[87]. Il contient un certain nombre d'interfaces y compris pour alimenter la base de données fédérale du Système d'information relatif à l'admission à la circulation (SIAC) prévu par la loi sur la circulation routière (LCR). Une cartographie des applications du SAN a été établie en collaboration avec la DGNSI (via l'applicatif Cartomega) de même qu'une documentation très détaillée relative aux différents processus (fils rouges). Les processus du SAN sont hautement informatisés, ce service vise en effet à moyen terme une gestion « zéro papier ».

Impératifs principaux de protection des données intégrés mais documentation à compléter

Les impératifs de protection des données sont, de manière générale, pris en compte : gestion segmentée des accès et journalisation des opérations dans VIACAR, plateforme sécurisée E-medko d'échanges de données médicales avec les médecins privés. On relève que, sur la base des informations extraites des opérations de journalisation, le SAN effectue régulièrement des contrôles sur les opérations réalisées par les collaborateur·trice·s et vérifie qu'il·elle·s n'ont pas accédé à des informations non nécessaires à leur tâche.

Il s'agit de la seule entité auditée ayant déclaré avoir été sollicitée par une personne qui a demandé à avoir accès à ses propres données. Le SAN a également fait l'objet d'une intervention de l'APDI pour demander l'anonymisation des fils rouges, qui contenaient des exemples nominatifs réels. Les informations relatives aux tests médicaux auxquels doivent se soumettre les conducteurs âgés de 70 ans et plus, ont fait l'objet d'interrogations en matière de protection des données et de secret médical auxquelles le SAN a dû apporter des justifications[88].

Une membre de l'état-major du SAN a suivi la formation en protection des données du CEP et sollicite l'APDI pour des questions en la matière.

Un travail de documentation spécifique à la protection des données est toutefois encore à réaliser pour les applications du SAN en référence à la recommandation générale n°7, ainsi que la formation de l'ensemble des collaborateur·trice·s (recommandation n°1).

---

[86] Les missions principales du SAN sont l'admission des véhicules à la circulation routière, l'admission des conducteurs à la circulation, la perception des taxes et redevances liées au trafic routier, la sanction des conducteurs qui commettent des infractions à la LCR (loi sur la circulation routière) et l'admission des conducteurs de bateaux et les bateaux à la navigation.

[87] Exposé des motifs et projet de décret accordant au Conseil d'Etat un crédit d'investissement de CHF 6'440'000.- pour financer la modernisation du système d'information du Service des automobiles et de la navigation, juin 2013.

[88] Source : « Le test des seniors ébranle le secret médical », journal 24 Heures du 07.09.2016.

Clauses contractuelles à compléter

Conformément au RIC[89], le contrat avec la société VIACAR AG a été signé par la DGNSI et le SAN. Les clauses contractuelles se réfèrent aux conditions générales pour les prestations informatiques de la Conférence suisse pour l'informatique (CSI). Si ces dernières mentionnent l'obligation de garder le secret de fonction et de respecter les dispositions en matière de protection des données, elles ne précisent toutefois pas que les données doivent être hébergées en Suisse. Une des conditions contractuelles minimales exposées au point 3.2.3 de ce rapport manque donc d'où la recommandation suivante adressée au SAN.

Compléter les dispositions contractuelles liés à l'application VIACAR afin de garantir l'hébergement des données en Suisse
Constatation n°9
L'application VIACAR utilisée par le SAN vise à gérer l'admission des véhicules et des personnes à la circulation routière et à la navigation, ainsi qu'à percevoir les taxes et les redevances. Elle contient des données personnelles sensibles. Cette application est utilisée par plusieurs cantons. Elle fait l'objet d'un contrat signé par les représentant·e·s de chaque canton et la société VIACAR AG, auquel sont annexées les conditions générales de la Conférence suisse sur l'informatique (CSI). Il est indiqué que des dispositions particulières peuvent y être rajoutées, ce qui n'a pas été le cas. Or, les conditions générales ne prévoient pas d'exiger que les données soient hébergées en Suisse, ce qui est une nécessité en cas de traitement de données soumises au secret de fonction.
Recommandation n°9 au Service des automobiles et de la navigation (SAN)
Dans le cadre des dispositions contractuelles liées au mandat de gestion de l'application informatique traitant la gestion de l'admission des véhicules et des personnes à la circulation routière et à la navigation du SAN, compléter les conditions générales de la CSI avec une clause précisant l'obligation d'héberger les données en Suisse.

[89] Règlement relatif à l'informatique cantonale (RIC) du 21 janvier 2009

4. DIRIS : politique de protection des données à mettre en place et nécessité de structurer et documenter les données selon ces principes

Un certain nombre de domaines différents traités

La Direction de l'insertion et des solidarités (DIRIS) est une des deux sections de la Direction générale de la cohésion sociale (DGCS). Elle a la charge de l'appui social à tous les groupes de population ou individus qui en ont besoin à un moment donné de leur parcours de vie. Elle comprend le Centre social d'intégration des réfugiés (CSIR)[90] qui emploie 80 personnes (73.9 ETP) ainsi que trois pôles employant 26 personnes au total (22.6 ETP) :

- Le pôle « Prévention et solidarités » s'occupe de la prise en charge des victimes de violence, de l'appui aux bénéficiaires de prestations complémentaires à l'AVS/AI hébergés en logements protégés, du soutien aux proches-aidant-e-s, de la lutte contre le surendettement et du développement des solidarités sous toutes ses formes.
- Le pôle « Appui social et orientation » gère le fonds cantonal de lutte contre la précarité, fournit des prestations d'appui et d'orientation dans le cadre du programme de formation pour jeunes adultes en difficulté (FORJAD), est responsable du financement des structures d'hébergement d'urgence du canton, du pilotage de la Centrale des Solidarités (« orientation accompagnée » de la population vaudoise en situation de vulnérabilité) et de la formation des assistant·e·s sociaux·ales des régions d'action sociale.
- Le pôle « Insertion socio-professionnelle » gère le dispositif des mesures d'insertion des bénéficiaires du RI non suivis par les ORP et celles visant l'insertion des jeunes adultes émargeant au RI (suivi des bénéficiaires, bilan des mesures et facturation, gestion des relations avec les mandataires externes chargés d'assurer le suivi social des bénéficiaires, etc.).

Pas d'application informatique-métier spécifique à la DIRIS

Contrairement à la majorité des autres entités-métiers auditées, l'activité de la DIRIS, centrée sur l'appui et la prise en charge sociale ou la gestion de partenaires externes délégataires de tâches publiques, n'est pas soutenue par des processus automatisés, tel que l'octroi de bourses d'études, de permis de conduire ou d'autorisations de circuler.

Il n'y a donc pas d'application informatique spécifique à la DIRIS, à l'exception de l'application MAORI[91] qui a remplacé l'application PROGRES en juin 2021 et qui depuis, permet notamment de segmenter les accès et d'intégrer le « journal social » qui contient les informations relatives au suivi social des bénéficiaires.

Obstacles techniques à une gestion conforme en matière de protection des données

Contrairement à d'autres entités, la DIRIS n'est pas équipée d'une gestion électronique des documents (GED) permettant la segmentation des accès et la journalisation des opérations (traçabilité des accès). A l'exception de celles gérées dans MAORI, les données traitées par le service sont donc enregistrées sur le serveur de l'Etat, sous forme *PDF*, *WORD* ou *EXCEL*.

[90] Le CSIR est compétent pour offrir un appui social et octroyer le revenu d'insertion aux réfugié·e·s admis·es en Suisse (permis B et permis F), conformément à la loi sur l'action sociale vaudoise (LASV). Dans le cadre de l'appui social qu'il fournit aux bénéficiaires, le CSIR propose des activités et programmes en lien avec le monde professionnel.

[91] Cette application traite entre autres les données pour l'octroi du revenu d'insertion (RI) des personnes émargeant à l'aide sociale et utilisée par le CSIR, chargé de l'octroi du RI aux réfugié·e·s. Elle a remplacé PROGRES qui était un logiciel ancien ne répondant plus aux impératifs de protection et de sécurité des données.

Or les serveurs de l'Etat ne permettent pour l'heure qu'une segmentation des accès sur trois niveaux seulement. La DGCS a bien établi un plan d'accès pour ses différentes entités, mais seul un niveau est segmentable par sous-entité. Cela signifie que tous les collaborateur·trice·s du CSIR ont toutes et tous les mêmes accès.

En outre, les collaborateur·trice·s s'échangent des messages et documents contenant souvent des données personnelles sensibles via la messagerie standard de l'Etat. Il n'y a pas eu de sensibilisation à l'utilisation de la plateforme sécurisée « *Partage* »[92]. Elle nécessite toutefois une inscription préalable de l'expéditeur et du destinataire et la transmission d'un mot de passe. Néanmoins, ni l'identification des problèmes de sécurité ni l'inadéquation des outils à disposition n'ont fait l'objet d'une requête auprès de la DGNSI (voir recommandation n°2).

Concept de protection des données à créer et politique à mettre en place

Si les collaborateur·trice·s de la DIRIS sont manifestement sensibilisé·e·s à l'aspect confidentiel des informations traitées, la protection des données n'a pas véritablement été intégrée au mode de gestion des activités de l'entité. Cette situation s'explique en partie par l'absence d'application informatique spécifique, dont la mise en place a, dans d'autres entités auditées, mené à une réflexion sur certains impératifs de protection et de sécurité des données (segmentation et journalisation des accès, type de données à traiter, degré de confidentialité, etc.).

Dans cette entité, il conviendrait de mettre un place une politique de protection des données qui règle les questions de conflit entre la nécessité de collecter et partager des informations, souvent sensibles et celle de les protéger en les gardant confidentielles. Une réflexion sur la conservation des données doit également être menée tout comme il faudrait anonymiser les données personnelles sensibles, figurant dans des fichiers utilisés à des fins de recherche.

Important travail documentaire à réaliser et registre des fichiers à compléter

La Cour est consciente que l'élaboration d'une politique de protection des données implique un important travail pour cette entité (voir la recommandation n°7 « *Identifier toutes les données personnelles ainsi que celles soumises au secret de fonction traitées au sein de l'entité ainsi que leurs flux et documenter les mesures de protection* »).

Le travail d'élaboration des fiches du registre des fichiers est en cours pour les entités de la DGCS. Le projet, qui n'a pas encore été validé par l'APDI a été transmis à l'équipe d'audit de la Cour. La DIRIS n'a pas prévu de déclarer le « Journal social » du CSIR comme fichier séparé de l'application MAORI. La Cour estime toutefois que dans le cas du CSIR, compte tenu du contenu très sensible et détaillé des informations figurant dans le Journal social, ce dernier devrait faire l'objet d'une déclaration séparée.

[92] Le service Partage.vd.ch répond aux besoins d'accès mobiles et d'échanges sécurisés de fichiers bureautiques avec des partenaires internes ou externes à l'Administration cantonale vaudoise (ACV). Cet outil est mis à disposition par la DGNSI et hébergé sur ses infrastructures.

Annoncer le système d'information relatif au suivi social des réfugié·e·s géré par le Centre social des réfugiés (CSIR) au registre des fichiers de l'APDI
Constatation n°10
La LPrD précise à l'art. 19 al. 1 que « *Le Préposé cantonal à la protection des données et à l'information tient un registre des fichiers, qui est public et accessible en ligne*. » Toutes les entités de l'ACV n'ont pas encore déclaré leurs fichiers définitifs à l'APDI, dont la Direction générale de la cohésion sociale (DGCS) à laquelle est rattachée la DIRIS. Un projet a toutefois été préparé, mais dans lequel ne figure pas le système d'information relatif au suivi social des personnes prises en charge par le Centre social des réfugiés (CSIR). Si les coordonnées individuelles sont intégrées à l'application PROGRES, déclarée dans le projet de registre des fichiers DGCS, le CSIR collecte des informations structurées supplémentaires figurant dans le « journal social » tenu à jour pour chaque bénéficiaire. Or ces informations répondent à la définition de fichier au sens de la LPrD et du manuel d'utilisation établi par l'APDI.
Recommandation n°10 à la Direction de l'insertion et des solidarités (DIRIS)
Déclarer tous les fichiers correspondant à la définition de l'art. 4 LPrD, notamment le système d'information relatif au suivi social des réfugié·e·s géré par le Centre social des réfugiés (CSIR), à l'APDI pour intégration au registre des fichiers prévu à l'art. 19 al. 1 LPrD.

Convention avec les délégataires de tâche publique à compléter

A l'instar d'un certain nombre d'entités de l'ACV, la DIRIS délègue une partie de ses missions à des entités externes à l'ACV : notamment le suivi social des bénéficiaires FORJAD via une convention signée entre les parties. Or si cette dernière comprend bien une clause de respect de la LPrD, aucune ne mentionne le secret de fonction.

Il faut préciser que l'entité délégataire d'une tâche publique n'est pas considérée, selon la LPrD, comme un sous-traitant, mais comme un nouveau responsable du traitement, lui-même soumis à la législation. Dès lors, et même si les dispositions ne l'exigent pas formellement comme en cas de sous-traitance, la Cour est d'avis que l'entité délégatrice doit s'assurer que le délégataire ait bien adopté les mesures adéquates en matière de protection et sécurité des données.

Compléter la convention de délégation d'une tâche publique à des entités externes avec une clause sur le respect du secret de fonction
Constatation n°11
La DIRIS délègue la tâche de suivi social des bénéficiaires d'un programme d'insertion professionnelle à des entités externes à l'Etat. Cette délégation fait l'objet d'une convention de collaboration entre la Direction générale de la cohésion sociale et l'organisme prestataire, précisant la nécessité de se conformer à la LPrD et à la LPD. Elle ne comprend toutefois pas de clause liant l'organisme prestataire au secret de fonction.

Recommandation n°11	à la Direction de l'insertion et des solidarités (DIRIS)
Compléter la convention de collaboration liant la Direction générale de la cohésion sociale et l'organisme prestataire lui délégant la tâche de mesures de suivi dans le cadre du programme de formation pour les jeunes adultes en difficulté (FORJAD) en précisant la nécessité de respecter le secret de fonction.	

5. OMC : Application des principes de protection des données à harmoniser dans les différents domaines traités et application TAO à sécuriser

Doté de 42 collaborateur·trice·s, l'Office du médecin cantonal (OMC) est en charge des missions confiées par la loi sur la santé publique (LSP) : *« le médecin cantonal est le médecin référent de l'administration cantonale. Il est responsable des questions médicales concernant la santé publique (…)* et notamment *(…) de l'organisation et de la mise en œuvre des mesures à prendre en cas d'événement particulier ou de catastrophe (ORCA sanitaire)* » (art.7 LSP). Ce domaine d'activité est très large : « *il intervient notamment dans la lutte contre les maladies transmissibles, la gestion des autorisations, les droits des patients, la protection des populations vulnérables, le respect de l'éthique, la gestion de crises sanitaires et la santé environnementale* [93]».

Le registre des fichiers (voir page 20) recense 14 fichiers pour l'OMC[94] qui pour certains traitent de données de nature à la fois médicale et pénale. Néanmoins, le Registre des fichiers ne contient pas les dossiers ou informations contenant des données personnelles et sensibles qui ne sont pas structurées en fichier. Par exemple en cas de décès d'un médecin établi dans le canton ou de départ à la retraite sans remise de cabinet, tous les dossiers médicaux détenus par ces médecins sont transférés dans les archives de l'OMC où ils sont stockés, ce qui représente un grand nombre de dossiers.

Le secret médical assure une certaine protection mais ne couvre pas toutes les exigences LPrD

Au cours des entretiens, les responsables de l'OMC ont admis que, selon eux·elles, les milieux médicaux avaient pris un certain retard pour intégrer les principes de la LPrD. Néanmoins, ce domaine étant couvert par le secret médical, qui entre dans le cadre du secret professionnel régi par l'art. 321 du Code pénal, un certain niveau de protection était assuré par ce biais. Or, la généralisation du traitement et de l'échange numérique des données médicales a créé de nouveaux risques en matière de sécurité et de confidentialité des données, que le seul secret médical ne suffit pas à pallier.

[93] Source : site internet de l'ACV

[94] Demandes d'exhumation de dépouille mortelle, gestion des annonces MEDREG (registre des professionnels de la santé), gestion des enquêtes du Conseil de santé (faits signalés, instruction, plénières et décision), gestion des demandes de levées de secret médical des professionnels de la santé, gestion des membres du Conseil de santé, gestion des courriers de mise en garde des professionnels de la santé ayant commis une infraction pénale d'importance moyenne et n'ayant aucun lien avec leur profession, GPECS : recensement des données relatives aux signalements et plaintes reçues à l'Office du médecin cantonal), GPECS : recensement et gestion des données relatives aux enquêtes du Conseil de santé, gestion du suivi de la COP (Commission d'examen des plaintes des patients, résidents ou usagers d'établissements sanitaires et d'établissements socio-éducatif), maladies transmissibles : surveillance, contrôle et intervention des déclarations obligatoires, plateforme de gestion des traitements agonistes opioïdes (traitement de substitution), procès-verbaux des séances du Conseil de santé, PROGRES: autorisations de pratiquer et d'exploiter (recensement des professionnels de la santé au bénéfice d'une autorisation de pratiquer et recensement des établissements sanitaires du canton de Vaud soumis à autorisation d'exploiter), registre des mesures de protection.

La Cour relève que si le secret médical autorise la communication de données médicales entre médecins, elle doit cependant respecter le principe de légalité requis par la LPrD. Au cours des entretiens, une certaine confusion régnait entre ces deux notions, ce qui témoigne à nouveau de la nécessité de renforcer les connaissances en matière de protection des données (recommandation n°1).

La recommandation n°7 représente un important travail pour l'OMC

Les responsables de l'OMC ont déclaré avoir conscience de l'ampleur de la tâche à effectuer afin de mettre tous leurs dossiers tant papiers que numériques, en conformité avec les dispositions de la LPrD. Cet office détient en effet un volume important de documents qui n'ont donc pas été organisés et traités selon les principes de cette législation. Cela concerne tant les données archivées qu'actuelles (à l'exception de celles traitées dans les applications informatiques récentes).

Ainsi, la recommandation n°7 qui prévoit une démarche d'identification et de documentation de toutes les données personnelles gérées et de leur flux[95], ainsi que d'élaboration d'une stratégie et politique de protection et de sécurisation des données, représente un travail très important pour cette entité.

Besoin de sécurisation spécifique pour les échanges de courriers électroniques

Le médecin cantonal est en outre très fréquemment sollicité directement par des citoyen·ne·s ou des entités externes pour des problèmes individuels en lien avec les questions de santé publique. Les échanges téléphoniques ou par courriers électroniques qui résultent de ces contacts contiennent tous par essence des données personnelles sensibles. Il existe clairement un besoin particulier de sécurisation pour ces échanges. Etant donné le grand volume d'échanges, réalisés souvent par téléphone portable, la solution de chiffrement proposée actuellement par la DGNSI est trop lourde pour être praticable par l'office[96].

Ce besoin, qui relève de la sécurité informatique, est à identifier par l'OMC (dans le cadre de la recommandation n°7) et, conformément à l'art. 10 al. 1 RIC, à transmettre ensuite à la DGNSI.

Nécessaire protection des données en cas d'envois de courriers électroniques multiples

L'Office du médecin cantonal a en outre commis une erreur en ne masquant pas les adresses des destinataires d'un courriel groupé à près de 300 destinataires, en lien avec la vaccination contre la COVID-19[97]. Cet évènement ayant eu lieu après l'exécution de cet audit, la Cour ne formule aucune recommandation formelle mais partage l'avis que ces envois multiples doivent expressément être effectués en « en copie cachée ».

[95] Dans le cas de l'OMC qui a déjà fourni des informations au registre des fichiers, il s'agit d'identifier toutes les autres données personnelles et sensibles, qui ne sont pas organisées sous forme d'un fichier structuré, mais qui doivent néanmoins être traitées et organisées selon les principes de la LPrD.

[96] La solution de chiffrement proposée actuellement par la DGNSI consiste à chiffrer le contenu du message et les pièces jointes via l'application zip contenant un mot de passe. Ce dernier est à transmettre via un autre mode de transmission (courriel par ordinateur si le message a été envoyé par téléphone ou vice-versa).

[97] « Vaud fait fuiter des centaines d'e-mails », article de 20 Minutes du 27 octobre 2021.

Les applications récentes intègrent des impératifs LPrD mais généralement pas les autres

L'audit n'a procédé qu'à l'examen sommaire de deux applications de l'OMC, toutes deux assez anciennes[98]. Ces applications concernent tout d'abord la gestion des autorisations de pratiquer (pour les médecins), dont les données sont traitées dans un module de l'applicatif PROGRES. Ce dernier, très ancien puisqu'il a été mis en œuvre en 1995, n'a pas été structuré pour respecter les dispositions de la protection des données. Il est cependant en cours de remplacement par un nouvel applicatif DEMAUT[99]pour lequel il est prévu d'intégrer ces impératifs.

Application TAO à sécuriser

L'autre application est la plateforme internet gérant la distribution des traitements de substitution aux opioïdes aux bénéficiaires, sur la base d'une ordonnance émise par un médecin et accessible par les pharmacies distributrices. Elaborée par la HEIG-VD sur mandat de l'OMC, cette application informatique a été adoptée par 20 cantons. Géré de manière centralisée à Unisanté[100] pour le canton de Vaud, qui agit sur mandat de l'OMC sur la base d'un contrat de prestation annuel, l'applicatif a permis d'améliorer l'efficacité du processus et de sécuriser le circuit de distribution.

Toutes les règles de sécurité, de confidentialité et les exigences LPrD ne sont toutefois pas respectées :

- Si la demande d'un médecin d'intégrer la plateforme est gérée de manière centralisée par Unisanté, les départs sont traités en majorité par les centres de traitement. Il n'y a donc pas de liste des intervenant·e·s en fonction. Pour la Cour, il est nécessaire de tenir une liste des intervenant·e·s à jour pour garantir la sécurité du fonctionnement de la plateforme et établir une procédure de contrôle centralisée à Unisanté ou à l'Office du médecin cantonal (ou à Unisanté et supervisée par l'OMC).
- Les contrats avec Unisanté et le prestataire informatique ne contiennent ni de clauses du respect de la LPrD ni de clauses du secret de fonction.
- Le contrat de développement de l'application TAO, signé avec le prestataire externe n'a pas, conformément aux exigences du RIC, été signé par la DGNSI bien que l'OMC ait déclaré être le responsable du traitement. Aucune analyse de sécurité n'a donc pu être menée par les services de l'Etat. Cette application, qui contient des données hautement sensibles, devrait être examinée sous cet angle par les responsables de la sécurité informatique de l'Etat.
- Enfin, il convient également de régler la question de l'identification du responsable du traitement. Il s'agit de déterminer si Unisanté doit être considéré comme un sous-traitant ou le délégataire d'une tâche publique, et dès lors, désigné comme responsable du traitement. Il s'agira ensuite d'adapter les contrats en conséquence.

[98] Néanmoins, d'autres ont été abordées dans la discussion générale lors des entretiens. Il s'avère que les applications récentes, comme GPECS par exemple, qui est une application pour la gestion des plaintes réalisée par la DGNSI, intègrent les impératifs basiques de protection et de sécurité en matière de gestion segmentée des accès et de journalisation. Par contre ce n'est pas le cas pour d'autres activités de l'office, gérées soit via des fichiers enregistrés directement sur le serveur, soit via des applicatifs plus anciens.

[99] Voir exposé des motifs et projet de décret accordant au Conseil d'Etat un crédit d'investissement de CHF 7'114'000.- pour financer le renouvellement du système d'information de l'Office du médecin cantonal, juillet 2020.

[100] Unisanté, centre universitaire de médecine générale et santé publique à Lausanne, est formé de la Policlinique médicale universitaire, l'Institut universitaire de médecine sociale et préventive, l'Institut universitaire romand de santé au travail, l'association Promotion Santé Vaud et la Fondation vaudoise pour le dépistage du cancer.

Renforcer les mesures de sécurité de la plateforme internet des traitements agonistes opioïdes (TAO)	
Constatation n°12	
La plateforme des traitements agonistes opioïdes (TAO) permet de mettre en lien des médecins et des pharmacies afin d'assurer la distribution de traitement de substitution aux patient·e·s qui en ont besoin. Cette mission est de la responsabilité de l'OMC qui a délégué la gestion de TAO à Unisanté, via un contrat de prestation. C'est toutefois l'OMC qui a signé le contrat pour de développement de l'application informatique, alors que le RIC prévoit que c'est la DGNSI qui gère les contrats avec les fournisseurs pour l'ACV (art. 21 al. 1 RIC). Ni le contrat avec le prestataire informatique, ni celui avec Unisanté ne contiennent de clauses de respect de la LPrD et du secret de fonction. La déclaration de confidentialité individuelle que l'OMC fait signer aux prestataires fait référence au secret de fonction. En outre, l'application TAO ne respecte pas tous les principes de sécurité, en particulier celui de la gestion des accès. La gestion des entrées dans le système est certes centralisée, mais Unisanté ne tient aucune liste des ayants droit actifs, cette tâche étant déléguée aux quatre centres de traitement qui gèrent les sorties.	
Recommandation n°12	**à l'Office du médecin cantonal (OMC)**
Renforcer les mesures de sécurité de l'application informatique TAO et, lors du renouvellement des contrats liés à cette application, les adapter conformément au RIC et à la LPrD : • Faire signer le contrat informatique par la DGNSI, cette dernière étant responsable selon le RIC de la gestion des relations avec les fournisseurs. • Intégrer une clause de respect de la LPrD et du secret de fonction dans le contrat informatique et dans le contrat de prestation avec Unisanté. • Clarifier la question de la responsabilité du traitement entre l'OMC et Unisanté. • Centraliser la gestion des accès (entrées ET sorties).	

6. OCBE : Processus automatisé et informatisé et bonne intégration des principes de protection des données

Un seul domaine géré, mais avec plusieurs types de données personnelles sensibles

L'Office cantonal des bourses d'étude et d'apprentissage (OCBE) est rattaché à la Direction des aides et des assurances sociales (DIRAAS), l'une des trois directions qui composent la Direction générale de la cohésion sociale (DGCS).

L'OCBE octroie des bourses d'études ou d'apprentissage lorsque la situation financière d'une personne ou celle de ses parents ne suffit pas à financer une formation après l'école obligatoire.

Les bourses ne sont pas remboursables, sauf en cas d'abandon injustifié de la formation ou d'aides perçues indument ou détournées. Et lorsque les critères pour obtenir une bourse d'études ou d'apprentissage ne sont pas remplis, la personne peut également solliciter un prêt[101].

L'octroi d'une bourse d'étude fait partie des mesures d'aides individuelles découlant des législations sociales et constitue donc une donnée personnelle sensible au sens de l'art. 4 al. 2 chiffre 2 LPrD. D'autres données sensibles sont également collectées par l'OCBE, telles que des données médicales, ou des justificatifs de situation familiale. Si les informations sur le revenu ne sont certes pas considérées comme sensibles au sens de la LPrD, elles sont néanmoins délicates.

Application informatique avec bonne gestion segmentée des accès

Les processus d'octroi sont complexes, mais le calcul est entièrement automatisé via une application informatique appelé « Logiciel Bourse (LB) ». Deux bases de données alimentent, entre autres, les applications « *Filemaker* bourse » et « *Filemaker* étudiant ». Les documents sont enregistrés dans une GED sécurisée mise en place par la DGNSI.

Les dossiers sont attribués aux gestionnaires via un échéancier *FILEMAKER*. L'accès aux autres dossiers est toutefois possible et est justifié par l'entité, d'une part, en raison du processus de validation avant décision (contrôle interne des quatre yeux) et, d'autre part, au vu d'impératifs organisationnels visant à pallier l'éventuelle absence d'un·e collaborateur·trice sans que le traitement de la procédure administrative en pâtisse ou soit ralenti.

Bases légales adaptées pour la collecte et l'échange de données sensibles avec les autres services

Si la base légale qui fonde la mission de l'OCBE, la loi sur l'aide aux études et à la formation professionnelle (LAEF) du 1er juillet 2014, contient des dispositions réglant la collecte, la transmission et l'échange de données personnelles sensibles, aucune ne mentionne la Direction de l'enfance et de la jeunesse (DJEJ) avec laquelle il existe pourtant une communication régulière d'informations (voir note n°60 p. 40).

Cas de rigueur traités de manière confidentielle

Le processus d'octroi des bourses prévoit également de traiter des cas de rigueur. Ils font l'objet d'un examen par le bureau de la commission cantonale des bourses d'études. Des documents contenant souvent des données personnelles sensibles sont fournis aux membres de la commission. Hors situation pandémie, les documents sont remis et consultés lors de la séance et ne sont pas transmis à l'extérieur des locaux de l'OCBE. Durant la période de télétravail forcé dû à la COVID-19, les documents ont toutefois été envoyés via la messagerie électronique.

Besoin d'une plateforme sécurisée pour l'échange de données personnelles sensibles

A l'instar d'autres entités comme l'OMC ou la DIRIS, l'OCBE échange des informations et des fichiers contenant des données personnelles sensibles par messagerie électronique, soit avec des personnes externes, soit avec d'autres entités étatiques. Lors de l'entretien d'audit, les représentants de l'OCBE ont fait part de leur besoin de pouvoir disposer d'une plateforme sécurisée. Ce besoin renvoie à la recommandation n°2 relative à la définition par le service de ses besoins en matière de sécurité informatique et leur transmission à la DGNSI.

[101] Le montant de la bourse ou du prêt est fixé d'après un budget comprenant les charges forfaitaires (logement, entretien, assurances, frais médicaux et dentaires, frais de garde, impôts, loisirs et frais de formation) et les ressources du·de la requérant·e, ainsi que celles des membres de sa cellule familiale. Les ressources sont déterminées en fonction du revenu déterminant unifié (RDU), montant calculé sur la base du revenu et de la fortune, selon des modalités unifiées, permettant de déterminer l'octroi des prestations sociales et d'aide à la formation et au logement cantonales.

Bonne intégration des principes de protection des données mais cartographie à établir

La Cour constate que l'OCBE a bien intégré les principes de protection des données lors de l'informatisation de ses tâches et prend soin de les intégrer dans le cadre de traitement de données non automatisé. Un travail de formalisation reste toutefois à établir dans le cadre de la recommandation n°7, relative à la cartographie des données et de leurs flux et à la documentation en matière de sécurité[102]. Les processus d'octroi des bourses étant automatisés, les critères d'octroi bien définis et les échanges de données avec les autres entités bien cadrés, la mise en œuvre de cette recommandation ne représentera pas une tâche conséquente. Elle permettra néanmoins d'identifier les besoins spécifiques en sécurité. La Cour attire également l'attention de l'OCBE sur les nouvelles exigences en matière de protection des données relatives à l'utilisation des numéros AVS (voir page 50).

7. DFAJ : Bonne application des principes de protection des données mais nécessité d'adapter les modèles de contrats

Trois types d'activités traitant de données personnelles sensibles

La Direction finances et affaires juridiques (DFAJ) est rattachée à la Direction générale de la santé (DGS) et emploie 23 personnes. Selon le registre des fichiers, elle gère plusieurs activités traitant de données personnelles sensibles dont : les bordereaux pour le paiement de la part cantonale pour les hospitalisations en cliniques privées[103] et le traitement des garanties de paiement et le paiement des factures pour les hospitalisations extra-cantonales. La DFAJ assure également le suivi financier des mandats pour les autres entités de la DGS, comme la mise sur pied du mandat de gestion externe de l'opération de traçage des cas COVID. L'une des cadres de cette direction a d'excellentes connaissances des dispositions en matière de protection des données, ayant précédemment travaillé dans le domaine.

Anonymisation des fichiers utilisés pour le remboursement de la part cantonale

L'examen sommaire de la Cour a porté essentiellement sur le fichier « Cliniques privées VD - Bordereaux pour paiement de la part cantonale » répertorié sur le Registre des fichiers (fiche N°594). Néanmoins, d'autres activités et fichiers de la DFAJ ont également été abordés en cours d'entretien (et notamment le fichier « mandats externes et traitement des hospitalisations extra-cantonales »).

La Cour relève que la DFAJ a mis en place des mesures pour protéger les données et mène une réflexion permanente pour respecter les dispositions de la LPrD. En particulier, les bordereaux reçus par les collaboratrices de la DFAJ chargées du contrôle de concordance avec les montants figurant sur les factures jointes, sont anonymisés avant d'être transférés à la comptabilité. Les bordereaux reçus sont stockés sous forme informatique dans des répertoires avec des accès limités. Les factures sont conservées sous format papier dans une armoire sous clé.

[102] Les fichiers de l'OCBE, à l'instar de ceux de l'ensemble de la DGCS ne figurent pas encore dans le registre des fichiers, mais le projet envoyé par la DGCS à l'APDI comprend les trois fichiers OCBE.

[103] Pour les résident·e·s vaudois·es, les coûts de l'hospitalisation en division commune sont entièrement couverts (à 45% par l'assurance de base et 55% par le canton) pour autant qu'il s'agisse d'un établissement inscrit sur la liste LAMal (loi sur l'assurance maladie) vaudoise. Le canton a signé des conventions avec cinq cliniques privées vaudoises, auxquelles la DFAJ rembourse donc la part cantonale.

Plateforme HIN sécurisée pour les échanges relatifs aux hospitalisations extra-cantonales …

Dans le cadre des hospitalisations extra-cantonales, les prestataires de soins demandent au canton de Vaud de fournir une garantie pour le paiement des soins dispensés aux résident·e·s vaudois·es. Une garantie de paiement pour traitement extra-cantonal peut être demandée au service en charge de la santé publique et celui-ci se détermine sur la prise en charge de l'hospitalisation concernée. L'octroi de cette garantie est géré par la DFAJ.

Le processus de demande de garantie est traité par le biais d'une plateforme « Health Info Net AG » (HIN) [104], partagée par plusieurs cantons. HIN a été fondé en 1996 à l'initiative de la FMH (organisation professionnelle du corps médical suisse) et de la Caisse des médecins. Des mesures de protection existent pour sécuriser les échanges et pour limiter les accès aux données sensibles.

Après l'octroi de la garantie, la DFAJ reçoit une facture. Cette facture est généralement reçue en format papier. Elle est ensuite scannée et anonymisée avant d'être envoyée aux collaborateur·trice·s de la comptabilité, et enregistrée sous forme anonyme sur le serveur. La liste des hospitalisations extra-cantonales n'est consultable que pour les personnes possédant une clé d'accès.

… par contre les envois des bordereaux et factures se font via courriel

Si les échanges relatifs au traitement des hospitalisations extra-cantonales s'effectuent via la plateforme HIN, les bordereaux et factures envoyés à la DFAJ dans le cadre du paiement de la part cantonale pour les cliniques privées sont envoyés par courriel, sans sécurisation particulière. A l'image d'autres entités auditées, la DFAJ devrait faire part de ses besoins en matière de sécurité pour la communication de données sensibles (recommandation n°2).

Modèle de contrat de sous-traitance ou de délégation de tâche publique à compléter

La DFAJ assure le suivi financier de plusieurs mandats de sous-traitance ou de délégation de tâches publiques. La Cour a examiné deux documents contractuels (un contrat et une convention de subventionnement) y relatifs : si la convention de subventionnement contenait les clauses de respect de la LPrD et du secret de fonction, le contrat ne mentionnait pas de telles dispositions.

Intégrer systématiquement des clauses de respect de la LPrD et du secret de fonction dans les dispositions contractuelles de délégation d'une tâche publique
Constatation n°13
Les contrats de délégation d'une tâche publique impliquant la collecte et la gestion de données personnelles et sensibles par les services de l'ACV doivent contenir des clauses exigeant le respect de la LPrD et du secret de fonction. Un des contrats gérés par la DFAJ portant sur un mandat lié à la mise en œuvre opérationnelle des dispositifs d'endiguement de la crise COVID-19 intègre les clauses de confidentialité et de respect du secret de fonction, mais ne mentionne pas les dispositions de la LPrD.

[104] « Pour les professionnel·le·s de la santé en Suisse, HIN est considéré comme la norme en matière de communication sécurisée. HIN garantit un traitement en toute confiance des données des patient·e·s car la sécurité intégrale des données et des informations est notre compétence principale depuis 1996 » (www.hin.ch).

Recommandation n°13	La Direction finances et affaires juridiques (DFAJ)
Intégrer systématiquement dans les contrats de délégation d'une tâche publique impliquant le traitement de données personnelles et sensibles les clauses de respect de la LPrD et du secret de fonction.	

8. SEPS : gérer en interne les envois de promotion des manifestations sportives

Nombre limité de données personnelles traitées

Le Service d'éducation physique et du sport (SEPS) a pour mission principale « *d'animer et de superviser l'éducation physique et sportive dans les écoles* » et « *d'organiser et d'animer le mouvement "Jeunesse+Sport*" »[105], ainsi que de soutenir les acteurs - institutionnels ou non - qui s'occupent d'éducation physique. Il emploie 22 collaborateur·trice·s.

Dans le cadre de son activité, le SEPS n'est pas amené à traiter de données personnelles sensibles. Néanmoins, le registre des fichiers géré par l'APDI comporte le nom de deux fichiers pour le SEPS : « *la base de données contenant les coordonnées des maîtres d'éducation physique* », et « *les préavis pour les élèves candidats au programme sport-études* ».

Bien que la loi sur l'éducation physique et le sport (LEPS) prévoit que l'intégration des élèves au programme « sport-études » puisse être assortie de la condition d'un suivi médical, cette option n'est en pratique jamais utilisée. De ce fait, le SEPS ne traite aujourd'hui aucune donnée médicale et gère uniquement les listes des candidat·e·s et des bénéficiaires. Les recours contre les décisions d'enclassement sont gérés par le secrétariat général du département.

Comme toutes les entités auditées, le SEPS est concerné par la nécessité d'identifier et de cartographier les données personnelles gérées et leurs flux et de documenter les mesures de protection (recommandation n°7). Compte tenu du nombre limité de données traitées, cette tâche ne représente pas un travail conséquent pour le SEPS.

Ne pas transmettre les adresses électroniques des enseignant·e·s à des tiers externes

Dans le cadre de sa mission de promotion du sport, le SEPS soutient l'organisation d'événements sportifs populaires tels que les *20km de Lausanne* ou les *24 heures de natation* par exemple en collaborant étroitement avec les organisateur·trice·s. Afin d'informer les enseignant·e·s en éducation physique de la tenue de telles manifestations et dans le but d'encourager les élèves à y participer, le SEPS communique les adresses électroniques des enseignant·e·s aux organisateur·trice·s.

Bien que les adresses électroniques ne constituent pas des données sensibles et que cette communication de données s'inscrive dans les missions légales du SEPS, cette démarche présente des risques : subtilisation ou transmission des adresses à d'autres, utilisation à d'autres fins que celle de la promotion du sport, etc. La Cour recommande au SEPS de procéder lui-même à l'envoi de tels messages de promotion. Cela réduit considérablement les risques et se justifie du fait qu'il est partie prenante de l'organisation de ces manifestations.

[105] Art. 3 al. 1 lettre a. de la loi sur l'éducation physique et le sport (LEPS).

Gérer en interne l'envoi d'informations aux professeur·e·s d'éducation physique pour promouvoir des manifestations sportives
Constatation n°14
Dans le cadre de sa mission de promotion du sport, le SEPS encourage les élèves à participer à des manifestions sportives (par exemple les 20 km de Lausanne). Dans ce but, il transmet à l'organisateur·trice de la manifestation la liste des adresses électroniques des enseignant·e·s en éducation physique afin que ces derniers promeuvent la manifestation auprès de leurs élèves. La communication de données personnelles doit respecter la LPrD, en particulier l'art. 15, qui impose qu'une condition au moins soit remplie : existence d'une base légale, nécessité pour accomplir une tâche publique, consentement exprès des personnes concernées, etc. ; ce qui ne paraît pas être le cas. Or, dans ce type de situations, la communication de ces données n'est pas nécessaire, l'envoi des informations pouvant être géré par le SEPS.
Recommandation n°14 au Service d'éducation physique et des sports (SEPS)
Gérer en interne au SEPS l'envoi à destination des enseignant·e·s en éducation physique d'informations de promotion d'un événement sportif auprès des élèves vaudois. Procéder à un envoi en copie cachée et sans communication des adresses électroniques individuelles à des prestataires externes à l'ACV.

Des situations inégales constatées entre les différentes entités-métiers auditées

Les situations dans les différentes entités auditées en matière d'application des principes de protection des données sont très inégales. Les problèmes constatés chez la plupart d'entre elles ne doivent toutefois pas amener à conclure qu'il existe automatiquement des problèmes de confidentialité des données à l'ACV. Au niveau des risques humains, les collaborateur·trice·s de l'ACV sont toutes et tous soumis·e·s au secret de fonction, notion connue, même si tous les détails ne sont pas spécifiés, et qui garantit un certain niveau de confidentialité des informations traitées. En outre, certain·e·s employé·e·s sont également soumis·e·s au secret professionnel, comme le secret médical, dont la portée leur est bien connue.

Le respect des secrets de fonction et professionnel constitue certes un premier bouclier de sécurité à l'ACV, mais n'assurent pas la conformité à la LPrD. Les éléments de non-respect de certaines dispositions de la LPrD constatés dans le cadre de cet audit, ainsi que le manque de support et de cadre pour les entités-métiers, signalent l'existence de risques en matière de confidentialité des données. Les cas avérés de violation de cette confidentialité témoignent également de la nécessité de renforcer les conditions cadres.

4.2.4 ENTITÉS-CADRES EN PROTECTION DES DONNÉES : EFFICIENCE CONSTATÉE MAIS CONTRÔLE À RENFORCER

La principale entité-cadre en matière de protection des données est l'APDI. Selon le dernier rapport d'activité de l'APDI, ses missions en matière de protection des données sont : surveiller l'application des prescriptions en matière de protection des données ; promouvoir la protection des données dans le canton ; informer les responsables de traitement sur les exigences posées en matière de protection des données ; renseigner les personnes concernées sur les droits découlant de la LPrD ; être consultée lors de l'élaboration de loi, règlement, directive ou autre norme impliquant le traitement de données personnelles ; intervenir, sur demande des responsables de traitement ou des personnes concernées, afin de résoudre des questions soumises à la LPrD ; être consultée sur les projets relatifs à l'installation de systèmes de vidéosurveillance et recourir à l'encontre des décisions qui ne seraient pas conformes ; tenir à jour un registre des fichiers public et accessible en ligne ; collaborer avec les autres autorités compétentes en matière de protection des données des autres cantons, de la Confédération ou de l'étranger ; traiter les recours prévus à l'art. 31 LPrD.

La DGNSI est avant tout en charge des questions de sécurité, thème qui sera traité au chapitre suivant (4.3). Toutefois, dans le cadre de sa mission de gestion des projets de nouvelles applications informatiques pour les services-métiers, la DGNSI, en collaboration avec ces derniers, doit appliquer les principes de protection des données aux solutions mises en œuvre[106]. Elle joue donc également un rôle d'entité-cadre pour la protection des données dans la mise en œuvre des projets informatiques.

Quant au SPEV, s'il est tenu comme toutes les entités de l'ACV d'appliquer la LPrD, il n'a aucune mission d'encadrement dans ce domaine. Son action sera abordée dans le chapitre traitant des directives liées à la sécurité à l'intention du personnel (télétravail et outils informatiques) (voir chapitre 4.3.2).

APDI : haut niveau de compétence juridique, mais nécessité de renforcer sa mission de surveillance et ses ressources en informatique

Compétence reconnue des autres entités de l'ACV

Après l'entrée en vigueur de la LPrD en 2008, l'Autorité de protection des données (APDI) a été instituée dès le 1er janvier 2009. Elle exerce son activité de manière indépendante.

Dans le cadre de cet audit, la Cour a sollicité l'autorité de protection des données et de droit à l'information (APDI), non seulement au titre d'entité auditée, mais également pour des questions pointues d'application de la législation. Elle témoigne de la haute compétence de l'APDI dans ce domaine juridique complexe et sa disponibilité pour apporter un soutien aux entités qui sont dépourvues de compétence interne. Ce constat est unanimement partagé par les entités-auditées.

[106] L'article 7 du RIC précise en effet que la DGNSI est chargée « *de l'appui aux services pour l'optimisation de leurs processus métiers et l'identification des besoins d'évolution de leur système d'information métier* » et « *de l'élaboration des solutions propres à chaque métier et de leur intégration au socle des systèmes d'information* ».

Spectre des missions très large

Ses missions légales (art. 36 et 37 LPrD), représentées schématiquement en page 18, sont résumées dans son dernier rapport d'activité disponible[107]. Tant le spectre de ses missions, que le cercle des entités sous sa surveillance sont larges : l'ACV, les communes et toutes les entités auxquelles le canton et les communes délèguent une tâche publique.

L'ampleur de la tâche de l'APDI est à la hauteur du changement culturel dans les entités qui y sont soumises, imposé par les dispositions en matière de protection des données introduites en 2008. Comme vu précédemment, toutes les entités de l'ACV ne l'ont encore pas intégré et partout, une mise à niveau des connaissances de l'ensemble des collaborateur·trice·s est reconnue comme nécessaire.

Ressources limitées en regard de l'ampleur de la mission et des sollicitations externes

Au moment de l'exécution de l'audit, l'APDI, en charge à la fois de la protection des données et du droit à l'information employait 7 personnes représentant 5.5 équivalent plein-temps (ETP), dont 1 ETP pour la fonction de délégué au droit à l'information, 0.6 ETP de secrétariat et 1 ETP en contrat à durée déterminée (juriste stagiaire).

L'APDI doit faire face à des demandes toujours plus nombreuses, que ce soit de la part des entités soumises à la LPrD ou de la part des citoyen·ne·s : en 2019, elle a été sollicitée à 1'132 reprises dont 981 fois pour des questions de protection des données (87%), soit plus du triple qu'en 2009. Certaines demandes sont conséquentes : traitement de recours, enquête sur dénonciation, réponses à des questions complexes, etc.

La Commission de gestion du Grand Conseil vaudois (COGES) a pointé des manquements

La COGES, qui suit l'activité de l'APDI avec attention depuis 2012, a adressé plusieurs observations au Conseil d'Etat : elle a notamment formulé une observation demandant que soit inséré un point relatif au traitement des questions de protection des données dans chaque exposé des motifs présenté au Grand Conseil. Cette insertion doit permettre d'intégrer la culture de la protection des données dans les entités de l'ACV et faire connaître l'existence des projets à l'APDI.

Durant les premières années de son activité, l'APDI s'est surtout concentrée sur sa mission d'autorisation des installations de vidéosurveillance, notamment communales (art. 22a LPrD).

Dans son rapport de 2014, la COGES, a souligné le retard pris par le bureau du·de la préposé·e à la protection des données dans la mise en place du registre des fichiers qui aurait dû être terminée en 2010 et a formulé une observation à ce sujet. Suite à cette observation, 1 ETP temporaire a été accordé pour cette mission. Dans ce même rapport, la COGES a demandé au Conseil d'Etat de dresser un bilan de l'activité de cette instance.

A ce jour, le registre des fichiers est en voie de finalisation concernant l'ACV. Les entités encore manquantes (telles que la DGCS) ont envoyé un premier projet, qui est en cours d'examen par l'APDI. Par contre le bilan de l'activité de l'APDI demandé n'a pas été établi, le Conseil d'Etat l'ayant prévu dans le cadre du futur exposé des motifs et projet de loi concernant la révision de la LPrD.

[107] Rapport d'activité pour la période du 1er septembre 2016 au 31 décembre 2018, Bureau de la préposée à la protection des données et à l'information.

La Cour partage le constat de la Conférence des Préposé·e·s suisses à la protection des données (PRIVATIM) de 2019 : « *dans la grande majorité des cantons, les ressources ne suffisent néanmoins toujours pas aux autorités de protection des données pour accomplir leurs tâches* » [108].

Au vu des constats établis dans le cadre de cet audit, la Cour estime toutefois prioritaire de créer ou renforcer la compétence en matière de protection et sécurité des données au sein des entités-métiers. Cet objectif peut être atteint avec le développement de la formation des collaborateur·trice·s (recommandation n°4) et la création de la fonction de délégué·e interne à la protection des données (recommandations n°6). Il est en effet illusoire de croire que seule une augmentation de la dotation de l'APDI suffise à améliorer l'application de la LPrD, alors que les responsables de traitement des données, c'est-à-dire les entités-métiers, disposent actuellement de compétences et connaissances insuffisantes en la matière.

Nécessité de renforcer ses compétences en informatique

Par contre, la Cour rejoint le constat établi par PRIVATIM concernant également le manque de ressources spécifiques en informatique dans les bureaux des préposé·e·s à la protection des données[109]. L'APDI ne dispose en effet d'aucun·e spécialiste en informatique. Or la généralisation de la numérisation des données, crée des interrogations nouvelles en matière d'accès et d'interface, de transfert via internet, d'hébergement dans le cloud, etc., relatives à la protection et à la sécurité des données.

Même si une bonne collaboration existe entre l'APDI et la DGNSI, il est nécessaire que l'APDI, pour pouvoir exercer sa mission de manière indépendante, puisse disposer en interne de compétences en nouvelles technologies (systèmes d'information, réseaux et développements informatiques)[110]. Ces compétences sont d'autant plus utiles qu'avec la généralisation du télétravail, des questions supplémentaires se posent en matière de sécurité des données en lien avec la LPrD. Elle doit aussi pourvoir exercer son activité de surveillance sur la DGNSI.

La recommandation est adressée à l'APDI[111].

Renforcer les compétences de l'APDI en informatique
Constatation n°15
Le développement très rapide des nouvelles technologies de l'information et de la communication (NTIC) génère de nouvelles questions en matière de protection des données et des risques accrus relatifs à la sécurité des données personnelles numériques des administré·e·s (comme dans toutes les administrations). En tant qu'autorité de surveillance de l'application de la LPrD, l'APDI est ainsi régulièrement et de plus en plus confrontée à des questions techniques ou relatives à la sécurité d'outils ou applications informatiques traitant de données personnelles. L'APDI ne dispose toutefois pas de ressources internes au bénéfice d'une formation en informatique et ne peut donc remplir sa mission dans ce domaine de manière autonome.

[108] Le bureau du préposé fédéral à la protection des données compte 31 collaborateur·trice·s, pour l'ensemble de la Confédération et du secteur privé du pays. Au niveau cantonal, Fribourg a des ressources similaires à Vaud soit 2,9 ETP et 2,0 ETP temporaires. Certains bureaux cantonaux sont encore moins dotés que le bureau vaudois : Genève (2,3 ETP), Neuchâtel et Jura (1,6 ETP). D'autres, à l'image de celui du canton de Zurich sont mieux dotés : 15 collaborateur·trice·s.

[109] Voir Communiqué de presse « Journée internationale de la protection des données 2020 »

[110] Pour illustrer l'interdépendance croissante entre protection des données et informatique, on peut mentionner le poste de spécialiste en protection des données dont la DGNSI vient de se doter.

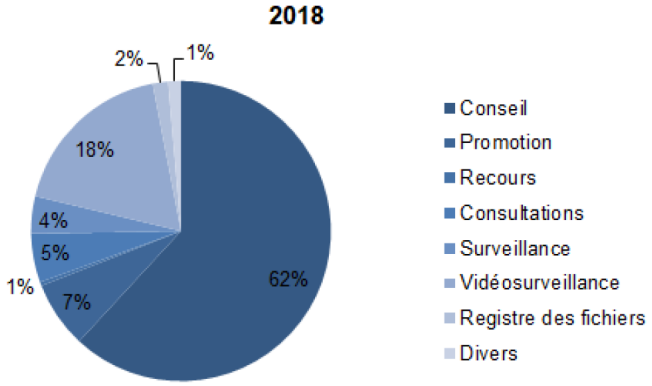
[111] Il appartient à l'APDI, dans le cadre du processus budgétaire, de faire part de ses besoins et de solliciter un nouveau poste.

Recommandation n°15	à l'APDI
Renforcer les compétences de l'APDI en informatique pour lui permettre de mieux appréhender les questions techniques posées par les systèmes et les technologies d'information, afin d'être en mesure de remplir sa mission de surveillance de manière autonome.	

Seule 4% de l'activité est dévolue à la mission de surveillance

La mission première de l'APDI est de surveiller l'application de la LPrD. Or, comme l'illustre la répartition des tâches de l'APDI en 2018 (voir le graphique ci-dessous) seule 4% de l'activité est liée aux tâches de surveillance[112], la majeure partie étant consacrée au conseil (62%), à la vidéosurveillance (18%) ou à la promotion (7%).

Répartition de l'activité de l'APDI par mission en 2018



Source : APDI rapport d'activité 2016-2018

Pour la Cour, l'activité de surveillance est la principale à même de garantir que les dispositions LPrD sont correctement et uniformément appliquées. Le chapitre précédent a montré que l'objectif de conformité n'est pas toujours atteint à l'ACV.

Le nombre total d'audits menés par l'APDI se monte à 12 depuis 2008. Si le type d'audits témoignent du souci de répartir les efforts sur les différents types d'entités soumises à la LPrD : 5 audits concernent l'ACV, 5 les communes et 2 des associations, ce faible nombre illustre le besoin de renforcer la mission de surveillance de l'APDI, les entités soumises à la LPrD dépassant le millier.

Le renforcement des compétences internes aux entités-métiers à l'ACV, qui devrait idéalement s'étendre aux autres entités soumises à la LPrD, devrait progressivement alléger les sollicitations auprès de l'APDI pour des questions simples et lui permettre de se concentrer sur sa mission première de surveillance.

Dans l'intervalle, la Cour est certes consciente qu'une augmentation des activités de surveillance ne pourra s'effectuer qu'au détriment de celles de support et de conseils et risque de causer une certaine insatisfaction des entités-métiers. Mais elle estime que depuis treize ans qu'est entrée en vigueur la LPrD, il est temps que la mission de l'APDI se concentre désormais sur la surveillance.

[112] En moyenne depuis 2009, ce pourcentage est même inférieur à 2%.

En effet, si l'essentiel de l'activité de l'APDI reste centrée sur le conseil, cela risque de contribuer au déséquilibre entre les entités : celles qui la sollicitent fréquemment continuent de s'améliorer tandis que les autres, en l'absence de contrôle, ne sont pas incitées à progresser.

Renforcer la mission de l'APDI en matière de surveillance de l'application de la LPrD
Constatation n°16
Devant faire face à un nombre important et croissant de demandes d'informations externes, soumise à de nombreuses sollicitations, et compte tenu de sa dotation actuelle, l'APDI n'est pas à même de remplir pleinement sa mission prioritaire de surveillance (art. 36 LPrD). Selon le rapport d'activité 2016-2018, les missions de surveillance ne représentent que le 4% de l'activité réalisée. La Cour relève la qualité et l'efficacité des audits menés par l'APDI qui débouchent sur des recommandations bien acceptées par les services. Leur mise en œuvre permet d'instaurer une vraie culture de protection des données qui fait défaut actuellement à l'ACV. Toutefois, depuis la création de l'APDI, seuls douze audits ciblés ont pu être menés.
Recommandation n°16 **à l'APDI**
Renforcer la mission de l'APDI en matière de surveillance de l'application de la LPrD en réalisant davantage d'audits ciblés dans les entités soumises à la LPrD.

Annoncer à l'APDI toute violation en matière de sécurité et confidentialité des données

Pour être en mesure d'exercer ses missions de surveillance et de sensibilisation, l'APDI doit être informée des problèmes rencontrés, particulièrement des cas où la sécurité et la confidentialité des données soumises à la LPrD ont été violées. Cela lui permet d'entreprendre des campagnes d'information, de lancer des audits ciblant les difficultés et d'assister les entités concernées dans les éventuelles mesures correctrices à prendre.

Or la Cour constate que l'APDI n'est pas systématiquement informée des incidents : les deux cas de violation de la confidentialité, signalés dans le cadre de cet audit n'avaient pas été transmis à l'APDI.

L'obligation de notifier toute violation de la sécurité des données à caractère personnel à l'autorité de contrôle figure parmi les dispositions de la Convention 108+. Elle est prévue par le RGPD ainsi que par la nLPD. Les dispositions vaudoises devraient ainsi également intégrer une telle clause. Le projet de révision de la LPrD étant en cours, cette recommandation est adressée au Conseil d'Etat.

Rendre obligatoire la déclaration à l'Autorité de protection des données de toute violation de la sécurité des données	
Constatation n°17	
Des cas de violation de la sécurité des données personnelles se sont déjà produits à l'ACV, par exemple la divulgation non autorisée de données sensibles. Même s'ils sont rares, ils peuvent potentiellement atteindre à la personnalité d'administré·e·s et causer d'importants dégâts d'image à l'Etat. Il est nécessaire que l'APDI soit informée de ces cas pour pouvoir être en mesure d'exercer efficacement sa mission de surveillance et, au besoin, pouvoir apporter un appui aux services concernés. Or il n'y a aucune obligation à ce niveau.	
Recommandation n°17	**au Conseil d'Etat**
Rendre obligatoire l'annonce à l' Autorité de protection des données de toute violation de la sécurité des données touchant des données personnelles sensibles ou entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée pour permettre à l'APDI d'exercer sa tâche de surveillance selon l'art. 36 al. 3 LPrD.	

Mission de l'APDI relative à la tenue du registre des fichiers non auditée …

La Cour a centré son audit sur la protection et la sécurité des données dans le cadre du télétravail et n'a donc pas retenu la question de l'accès des individus à leurs propres données gérées par l'ACV. En conséquence, l'examen de la tenue par l'APDI du registre des fichiers, qui a pour but de faciliter cet accès, n'a pas été réalisé.

De plus, le cadre légal européen (RGPD), sur lequel s'est alignée la loi fédérale révisée (nLPD), a supprimé la notion de registre des fichiers au profit de celle de registre des activités de traitement (art. 30 RGPD et art. 12 nLPD). Dès lors, il a été jugé peu pertinent d'auditer un outil qui sera vraisemblablement amené à être modifié lors de la révision en cours de la LPrD.

… mais constat posé sur la nécessité d'améliorer ou de compléter l'outil

Les fiches qui figurent dans le registre des fichiers, accessible en ligne sur la page internet de l'APDI, ont toutefois été consultées dans le cadre de cet audit, en particulier pour sélectionner les applications et activités à examiner dans les entités-métiers.

La Cour constate que si cet outil représente une première étape du recensement des activités de l'entité-métier comprenant l'utilisation de données personnelles, il souffre d'un défaut de transparence : seuls le titre du fichier et son but donnent des indications sur le traitement réalisé. Peu d'information n'est fournie sur les données traitées, leur utilisation, leur flux ou les différentes entités concernées. L'outil actuel ne permet donc pas aux citoyen·ne·s d'avoir une vision claire sur les données qui les concernent et l'utilisation qui en est faite. Il est ainsi nécessaire de compléter ces informations par le détail des données traitées, leur utilisation, leur flux et les mesures de sécurité adoptées pour les protéger (voir recommandation n°7[113]).

[113] Cette recommandation reprend une partie des exigences posées par les nouvelles dispositions du RGPD relative au registre des activités de traitement demandant d'identifier les parties prenantes intervenant dans le traitement, les catégories de données, leurs buts, les entités qui y accèdent ou à qui elles sont communiquées, le délai de conservation, les mesures de sécurisation (Source : CNIL).

En outre, le registre des fichiers exigé par l'actuelle LPrD, n'est pas complet : on l'a vu, certaines entités de l'ACV traitent de données personnelles et sensibles sans pourtant y être recensées. Par ailleurs, ce registre ne comprend toujours pas les fiches signalétiques des fichiers détenus par les communes vaudoises, ainsi que par les établissements publics et les entités privées délégataires de tâches légales.

DGNSI : intégration récente des principes de protection des données dans son activité conformément à la stratégie fixée par le Conseil d'Etat

Principes de protection des données intégrés dans la stratégie numérique de l'Etat dès 2018 …

Le Conseil d'Etat a, dans son dernier programme de législature 2017-2022, accordé un haut degré de priorité à la protection des données, en lien avec la sécurité des données numérique, dans le cadre de l'objectif « *1.3 Accompagner la transition numérique* ».

En novembre 2018, il a publié un document qui pose les bases pour doter le Canton des infrastructures indispensables au développement numérique[114] : « l*e Conseil d'Etat entend ainsi doter le canton de Vaud d'une politique publique de la donnée, fondée notamment sur les principes de souveraineté et de sécurité (…) tout en protégeant les personnes, les entreprises et autres collectivités des risques découlant d'une utilisation abusive de ces données* ».

… et dans le plan directeur cantonal des systèmes d'information 2018-2023

La dernière version du plan directeur cantonal des systèmes d'information (2018-2023) a bien intégré les orientations stratégiques définies par le Conseil d'Etat : parmi les deux axes d'évolution prioritaires se trouve la nécessité de « renforcer la sécurité numérique et la protection des données », faisant clairement ressortir l'objectif du programme de législature lié à la transition numérique. Des cinq actions[115] prévues pour répondre aux besoins de cet axe, la dernière se réfère directement aux dispositions de la législation sur la protection des données : identification et protection des données. Elle prévoit de développer une gouvernance des données par domaine clé, d'inventorier et classifier ces données et d'assurer un niveau de protection adéquat lors de leur stockage, leur traitement et leur communication.

La nécessité d'envisager chacune des actions dans un objectif de protection des données est clairement spécifiée. Par exemple en matière de sécurisation de l'architecture des systèmes, il est indiqué que la sécurité et la protection des données doivent être prises en compte dès la conception des solutions (principes de « *security-by-design* » et « *privacy-by-design*[116] »).

Les impératifs de protection des données personnelles tout au long de leur cycle de vie sont également repris dans les deux EMPD relatifs à la sécurité informatique[117], témoignant de leur prise en compte dans la construction de la politique de sécurité informatique à l'ACV.

On constate ainsi qu'au niveau de la stratégie et des objectifs en matière de développement informatique, la question de la protection des données est désormais intégrée[118].

[114] Stratégie numérique, Etat de Vaud, novembre 2018

[115] Les quatre premiers relèvent de la sécurité : sensibilisation des parties prenantes ; gestion des identités et limitation des accès ; intégration de la sécurité dans l'architecture des systèmes et prévention ; détection des incidents.

[116] Le principe de "privacy by design" a été instauré par le Règlement général sur la protection des données (RGPD) de 2018.

[117] EMPD n°61 (2013) et n°147 (2019)

[118] A noter qu'elle ne figurait pas de manière aussi claire dans le précédent plan directeur cantonal informatique 2013-2018 centré sur la nécessité d'améliorer la sécurité générale des systèmes d'information.

Compétences renforcées en protection des données à la DGNSI

Pour concrétiser le programme prévu par le plan directeur cantonal et la stratégie numérique en faveur de la protection des données, la DGNSI a renforcé son organisation et créé deux nouveaux postes : celui de délégué au numérique (en octobre 2019), chargé entre autres d'établir une politique de la donnée, ainsi qu'un poste de juriste en matière de protection des données (en juillet 2020). Ce dernier officie comme délégué à la protection des données interne à la DGNSI, permettant d'éviter le recours systématique aux services de l'APDI. Directement rattaché au poste de délégué au numérique, il est associé à tous les projets de développement impliquant des questions de protection des données. A noter également qu'un des collaborateur·trice·s de l'Unité de sécurité des systèmes d'information (USSI) de la DGNSI a suivi une formation CAS en matière de protection des données, renforçant encore les compétences de la DGNSI dans ce domaine.

En outre, une nouvelle structure a été mise en place : le Comité d'Experts Délégués au Numérique (CEDN), auquel participe les responsables l'USSI et la préposée à la protection des données. Ce comité a été mis en place pour examiner les projets informatiques « en nuage » (solutions externalisées dans le cloud) et sera amené à jouer un rôle consultatif dans le domaine de la politique de la donnée.

Adaptation de directives et d'outils de gestion pour intégrer les principes LPrD

Au niveau de la gestion de projets, de nouveaux outils ont été créés, dont une grille d'évaluation des enjeux sécuritaires pour des projets de développement ou modification d'applications centrée sur la sécurité et la protection des données. Elle comprend un volet examinant la question de la protection des données sous l'angle de 25 éléments à renseigner (par exemple le responsable du traitement ou la nature des données traitées) ou à analyser (par exemple le concept de « *privacy by default/by design* » est-il appliqué ?). Cette grille permet de déterminer si les mesures prévues dans le projet sont suffisantes pour respecter les principes de protection des données.

La Cour note toutefois que cet outil est récent, un seul projet ayant été analysé sur cette base.

D'autres outils ont été récemment élaborés, conjointement à la création du CEDN, pour cadrer et examiner les solutions informatiques externalisées et régler les problèmes en matière de sécurité et protection des données que représente le stockage des données sur le cloud : une grille d'analyse, une directive et une check-list pour les contrats de sous-traitance en matière d'informatique externalisée.

Des démarches récentes

Avec ces nouveaux outils et le renforcement de ses ressources, la DGNSI est bien outillée pour traiter les questions de protection des données. La Cour note toutefois que ces éléments sont très récents en regard de l'entrée en vigueur de la LPrD en 2008.

Des principes de protection des données pas intégrés à tous les processus

Il reste néanmoins d'importants chantiers à mener, des procédures et des outils à adapter. Parmi les éléments-clés, on relève la nécessité de réaliser une cartographie des données numériques, l'intégration d'une étape d'analyse des données sous l'angle des dispositions en matière de protection des données dans l'élaboration des schémas directeurs métiers, ainsi que la révision des outils contractuels de la DGNSI.

Le modèle de schéma directeur métier doit comprendre un volet « protection des données »

A l'Etat de Vaud, le processus d'élaboration d'un système d'information numérique, se fonde sur les orientations stratégiques fixées par le Conseil d'Etat, déclinées ensuite dans le plan directeur cantonal des SI sur cinq ans.

Un schéma directeur métier des systèmes d'informations est ensuite élaboré pour chaque entité-métier gérant des applications complexes. Il définit, pour un ou plusieurs services, les principes, les étapes et les projets d'évolution du système d'information métier pour les 5 à 10 ans à venir, en adéquation avec les orientations stratégiques du métier et dans le cadre fixé par le plan directeur cantonal des SI.

La méthode d'élaboration des schémas directeurs métiers est définie dans une directive « *Exigences relatives aux schémas directeurs sectoriels du SI* » qui prévoit plusieurs étapes[119]. Or la Cour constate qu'il n'existe aucun volet ni étape d'analyse en matière de protection des données. Seule l'annexe « Analyse de l'existant » comprend quelques questions relatives à l'identification des données personnelles et sensibles ainsi qu'une référence à la nécessité de se conformer à la LPrD au niveau de la cartographie des données. Il n'existe aucune analyse de risques en matière de protection des données, comme cela est le cas avec la grille d'évaluation des enjeux sécuritaires pour des projets de développement ou modification d'applications.

Cartographie des applications à compléter avec les types de données personnelles traitées

L'identification et la protection des données numériques fait partie des actions prévues dans le plan directeur cantonal des SI 2018-2023 : « *développer progressivement une gouvernance des données par domaine-clé* » et « *inventorier et classifier ces données »,* dans le but d' « *assurer un niveau de protection adéquat lors de leur stockage, leur traitement et leur transmission* ».

Un projet pilote de nouvelle cartographie des données a été initié à la DGNSI, distinct de la cartographie existante des applications informatiques « Cartomega ». Cette dernière avait été élaborée pour répondre aux dispositions prévues par le RIC à l'art. 20 al. 1 : « *dans le but d'assurer la maîtrise du patrimoine informatique, la DSI tient à jour notamment : la cartographie des applications informatiques (fonctionnalités et données associées) ; chaque fois que possible et en collaboration avec les services, la cartographie des processus …* ». Si elle illustre les applications existantes et les connexions entre elles, elle ne met pas en évidence les données personnelles et sensibles à protéger selon la LPrD qu'elles contiennent. La Cour constate en outre qu'elle n'est pas complète pour tous les services.

Le rajout dans l'application Cartomega d'une couche informative renseignant sur le type de données traitées dans les applications ainsi que de leur flux serait une solution pour réaliser l'action « identifier et protéger les données » prévue dans le plan directeur cantonal informatique 2018-2023.

[119] Ces étapes sont : Analyse de l'existant, Construction de la cible fonctionnelle, Diagnostic d'urbanisme et Orientations, Architecture logique et Migration. Cette analyse doit s'appuyer sur la documentation et l'analyse par les services de leur stratégie, leurs processus, leur organisation et leurs besoins fonctionnels comme le prévoit le RIC (art. 10 al. 2).
Chaque étape du schéma directeur métier fait l'objet d'un canevas donnant le fil rouge de l'analyse à réaliser. Ces canevas figurent dans des documents formant les annexes de la directive. Dans l'étape d'analyse de l'existant, sont prévues : une cartographie des processus existants, une cartographie applicative de l'existant, une cartographie des macro-données, une cartographie des risques. L'objectif de cette étape est de comprendre et décrire les métiers des services au travers des processus métier, dresser un diagnostic du système actuel, identifier les forces et faiblesses, les risques et les opportunités d'amélioration.

Modèles contractuels à réviser

La DGNSI dispose de plusieurs documents contractuels en matière de sous-traitance informatique :

- les conditions générales DSI (08.4 CG) ;
- le contrat-cadre de prestation (08.4 CC) ;
- les accords de confidentialité personnes et entreprises (05.4) ;
- une check-list et un contrat-type de sous-traitance de solution informatique externalisée.

Ces quatre documents, dont certains sont antérieurs à la LPrD, contiennent des dispositions qui parfois se recoupent, créant des redondances. Certaines sont obsolètes ou contradictoires. D'autres enfin ne sont pas correctes. Par exemple :

- Les bases légales en matière de protection des données ne sont plus à jour dans les conditions générales et le contrat-cadre ; elles se réfèrent en effet à la version précédente de la LPrD.
- Les documents spécifient que le sous-traitant doit se conformer aux dispositions fédérales en matière de protection des données ou aux dispositions vaudoises. Or ce sont obligatoirement les deux régimes qui s'appliquent aux sous-traitants.
- Les accords de confidentialité se réfèrent à la directive LPers 50.1, dont certaines clauses ne sont plus actuelles (voir constatation n°20).
- Le contrat-cadre spécifie que le sous-traitant « *certifie que de telles données* [confidentielles] *ne seront pas stockées dans des machines sises hors de ses locaux professionnels* », disposition qui ne tient pas compte des possibilités d'hébergement « *en nuage* » avec chiffrement sécurisé décrit très précisément dans la check-list.

De manière générale, ces dispositions doivent être réactualisées et simplifiées. En outre, aucune d'entre elles ne mentionne la nécessité pour le sous-traitant de respecter le secret de fonction (art. 18 LInfo et 320 CP).

Adapter tous les outils, modèles et procédures informatiques pour renforcer la protection des données
Constatation n°18
La DGNSI a adopté une politique de sécurité conforme aux bonnes pratiques. Sa mise en œuvre est encore en cours. Les mesures informatiques pour assurer la protection des données au sens de la LPrD doivent s'appuyer sur cette politique de sécurité consolidée, raison pour laquelle elles ont été élaborées dans un deuxième temps. Ce n'est que depuis très récemment, soit dès 2018, que la protection des données constitue un axe prioritaire selon le plan directeur informatique. Si au niveau de l'organisation, la DGNSI bénéficie de ressources supplémentaires en matière de protection des données et a créé des structures adéquates, des outils et processus doivent encore être développés.

Recommandation n°18	à la DGNSI
Pour répondre aux impératifs de protection des données personnelles et des données à protéger dans le domaine numérique et répondre à l'objectif prioritaire du plan directeur cantonal informatique, la DGNSI doit poursuivre l'adaptation de ses processus, modèles et outils. Il est notamment nécessaire, en collaboration au besoin avec les entités-métiers : • d'adapter la directive et les modèles du processus d'élaboration des schémas directeurs informatiques sectoriels du SI ; • d'établir une cartographie des données numériques personnelles et sensibles ainsi que celles soumises au secret de fonction gérées par les services (en complétant par exemple l'application Cartomega) ; • de réactualiser les dispositions contractuelles DGNSI avec les sous-traitants.	

4.3 SÉCURITÉ DES DONNÉES : POLITIQUE GLOBALEMENT CONFORME AUX BONNES PRATIQUES

4.3.1 DGNSI : POURSUIVRE L'IMPORTANT TRAVAIL DE MISE À NIVEAU RÉALISÉ EN MATIÈRE DE SÉCURITÉ INFORMATIQUE

Sécurité informatique : pilier principal de la protection des données

Une politique efficace de protection des données numériques au sens de la LPrD ne peut s'élaborer que dans le cadre d'une architecture informatique sécurisée. Il est en effet de peu d'utilité de mettre en œuvre les principes de la LPrD, si les supports hébergeant les données traitées ou leurs canaux de transmission présentent des vulnérabilités. A l'inverse, les mesures de protection des données forment un rempart important en cas de défaut de sécurité (intentionnel ou accidentel).

Des cyberattaques contre des entités publiques …

Les questions de sécurité constituent une réelle menace tant pour le secteur privé que public. Rien qu'en 2021, la presse s'est fait l'écho de problèmes de sécurité informatique rencontrés par plusieurs entités[120] dont au moins une s'est fait subtiliser des informations contenant des données personnelles et sensibles dans le but d'obtenir une rançon (rançongiciel)[121]. Le refus de cette commune a entraîné la publication de ces informations sur le darknet[122]. Le dégât d'image subi par ces entités, voire par les personnes dont les données ont été divulguées et les risques représentés pour elles, illustrent l'interdépendance entre sécurité et protection des données.

[120] Le premier cas est celui de la commune de Rolle mais, selon les médias, d'autres communes vaudoises auraient également été victimes de cyberattaques (source : « La cyberattaque contre la commune de Rolle démontre que nul n'est à l'abri », journal 24 Heures, 04.09.2021) ; le second, celui de la commune de Montreux. Peu de temps auparavant, une rançon estimée à 400'000 dollars a été payée aux pirates informatiques qui avaient bloqué certaines données du comparateur en ligne Comparis au début du mois de juillet. Le gymnase intercommunal de la Broye a également fait l'objet d'un piratage informatique, dont la tentative de rançon a été déjouée.
[121] Une autre « technique » consiste à pénétrer le système d'information, en prendre le contrôle et crypter toutes les données qui seront déchiffrées contre rançon.
[122] Le darknet est un réseau privé virtuel utilisant des protocoles spécifiques qui intègrent des fonctions pour anonymiser les utilisateur·trice·s et les données. Certains darknets se bornent à l'échange de fichiers alors que d'autres construisent de véritables écosystèmes. Le néologisme Darknet désigne l'ensemble de ces darknets.

… qui sont en forte croissance

Le Centre national pour la cybersécurité (NCSC) enregistre une croissance importante des annonces de cyber-incidents signalés par des privés et entités publiques. Si en 2020 le nombre de rançongiciels (tous secteurs confondus) annoncés était de 68, il s'élève déjà à 119[123] pour les 9 premiers mois de 2021. Les pirates ne se contentent plus de rançonner l'entreprise ou l'établissement public qui gère les données, mais s'en prennent de plus en plus souvent directement aux personnes dont les données ont été subtilisées en les rançonnant à leur tour[124].

Politique de sécurité informatique mise en place dès 2011 à l'ACV

L'ACV a jusqu'à présent été préservée des problèmes majeurs de cyberattaques. Cela s'explique en partie par la priorité accordée depuis une dizaine d'années à la mise en place d'une véritable politique de sécurité des systèmes d'information de l'Etat.

Le vaste chantier de la mise en œuvre d'une politique coordonnée de sécurité informatique à l'Etat a débuté en 2010 avec la création de l'Unité de sécurité des systèmes d'information (USSI). Il s'est poursuivi en 2011 avec l'adoption par le Conseil d'Etat de la « Politique générale de sécurité des systèmes d'information (PGSSI) ». Ce document a fondé les jalons de l'organisation et du déploiement de mesures de sécurité informatique à l'Etat visant à « *s'assurer que les systèmes d'information (SI) soient protégés contre les risques qui menacent leur disponibilité, leur intégrité et leur confidentialité* ». Il définit en outre les responsabilités des différents acteurs.

Système de management de la sécurité de l'information (SMSI) conforme aux bonnes pratiques

Dans le cadre de cette politique, deux importants EMPD ont été acceptés par le Grand Conseil, afin de sécuriser les données gérées par l'Etat mais également pour le développement de la cyberadministration.

Le premier EMPD adopté en 2013, d'un montant de CHF 8.5 millions, a permis une première série de mesures de diminution des risques en prévenant et en détectant d'éventuelles attaques contre les systèmes d'information par la mise en place d'un système de management de la sécurité de l'information (SMSI) conformément aux meilleures pratiques (normes ISO).

Ce projet a en outre permis :

- la création d'un site secondaire offrant la redondance d'un certain nombre d'applications et de plateformes informatiques jugées indispensables ;
- l'établissement d'un plan de secours en cas de catastrophe ;
- la réalisation de mesures de cloisonnement de l'infrastructure ;
- la modernisation de la plateforme de gestion des identités et des accès ;
- la mise en place d'un centre opérationnel de sécurité (SOC) qui traite les incidents de sécurité découlant d'attaques depuis Internet vers l'informatique cantonale[125] ;
- la réalisation d'un programme de formation e-learning sur la sécurité informatique (ESUSI).

[123] Source : « La Suisse harcelée par des hackers », journal Le Temps, le 16.09.2021.
[124] Source : « Rapport semestriel d'activité 2e semestre 2020 », Centre national pour la cybersécurité NCSC.
[125] Le SOC collecte 75 millions d'événements par jour, en moyenne 30 alertes par jour sont générées donnant lieu à 2 à 3 investigations quotidiennes (Source : DGNSI).

La deuxième phase du chantier « sécurité informatique » a démarré avec l'acceptation d'un deuxième EMPD en 2019 prévoyant une série de mesures selon quatre axes[126]. Ces mesures sont encore en cours, principalement les volets concernant la sécurité avec les personnes et la gestion des accès, la priorité ayant porté sur l'architecture et les réponses aux incidents. La DGNSI vise à moyen terme l'accréditation à la norme ISO 27001 sur la sécurité informatique.

Sécurité des équipements et outils informatiques en télétravail

Les accès à distance nécessaires au télétravail avaient déjà été mis en place avant la pandémie de COVID-19 pour répondre aux besoins en télétravail introduit à l'ACV dès 2011. Plusieurs outils d'accès au réseau ACV ont été implantés : tout d'abord Citrix puis Pulse Secure. Ce dernier, privilégié par la DGNSI, est une connexion VPN (Virtual Private Network) chiffrée offrant une bonne protection et permettant de connecter le poste de travail au réseau cantonal comme s'il se trouvait sur le lieu de travail traditionnel.

Sécurité avec les personnes : informations disponibles mais insuffisamment diffusées et connues

Des mesures visant la formation et l'information des collaborateur·trice·s ont été mises en place depuis le démarrage de l'audit : les informations et bonnes pratiques qui figuraient à différents endroits en 2020 (notamment sous « télétravail » ou « sécurité informatique ») sont désormais regroupées dans l'intranet sous l'onglet informatique-téléphonie puis « Sécurité de l'information et cybersécurité » qui comprend notamment un aide-mémoire de sécurité pour les nouveaux collaborateur·trice·s et plusieurs formations en ligne (dont ESUSI).

La DGNSI publie en outre des informations relatives à la sécurité dans la Gazette et tient à jour régulièrement une rubrique « Actualités » qui informe des nouveautés en matière informatique à l'ACV et signale les problèmes de sécurité.

Néanmoins la Cour estime que ces informations mériteraient une diffusion mieux coordonnée : l'information devrait venir directement aux collaborateur·trice·s plutôt qu'il·elle·s ne doivent la chercher. Le résultat des campagnes de « faux-phishing » de la DGNSI mentionnées au point 4.1.2 ont en effet mis en évidence qu'une part non négligeable des employé·e·s ne sont pas encore sensibilisé·e·s aux risques liés à certaines pratiques.

Directive informatique à l'intention du personnel (LPers 50.1) obsolète et incomplète

En outre, la seule directive contraignante à l'intention du personnel traitant de sécurité informatique est la directive LPers 50.1 « *Utilisation d'Internet, de la messagerie électronique, de la téléphonie et du poste de travail* ». Liée à l'article 50 de la loi sur le personnel de l'Etat de Vaud[127], elle a été édictée à l'époque de l'entrée en vigueur de la LPers au début des années 2000. Elle contient des principes généraux qui sont toujours d'actualité, par exemple l'interdiction de modifier la configuration matérielle du poste ou de désinstaller la protection antivirus. Par contre elle contient certaines clauses qui mériteraient une actualisation :

[126] 1. Sécurité avec les personnes : développement de programmes de sensibilisation ; 2. Contrôle des accès : amélioration du contrôle des accès fournisseurs ; 3. Architecture de sécurité : sécurisation des données stockées et des applications ; 4. Réponses aux incidents de sécurité : renforcement et amélioration de l'équipement du SOC.
[127] Art. 50 LPers : *Engagements et devoirs du collaborateur*.

- l'interdiction de se connecter à un réseau via le téléphone mobile (4.3 lettre f) semble étrange, alors que certain·e·s collaborateur·trice·s ne disposant pas d'un wifi à leur domicile, se connectent de cette manière au réseau cantonal pour pratiquer le télétravail. Ce procédé devrait être à nouveau autorisé, du fait du chiffrement de la connexion via VPN.
- le respect de la clause stipulant « *A moins d'être cryptées, les données personnelles jugées sensibles (cf. art. 101 RLPers) ne sont pas transmises par la messagerie électronique* » (4.2 lettre f), nécessite la mise à disposition d'outils adaptés pour certaines entités (voir chapitre 4.2.3).

Pour la Cour, afin de pallier l'obsolescence rapide des pratiques informatiques, cette directive ne devrait pas contenir d'éléments techniques sujets à obsolescence mais se contenter de faire référence à des bonnes pratiques édictées par la DGNSI et visant à prévenir les risques liés à la sécurité des données (recommandation n°19).

Mesures de sécurité de la DGNSI : niveau satisfaisant constaté ou en voie de l'être

La Cour n'a pas réalisé un audit informatique du système en place. Elle a vérifié l'existence des mesures techniques et organisationnelles adoptées. Elle a pu constater, au travers des entretiens avec la DGNSI, de l'examen des différents EMPD et en s'appuyant sur des audits réalisés par d'autres entités, que les mesures de la DGNSI pour sécuriser l'informatique cantonale étaient conformes aux bonnes pratiques ou en voie de l'être.

En effet, conformément à sa mission légale, le Contrôle cantonal des finances (CCF) audite régulièrement la sécurité informatique de l'ACV et a attesté de son bon niveau dans plusieurs rapports.[128]

De même, un rapport d'audit de sécurité de l'information réalisé par une société externe sur mandat de l'APDI « Audit du système d'information du Revenu Déterminant Unifié (SI-RDU) » en 2015, atteste de la politique de sécurité informatique développée par la DGNSI : « *Nous avons observé qu'il existe une politique de sécurité informatique développée par la DSI (…) Nous avons examiné cette politique de sécurité et avons pu constater qu'elle est bien alignée avec les exigences du standard de sécurité ISO 27001* ».

L'aide sollicitée par les entités publiques victimes de cyberattaques témoigne des compétences pointues dans le domaine de la sécurité informatique de la DGNSI : les données du gymnase intercantonal de la Broye ont en effet été restaurées par les spécialistes du Centre opérationnel de sécurité (SOC)[129]. Ces derniers ont également apporté leur support et conseil aux communes touchées par des cyberattaques.

[128] Les rapports du CCF n'étant pas publics, ils ne sont pas nommément cités dans cet audit.
[129] Communiqué du GYB, 18 août 2021 : « Une cyberattaque sur le système informatique du gymnase mise en échec ».

Recommandations sur la sécurité avant tout destinées au personnel et aux services

Renforcer les compétences des collaborateur·trice·s et responsabiliser les services-métiers

La Cour relève toutefois un potentiel d'amélioration concernant la responsabilité des services-métiers d'identifier leurs besoins en sécurité informatique, d'en faire part à la DGNSI et la nécessité d'instaurer une formation de base obligatoire du personnel dans ce domaine (recommandations n°2 et 4 voir chapitre 4.1).

Adapter la directive à l'intention du personnel et consolider une liste de bonnes pratiques

S'il paraît logique que la directive émise par le SPEV ne contienne que des clauses générales, au risque de mentionner des mesures ou pratiques qui deviennent obsolètes avec l'évolution technologique très rapide, elle devrait toutefois se référer à une liste de bonnes pratiques évolutive, facilement accessible. Cette liste manque actuellement, les informations se retrouvant éparpillées dans différentes pages thématiques du site Internet de l'Etat de Vaud.

Traiter certaines pratiques risquées

La Cour a d'autre part identifié des risques liés à l'utilisation possible de périphériques non homologués par la DGNSI. D'autre part, si l'utilisation d'un ordinateur portable professionnel doté de la technologie VPN a été reconnue comme sûre, le fait de pouvoir accéder à sa messagerie professionnelle et réceptionner des fichiers (pouvant contenir des données personnelles sensibles) via son téléphone privé par exemple, nécessite également une analyse. En effet, la plupart des smartphones ont par défaut une sauvegarde dans le cloud, ce dernier étant rarement hébergé en Suisse. Certaines applications peuvent également accéder au carnet d'adresses, à l'agenda, voire à la messagerie électronique.
De plus, la Cour préconise une meilleure réglementation des impressions : le fait de pouvoir, depuis son poste de travail, imprimer sur n'importe quelle imprimante de l'Etat augmente sensiblement le risque de communiquer des données personnelles et sensibles hors du champ des ayants droits. La récente décision de la DGNSI de privilégier les imprimantes multifonction « d'étage » aux imprimantes individuelles nécessite également une analyse au cas par cas, certaines machines se trouvant dans les lieux de fort passage.

Préciser et consolider les règles de bonnes pratiques à respecter par les collaborateur·trice·s en matière de sécurité informatique
Constatation n°19
La DGNSI est en cours de certification ISO 27001 et certaines mesures sont déjà en place. Les règles de bonnes pratiques pour le personnel, figurent sur plusieurs supports : directive LPers 50.1, e-learning ESUSI, site intranet, etc. Seule la directive LPers est contraignante mais elle est incomplète et obsolète (voir constat n°20). Il manque une liste claire et consolidée de bonnes pratiques à laquelle les collaborateur·trice·s devraient obligatoirement se référer. En outre, certains risques ne sont pas traités, notamment le transfert et l'enregistrement de données sur des périphériques non homologués par la DGNSI, le transfert de données via le téléphone portable ou l'ordinateur personnel et la possibilité d'imprimer sur n'importe quelle imprimante de l'Etat depuis son poste fixe sans besoin d'identification.

Recommandation n°19	à la DGNSI
Etablir une liste de bonnes pratiques en matière de sécurité informatique contraignante et à laquelle les dispositions générales LPers pourraient se rapporter ainsi qu'une liste d'outils (e-learning, informations, etc.) regroupées en un seul endroit. Il s'agira d'y régler les points susceptibles de poser des problèmes de sécurité, notamment : • l'utilisation des périphériques non homologués par la DGNSI (clés USB, etc.) ; • la possibilité d'accéder à ses courriels professionnels via le téléphone portable ou l'ordinateur personnels avec la possibilité d'y enregistrer des pièces jointes hors des infrastructures de l'ACV ; • la possibilité d'imprimer sur n'importe quelle imprimante de l'Etat depuis son poste de travail.	

4.3.2 SPEV: CADRE NORMATIF SUR LA RESPONSABILITÉ DU PERSONNEL EN MATIÈRE DE SÉCURITÉ EN PARTIE À RÉVISER

Deux directives sur la responsabilité du personnel en matière de sécurité

Le SPEV a la charge du cadre normatif lié au personnel de l'ACV : la question de la responsabilité des collaborateur·trice·s en matière de sécurité des données traitées est réglée par l'art. 50 LPers alinéa 2[130] qui fait référence à la nécessité de respecter les « *normes en vigueur* ». Deux directives du SPEV traitent de sécurité des données : la directive LPers 50.1 « *Utilisation d'Internet, de la messagerie électronique, de la téléphonie et du poste de travail* » et la directive DT 48.8 sur le télétravail. Le règlement d'application de la loi sur le personnel (RLPers) comprend également un chapitre sur le télétravail qui contient un article sur la protection et la sécurité des données (art. 118e[131]).

La révision de la directive sur le télétravail clarifie les questions de responsabilité du personnel

La première version de la directive DT 48.8 en vigueur jusque fin 2020, ne contenait que quelques éléments relatifs à la sécurité et reprenait en particulier l'article 118 RLPers, sans apporter de précisions supplémentaires : « *Le/la collaborateur-trice qui effectue du télétravail est responsable de la protection des données qu'il traite depuis le lieu de télétravail et il veille au respect du secret de fonction* ». Cet article crée une ambiguïté sur la notion de responsabilité de la sécurité des données traitées qui incomberait au collaborateur·trice·s en télétravail et non plus au responsable du traitement comme spécifié par la LPrD (art. 10).

[130] détaillé au chapitre relatif à la responsabilité des différents acteurs en matière de protection et sécurité des données (point 4.1.1).

[131] Art. 118e RLPers : Confidentialité et protection des données

[1] Le collaborateur accorde une attention particulière au respect du secret de fonction et à la confidentialité des données traitées.

[2] Il est responsable de la sécurité des données au lieu de télétravail. Il s'assure en particulier que les fichiers informatiques et les documents sont protégés contre les accès non autorisés et les vols.

[3] La destruction de documents confidentiels et de ceux contenant des données personnelles s'effectue exclusivement au lieu de travail ordinaire.

[4] Le télétravail depuis un lieu public est interdit.

La révision de la directive DT 48.8 au 1er janvier 2021 a apporté de notables précisions. Son chapitre 10 « *Secret de fonction, sécurité et protection des données* » a ainsi été complété et apporte des précisions sur la notion de responsabilité incombant au personnel en matière de sécurité : interdiction de prêter son ordinateur professionnel à des tiers, obligation de surveiller étroitement le matériel et les documents professionnels durant les trajets, obligation de protéger l'accès au poste de travail par un mot de passe, nécessité de déclarer toute perte ou vol de données sensibles, etc.

Directive LPers 50.1 à réviser

Comme détaillé au point 4.3.1, la directive LPers 50.1 est à réviser. Compte tenu de la différence de rythme entre l'évolution technologique rapide et le processus de révision d'une directive, il est proposé de n'y introduire que des éléments généraux et de faire référence à une liste de bonnes pratiques en matière de sécurité qui serait régulièrement tenue à jour.

Réviser la directive générale traitant de sécurité informatique à l'intention des collaborateur·trice·s	
Constatation n°20	
La seule directive traitant de sécurité informatique à l'intention des collaborateur·trice·s est une directive, liée à l'art. 50 LPers « Engagements et devoirs du collaborateur ». Il s'agit de la directive 50.1 « *Utilisation d'internet, de la messagerie électronique, de la téléphonie et du poste de travail* ». Cette directive élaborée au début des années 2000, n'est plus à jour. Elle contient des éléments obsolètes. La liste détaillée des bonnes pratiques en matière de sécurité informatique ne devrait pas figurer dans cette directive, mais être publiée par la DGNSI car elle est amenée à être adaptée fréquemment (voir constatation n°19).	
Recommandation n°20	**au SPEV**
Réviser les dispositions LPers en matière d'utilisation du matériel informatique en faisant référence aux bonnes pratiques à définir et à actualiser par la DGNSI (voir recommandation n°19). Pour des raisons d'efficacité, il convient de séparer les directives se rapportant au personnel, de celles liées aux mesures informatiques. En effet, les dispositions LPers ne devraient pas comporter de mesures d'ordre techniques, amenées à rapidement évoluer du fait de l'évolution technologique.	

5. CONCLUSION

UN CADRE À CRÉER POUR QUE LES PRINCIPES DE PROTECTION DES DONNÉES SOIENT INTÉGRÉS DANS LES ENTITÉS-MÉTIERS

Au terme de cet audit, des constats généraux se dessinent. L'Administration cantonale vaudoise (ACV), par le biais de la Direction générale du numérique et des systèmes d'information (DGNSI), a mis en place une politique de sécurité informatique. Cette dernière, en voie de certification de conformité aux bonnes pratiques (ISO 27001), offre ainsi un standard de protection aux données personnelles numériques traitées par les entités de l'ACV. Au niveau confidentialité, la Cour relève que les collaborateur·trice·s des entités-métiers sont globalement sensibilisé·e·s au secret de fonction ou au secret professionnel.

Le bouclier de protection formé tant par la culture du secret commune au personnel de l'ACV que par les mesures de sécurité mises en place par la DGNSI, présente toutefois des failles, la plupart du temps d'origine humaine. Le déficit de formation et de sensibilisation régulière du personnel sur les dispositions régissant la protection des données, reconnu par les entités auditées, ainsi que le manque de compétences internes dans ce domaine, génèrent des risques. Des cas de fuites de données se sont produits, essentiellement par maladresse ou inadvertance. Les collaborateur·trice·s ne sont de surcroît pas au fait des règles basiques de sécurité informatique, comme le confirment les tests de faux phishing organisés régulièrement par la DGNSI.

Au niveau stratégique, le Conseil d'Etat et la DGNSI ont pris en compte les enjeux de protection et de sécurité des données, mais de manière relativement récente. En toute logique, la priorité a été donnée dès 2011 à la sécurisation de l'architecture informatique de l'ACV, qui présentait alors de sérieuses lacunes. Les principes de protection des données dans les projets informatiques ont été intégrés ultérieurement et sont mis en œuvre au fil du renouvellement des applicatifs.

Les mesures de protection des données requises par les dispositions légales ne se limitent toutefois pas à la sécurité informatique et à la confidentialité. Leur mise en œuvre est essentiellement du ressort des responsables de traitement, à savoir les entités-métiers. De par leur connaissance du domaine d'activité et de leurs missions, elles sont les seules à même de pouvoir analyser la finalité de la collecte des données personnelles qu'elles gèrent, leur caractère proportionné, leur délai de conservation, leur exactitude, la nécessité de leur transmission et leur besoin de sécurisation. La Cour a constaté qu'aucune entité-métier auditée n'a encore adopté de véritable stratégie portant sur l'ensemble des données personnelles traitées. Aucune n'a non plus adopté de mesures visant à faciliter l'accès des citoyen·ne·s à leurs propres données, qui est un élément important de la législation sur la protection des données. Ces entités-métiers ne sont de surcroît pas ou peu conscientes des responsabilités qui leur incombent.

La situation varie cependant selon les entités. Certaines entités-métiers n'ont entamé aucune démarche pour identifier les données personnelles traitées, accumulant ces dernières sans les trier ou les anonymiser, et n'ont pas non plus entrepris de réflexion sur le besoin de les sécuriser, qu'elles soient enregistrées ou transmises à des tiers. D'autres ont intégré quelques principes et adopté certaines mesures, mais de manière réactive et au coup par coup.

L'examen de cas concrets a révélé quelques manquements au sein des entités-métiers, que la Cour recommande de corriger : lacunes dans les contrats, maîtrise insuffisante de la gestion des accès, manque de contrôle sur le lieu d'hébergement des données sous-traitées, défaut de traçabilité de l'autorisation de transmission, application informatique d'entités délégataires insuffisamment sécurisée, transmission d'adresses courriel de collaborateur·trice·s à des entités externes, etc.

La Cour a surtout relevé un manque de conditions cadres pour orienter et soutenir les entités-métiers dans l'application des dispositions de la LPrD.

L'entité-cadre principale, l'Autorité de protection des données et de droit à l'information (APDI), affiche certes un haut niveau de compétence juridique, mais n'est pas en mesure de surveiller, encadrer et accompagner toutes les entités soumises à cette législation (ACV, communes et entités délégataires d'une tâche publique). La Cour recommande ainsi de créer des compétences internes aux entités de l'ACV par la création d'une formation minimale obligatoire pour tout le personnel et la désignation d'un·e délégué·e interne à ces questions. Quant à l'APDI, la Cour lui recommande de se recentrer sur sa mission de surveillance et de renforcer ses compétences en informatique. D'autres recommandations liées au cadre général portent sur l'adaptation des bases légales des métiers pour offrir une densité normative suffisante au traitement des données. La directive LPers 50.1 sur les bonnes pratiques informatiques pour le personnel doit également être actualisée.

La recommandation principale est adressée aux entités-métiers. Elle vise à leur faire adopter une stratégie interne pour gérer le traitement des données personnelles conformément aux dispositions légales. Cela implique l'identification de toutes les données personnelles traitées, leur analyse et la définition d'une politique systématique en vue d'une bonne application des principes requis.

La mise en place d'un tel concept de protection des données dans chaque entité permettra non seulement de se conformer aux dispositions légales en la matière, mais contribuera à poser les jalons d'une véritable politique de la donnée que l'ACV ambitionne d'élaborer. Cette dernière se doit en effet d'être cohérente dans l'ensemble des entités de l'Etat pour garantir aux citoyen·ne·s le respect du droit à la protection de leurs données que leur confère la Constitution.

Ce n'est que si la sphère privée des usager·ère·s est protégée que la transition numérique voulue par le Conseil d'Etat emportera l'adhésion des citoyen·ne·s.

6. RÉCAPITULATIF DES RECOMMANDATIONS ET REMARQUES DES ENTITÉS AUDITÉES

6.1 RECOMMANDATIONS AU CONSEIL D'ETAT

N°5 (p. 41)	Actualiser les bases légales indispensables à la collecte, au traitement et au transfert des données personnelles comme requis par la LPrD
Dans le cadre de la révision de la LPrD et sur la base du travail d'analyse et de documentation à réaliser par les entités-métiers (voir recommandation n°7), proposer au législateur une adaptation des bases légales « métier » lacunaires en matière de traitement des données personnelles afin de légaliser la collecte, le traitement et la communication de toutes les données personnelles traitées par l'ACV. Cette mise à jour des bases légales doit également concerner les domaines de la police et de la justice afin de se conformer aux exigences du développement des acquis Schengen.	
Position du Conseil d'Etat	Acceptée ☒ Refusée ☐
Justification (en cas de refus) : --	

N°6 (p. 46)	Désigner un·e délégué·e à la protection des données dans chaque entité-métier
Prévoir l'obligation pour chaque entité-métier de désigner parmi les membres de leur personnel, un·e délégué·e à la protection des données, au bénéfice d'une formation spécifique (ou à former), chargé·e de régler les questions courantes de protection des données internes au service et d'être le point de contact pour l'APDI et les administré·e·s.	
Position du Conseil d'Etat	Acceptée ☒ Refusée ☐
Justification (en cas de refus) : --	

N°17 (p. 72)	Rendre obligatoire la déclaration à l' Autorité de protection des données de toute violation de la sécurité des données
Rendre obligatoire l'annonce à l' Autorité de protection des données de toute violation de la sécurité des données touchant des données personnelles sensibles ou entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée pour permettre à l'APDI d'exercer sa tâche de surveillance selon l'art. 36 al. 3 LPrD.	
Position du Conseil d'Etat	Acceptée ☒ Refusée ☐
Justification (en cas de refus) : --	

6.2 REMARQUES DU CONSEIL D'ETAT

canton de vaud
LIBERTÉ ET PATRIE

CONSEIL D'ETAT

Château cantonal
1014 Lausanne

Cour des comptes
Rue de Langallerie 11
1014 Lausanne

Lausanne, le 22 décembre 2021

Audit de la protection des données personnelles dans l'Administration cantonale vaudoise – Projet de rapport pour consultation officielle

Monsieur le Président,
Mesdames les Vice-présidentes,

Votre envoi du 24 novembre 2021 nous est bien parvenu. Il a retenu toute notre attention et nous y répondons comme suit.

L'audit que vous avez réalisé sur la protection et la sécurité des données personnelles dans l'Administration cantonale vaudoise (ci-après : ACV), vous amène à préconiser un certain nombre de mesures visant à améliorer la protection et la sécurité des données personnelles traitées par l'administration. Nous saluons cette démarche et le sens général de ces recommandations, qui rejoignent les principes fondant la Stratégie numérique du Conseil d'Etat adoptée en novembre 2018 et les réflexions en cours dans le cadre des travaux de révision de la loi du 11 septembre 2007 sur la protection des données personnelles (LPrD).

Certaines de ces recommandations sont directement adressées au Conseil d'Etat et nous nous déterminons comme suit à leur sujet :

Ad chapitre 4.2 « Renforcer l'implication des entités-métiers et le contrôle par l'APDI »

Recommandation N°5 *Actualiser les bases légales indispensables à la collecte, au traitement et à la communication des données personnelles comme requis par la LPrD* :

- Nous nous rallions à cette recommandation, d'autant que la révision complète de la LPrD actuellement en cours vise à adapter les bases légales aux révisions des droits fédéral et européen de la protection des données, ainsi qu'aux évolutions technologiques récentes.

- Nous relevons que la mise à jour des normes légales concernant spécifiquement les domaines de la police et de la justice est en cours : l'objectif est de proposer au Grand Conseil d'adopter, à l'instar de la Confédération une base légale répondant aux exigences du développement des acquis Schengen.

Recommandation N°6 *Désigner un·e délégué·e à la protection des données dans chaque entité-métier responsable de traitement* :

- Nous partageons pleinement l'objectif visé par cette recommandation, à savoir le renforcement des compétences en matière de protection des données personnelles au sein des entités chargées de collecter ou de traiter ces données. Des réflexions sont ainsi en cours, dans le cadre des travaux de révision de la LPrD, pour déterminer le dispositif le plus

efficient à mettre en place à cette fin. Dans ce contexte, la possibilité de désigner un-e délégué-e à la protection des données personnelles sera étudiée.

Recommandation N° 17 *Rendre obligatoire la déclaration à l'autorité de protection des données de toute violation de la sécurité des données*

- Nous nous rallions à cette recommandation. L'actualité récente illustre la nécessité de mettre en place une procédure d'annonce afin de limiter les dommages éventuels ; il est ainsi prévu, dans le cadre des travaux de révision de la LPrD, d'inclure une proposition de base légale portant sur ce point.

Nous vous prions de croire, Monsieur le Président, Mesdames les Vice-présidentes, à l'assurance de nos sentiments les meilleurs.

AU NOM DU CONSEIL D'ETAT

LA PRESIDENTE	LE CHANCELIER
Nuria Gorrite	Aurélien Buffat

6.3 ENTITÉS-CADRES

6.3.1 RECOMMANDATIONS À L'AUTORITÉ DE PROTECTION DES DONNÉES ET DE DROIT À L'INFORMATION (APDI)

N°1 (p. 34)	Informer les services de leur responsabilité en matière de protection des données
Rappeler formellement aux responsables de traitement leur responsabilité en matière de respect des dispositions LPrD (en accord avec l'art. 37 LPrD, al. 1 lettre b).	
Position de l' APDI	Acceptée ☒ Refusée ☐
Justification (en cas de refus) : --	

N°15 (p. 69)	Renforcer les compétences de l'APDI en informatique
Renforcer les compétences de l'APDI en informatique pour lui permettre de mieux appréhender les questions techniques posées par les systèmes et les technologies d'information, afin d'être en mesure de remplir sa mission de surveillance de manière autonome.	
Position de l' APDI	Acceptée ☒ Refusée ☐
Justification (en cas de refus) : --	

N°16 (p. 71)	Renforcer la mission de l'APDI en matière de surveillance de l'application
Renforcer la mission de l'APDI en matière de surveillance de l'application de la LPrD en réalisant davantage d'audits ciblés dans les entités soumises à la LPrD.	
Position de l' APDI	Acceptée ☒ Refusée ☐
Justification (en cas de refus) : --	

6.3.2 REMARQUES DE L'AUTORITÉ DE PROTECTION DES DONNÉES ET DE DROIT À L'INFORMATION (APDI)

canton de vaud

Autorité de protection des données et de droit à l'information

Rue Saint-Martin 6
Case postale 5485
1002 Lausanne

Par courrier recommandé

Cour des Comptes
A l'attention de Monsieur Bolay
Président
A l'attention de Madame Schwaar
Vice-présidente
Rue Langallerie 11
1014 Lausanne

Réf : 21_0974

Lausanne, le 15 décembre 2021

Audit de protection des données personnelles dans l'Administration cantonale vaudoise – Projet de rapport pour consultation officielle

Monsieur le Président,
Madame la Vice-présidente,

J'accuse bonne réception de votre courrier du 24 novembre 2021 relatif à l'objet cité sous rubrique.

Dans le délai imparti, je vous confirme accepter sans réserve les trois recommandations formulées à l'attention de l'Autorité de protection des données et de droit à l'information au chapitre six du projet de rapport. S'agissant de la première recommandation, un plan d'action sera établi dans les meilleurs délais. En ce qui concerne la seconde, un renfort technique apparaît effectivement indispensable au bon fonctionnement de l'Autorité. Cela contribuera au surplus à renforcer son indépendance. Finalement, l'Autorité réalisera davantage de surveillance, en fonction de ses ressources financières et humaines disponibles. Dans tous les cas, je serai particulièrement attentive à ce qu'un équilibre soit maintenu entre les entités soumises à la loi.

Je vous remercie pour la qualité de cet audit, dont les recommandations s'inscrivent dans le cadre des futurs développements législatifs cantonaux. Sa teneur me conforte dans la nécessité de poursuivre nos efforts afin que les compétences en matière de protection des données des entités soumises à la loi continuent à s'accroître.

En demeurant à votre entière disposition pour tout renseignement complémentaire, je vous prie de croire, Monsieur le Président, Madame la Vice-présidente, à l'assurance de ma considération distinguée.

Cécile Kerboas

Préposée à la protection des données

Annexe : formulaire recommandations
Copie : Chancellerie d'Etat, pour information

6.3.3 RECOMMANDATIONS À LA DIRECTION GÉNÉRALE DU NUMÉRIQUE ET DES SYSTÈMES D'INFORMATION (DGNSI)

N°2 (p. 35)	Informer les services de leur responsabilité en matière de sécurité informatique et gestion de leurs processus
Rappeler formellement aux chef·fe·s de service leur responsabilité découlant du Règlement sur l'informatique cantonale (RIC) et de la Politique générale de sécurité des systèmes d'information (PGSSI), en matière de définition de leurs besoins en sécurité informatique, d'optimisation de leurs processus et de documentation de leur activité. Les services doivent en outre s'assurer que leurs collaborateur·trice·s et leurs sous-traitants appliquent la politique générale de sécurité.	
Position de la DGNSI	Acceptée ☒ Refusée ☐
Justification (en cas de refus) : --	

N°18 (p. 76)	Adapter tous les outils, modèles et procédures informatiques pour renforcer la protection des données
Pour répondre aux impératifs de protection des données personnelles et des données à protéger dans le domaine numérique et répondre à l'objectif prioritaire du plan directeur cantonal informatique, la DGNSI doit poursuivre l'adaptation de ses processus, modèles et outils. Il est notamment nécessaire, en collaboration au besoin avec les entités-métiers : • d'adapter la directive et les modèles du processus d'élaboration des schémas directeurs informatiques sectoriels du SI ; • d'établir une cartographie des données numériques personnelles et personnelles et sensibles ainsi que celles soumises au secret de fonction gérées par les services (en complétant par exemple l'application Cartomega) ; • de réactualiser les dispositions contractuelles DGNSI avec les sous-traitants.	
Position de la DGNSI	Acceptée ☒ Refusée ☐
Justification (en cas de refus) : --	

N°19 (p. 81)	Préciser et consolider les règles de bonnes pratiques à respecter par les collaborateur·trice·s en matière de sécurité informatique
Etablir une liste de bonnes pratiques en matière de sécurité informatique contraignante et à laquelle les dispositions générales LPers pourraient se rapporter ainsi qu'une liste d'outils (e-learning, informations, etc.) regroupées en un seul endroit. Il s'agira d'y régler les points susceptibles de poser des problèmes de sécurité, notamment : • l'utilisation des périphériques non homologués par la DGNSI (clés USB, etc.) • la possibilité d'accéder à ses courriels professionnels via le téléphone portable ou l'ordinateur personnels avec la possibilité d'y stocker des pièces jointes ensuite sauvegardées hors des infrastructures de l'ACV. • la possibilité d'imprimer sur n'importe quelle imprimante de l'Etat depuis son poste de travail.	
Position de la DGNSI	Acceptée ☒ Refusée ☐
Justification (en cas de refus) : --	

6.3.4 REMARQUES DE LA DIRECTION GÉNÉRALE DU NUMÉRIQUE ET DES SYSTÈMES D'INFORMATION (DGNSI)

canton de vaud

Direction générale du numérique et des systèmes d'information

Avenue de Longemalle 1
1020 Renens

Cour des comptes
Madame Valérie Schwaar
Rue de Langallerie 11
1014 Lausanne

Réf. : DGI/MBT/avx
Affaire traitée par : Sam Vuilleumier
No téléphone : 021 316 95 36

Renens, le 15 décembre 2021

Audit de protection des données personnelles dans l'ACV - Recommandations de la Cour de comptes à la DGNSI

Madame,

Votre communication du 25 novembre du projet de rapport cité en titre a retenu toute notre attention.

Nous avons pris connaissance de vos constats d'audit et de vos recommandations. Nous n'avons pas de remarque particulière à formuler sur les risques relevés et présentés.

Les 3 recommandations attribuées à la DGNSI sont acceptées en l'état. Le plan de leur mise en œuvre sera détaillé de manières pragmatique et concrète en tenant compte des contraintes métier et des ressources. Il intégrera une feuille de route qui sera suivie par les directions concernées de la DGNSI.

Nous vous prions de trouver dans l'annexe jointe, comme souhaité, les déterminations de la Direction générale du numérique et des systèmes d'information sur les recommandations qui nous concernent.

Nous restons à votre disposition pour tout renseignement complémentaire et vous adressons, Madame, l'expression de nos sentiments distingués.

Le Directeur général

Patrick Amaru

Le Directeur de la sécurité du système d'information

Marc Barbezat

Annexe : Déterminations DGNSI sur les trois recommandations

Copie : SG-DIRH

Direction générale du numérique et des systèmes d'information - DGNSI
Avenue de Longemalle 1, 1020 Renens
www.vd.ch - Tél. +41 21 316 26 00

6.3.5 RECOMMANDATIONS AU SERVICE DU PERSONNEL (SPEV)

N°3 (p. 36)	Informer les services de leur responsabilité en matière de formation (en sécurité et en protection des données)
Rappeler formellement aux chef·fe·s de service leur responsabilité de garantir un niveau adéquat des compétences des collaborateur·trice·s en matière de protection et sécurité des données et, le cas échéant, prévoir une formation pour les collaborateur·trice·s en fonction du besoin nécessité par leur fonction (art. 38 al. 1 LPers).	
Position du SPEV	Acceptée ☒ Refusée ☐
Justification (en cas de refus) : --	

N°4 (p. 39)	Mettre en place une formation minimale et obligatoire en matière de protection des données, de secret de fonction et de sécurité informatique
Instaurer une formation basique minimale obligatoire sur les devoirs et obligations du personnel de l'Etat dans les trois domaines que sont la protection des données (au sens de la LPrD), la sécurité informatique et le secret de fonction. Cette formation est destinée aux collaborateur·trice·s n'ayant pas eu de formation spécifique au préalable dans ces domaines.	
Position du SPEV	Acceptée ☒ Refusée ☐
Justification (en cas de refus) : --	

N°20 (p. 83)	Réviser la directive générale traitant de sécurité informatique à l'intention des collaborateur·trice·s
Réviser les dispositions LPers en matière d'utilisation du matériel informatique en faisant référence aux bonnes pratiques à définir et à actualiser par la DGNSI (voir recommandation n°19). Pour des raisons d'efficacité, il convient de séparer les directives se rapportant au personnel, de celles liées aux mesures informatiques. En effet, les dispositions LPers ne devraient pas comporter de mesures d'ordre techniques, amenées à rapidement évoluer du fait de l'évolution technologique.	
Position du SPEV	Acceptée ☒ Refusée ☐
Justification (en cas de refus) : --	

6.3.6 REMARQUES DU SERVICE DU PERSONNEL (SPEV)

canton de vaud

Service du personnel

Rue Caroline 4
1014 Lausanne

Cour des comptes
Mme Valérie Schwaar, Vice-présidente
Rue de Langallerie 11
1014 Lausanne

Réf. : PCT
Philippe.Chaubert@vd.ch
T 41 21 316 19 01

Lausanne, le 15 décembre 2021

Audit de protection des données personnelles dans l'ACV

Madame la Vice-présidente

Conformément à votre demande, je vous adresse ci-joint la détermination du SPEV quant aux recommandations de la Cour des comptes émises dans le cadre de l'audit de protection des données personnelles dans l'Administration cantonale vaudoise (ACV).

D'une manière générale, les recommandations adressées au SPEV s'inscrivent en concordance avec les constatations que nous avons pu faire, notamment lors de la nouvelle formation des cadres. Par ailleurs, de plus en plus sollicités sur la question, nous avons déjà constitué un groupe de travail composé de spécialistes du domaine, en charge de proposer courant 2022 une formation pour les cadres, en particulier pour les cadres supérieurs et les chef-fe-s de service sur le thème de la sécurité et la protection des données.

Ces travaux nous permettront d'élaborer ensuite une formation de base destinée à l'ensemble des collaborateurs-trices de l'ACV sur les devoirs et obligations du personnel de l'Etat dans les domaines de la protection des données et du secret de fonction. Il s'agira également d'adapter la formation déjà disponible actuellement sur la sécurité informatique. Ces formations seront intégrées aux formations obligatoires du cursus d'intégration des nouveaux-velles collaborateurs-trices de l'ACV. Dans ce cadre-là, nous allons examiner les possibilités de développer un « monitoring » du suivi et de la réussite des modules de formation obligatoires.

Après avoir rappelé aux autorités d'engagement leurs rôles et responsabilités quant à la formation de leurs collaborateurs-trices, notamment dans le domaine de la protection des données, le SPEV leur proposera un appui à la mise en œuvre d'une formation adaptée aux besoins et spécificités de leur entité. Ces formations pourraient se concevoir sous forme présentiel, webinaire ou e-learning en fonction des situations.

canton de vaud | Service du personnel

Audit de protection des données personnelles dans l'ACV

Dans l'attente d'une révision des dispositions de la LPers et du RLPers, le SPEV proposera au Conseil d'Etat, en collaboration avec la DGNSI, l'adoption d'une directive LPers transitoire conforme aux principes de la Stratégie numérique du Conseil d'Etat, traitant des droits et obligations du personnel en matière de sécurité informatique, à l'exclusion des aspects techniques et matériels du ressort de la DGNSI.

En vous remerciant de nous avoir consultés sur vos recommandations, je vous prie de recevoir, Madame la Vice-présidente, mes salutations les meilleures.

Philippe Chaubert

Chef de service

Annexes mentionnées

Copie
- M. Michel Rubattel, Secrétaire général DIRH

6.4 ENTITÉS-MÉTIERS

6.4.1 RECOMMANDATION A L'ENSEMBLE DES ENTITÉS-MÉTIERS

N°7 (p. 47)	Identifier toutes les données personnelles ainsi que celles soumises au secret de fonction traitées au sein de l'entité ainsi que leurs flux et documenter les mesures de protection

- Identifier toutes les données (personnelles, sensibles ainsi que les profils de personnalité) traitées dans les fichiers informatiques ou dans les registres papier puis établir, notamment à partir du registre des fichiers selon l'art. 19 LPrD, une cartographie de celles-ci ainsi que de leur flux. Cela s'inscrit dans l'obligation des services de documenter leurs processus (art. 10 al 2 RIC).
- Faire de même avec les données personnelles soumises au secret de fonction, qui sont à définir au préalable.
- Une fois la cartographie des applicatifs et registres contenant ces types de données réalisée, documenter les mesures adoptées pour se conformer à la LPrD (art. 10) et pour assurer la sécurité de ces données en général.
- Vérifier et documenter les bases légales du traitement des données personnelles identifiées.
- Au besoin, compléter le registre des fichiers, si la démarche de documentation a révélé que ce dernier n'était pas complet.

Position des 8 entités-métiers auditées

1. DGEO	Acceptée ☒	Refusée ☐	**2. OPS**	Acceptée ☒	Refusée ☐
3. SAN	Acceptée ☒	Refusée ☐	**4. DIRIS**	Acceptée ☒	Refusée ☐
5. OMC	Acceptée ☒	Refusée ☐	**6. OCBE**	Acceptée ☒	Refusée ☐
7. DFAJ	Acceptée ☒	Refusée ☐	**8. SEPS**	Acceptée ☒ ☐	Refusée ☐

Justification (en cas de refus) DGEO: --

Justification (en cas de refus) OPS: --

Justification (en cas de refus) SAN: --

Justification (en cas de refus) DIRIS: --

Justification (en cas de refus) OMC: --

Justification (en cas de refus) OCBE: --

Justification (en cas de refus) DFAJ: --

Justification (en cas de refus) SEPS: --

6.4.2 RECOMMANDATIONS SPÉCIFIQUES AUX ENTITÉS-MÉTIERS

- **À L'OFFICE DE PSYCHOLOGIE SCOLAIRE (OPS)**

N°8 (p. 52)	Recueillir l'accord par écrit en cas de communication de données sensibles entre professionnel·le·s impliqué·e·s dans la prise en charge de l'élève

En cas de communication de données personnelles sensibles entre professionnel·le·s impliqué·e·s dans la prise en charge de l'élève en matière de pédagogie spécialisée, recueillir l'accord par écrit des parents, voire de l'élève, pour assurer une traçabilité des dispositions prévues à l'art 63 al. 1 LPS.

Position de l'OPS Acceptée ☐ Refusée ☒

Justification (en cas de refus) : La LPS demande que l'on obtienne le consentement et c'est ce à quoi nous nous s'engageons. Elle ne demande pas que l'on apporte la preuve de ce consentement. Pour les très rares situations que cela pourrait concerner, l'exigence de l'écrit qui est demandée est disproportionnée.

D'ailleurs notre mode de fonctionnement requiert parfois que le consentement soit implicite, par exemple, lors d'un réseau auquel participent de nombreux professionnels et les parents et même si les éléments importants transmis ont été discutés. Un accord écrit des parents lors de la première consultation n'est pas suffisant et obtenir au préalable leur accord sur chaque élément qui pourrait être évoqué en séance rendrait la pratique des réseaux impossibles.

Recueillir l'accord écrit des parents entraîne une charge administrative importante et n'apporte pas plus de garantie probante de l'adhésion des parents.

Proposition alternative : Faire figurer dans le journal d'intervention de chaque dossier, notamment lors de la première séance et à chaque fois que cela est nécessaire, la mention explicite de l'information et de l'accord oral des parents. On inscrirait ainsi le consentement dans une vraie logique dynamique qui tient compte de la possible évolution de l'accord des parents.

Remarque de la Cour : Si la loi exige l'accord des parents, voire de l'élève, elle ne dit effectivement rien de sa forme. Il peut en effet être valablement exprimé oralement, mais dans ce cas la preuve est plus difficile à rapporter. Une consignation dans le journal comme proposé n'est pas une preuve absolue mais c'est déjà un indice important.

La Cour admet cette proposition alternative, en précisant toutefois que :

- Un consentement ne peut pas être implicite ;
- Un consentement n'est valable que s'il est éclairé, soit si la personne a été complètement informée dans des termes qu'elle comprend. À cet égard, une information écrite serait bienvenue (au moins en termes généraux), car elle clarifie les informations transmises et permet à la personne concernée de les consulter ultérieurement, sans le stress lié à l'entretien avec une autorité.

- **AU SERVICE DES AUTOMOBILES ET DE LA NAVIGATION (SAN)**

N°9 (p. 54)	Compléter les dispositions contractuelles liés à l'application VIACAR afin de garantir l'hébergement des données en Suisse
Dans le cadre des dispositions contractuelles liées au mandat de gestion de l'application informatique traitant la gestion de l'admission des véhicules et des personnes à la circulation routière et à la navigation du SAN, compléter les conditions générales de la CSI avec une clause précisant l'obligation d'héberger les données en Suisse.	
Position du SAN	Acceptée ☒ Refusée ☐
Justification (en cas de refus) : --	

- **À LA DIRECTION DE L'INSERTION ET DES SOLIDARITÉS (DIRIS)**

N°10 (p. 57)	Annoncer le système d'information relatif au suivi social des réfugié·e·s géré par le Centre social des réfugiés (CSIR) au registre des fichiers de l'APDI
Déclarer tous les fichiers correspondant à la définition de l'art. 4 LPrD, notamment le système d'information relatif au suivi social des réfugié·e·s géré par le Centre social des réfugiés (CSIR), à l'APDI pour intégration au registre des fichiers prévu à l'art. 19 al. 1 LPrD.	
Position de la DIRIS	Acceptée ☒ Refusée ☐
Justification (en cas de refus) : --	

N°11 (p. 57)	Compléter la convention de délégation d'une tâche publique à des entités externes avec une clause sur le respect du secret de fonction
Compléter la convention de collaboration liant la Direction générale de la cohésion sociale et l'organisme prestataire lui délégant la tâche de mesures de suivi dans le cadre du programme de formation pour les jeunes adultes en difficulté (FORJAD) en précisant la nécessité de respecter le secret de fonction.	
Position de la DIRIS	Acceptée ☒ Refusée ☐
Justification (en cas de refus) : --	

- **À L'OFFICE DU MÉDECIN CANTONAL (OMC)**

N°12 (p. 61)	Renforcer les mesures de sécurité de la plateforme internet des traitements agonistes opioïdes (TAO)
Renforcer les mesures de sécurité de l'application informatique TAO et, lors du renouvellement des contrats liés à cette application, les adapter conformément au RIC et à la LPrD : • Faire signer le contrat informatique par la DGNSI, cette dernière étant responsable selon le RIC de la gestion des relations avec les fournisseurs. • Intégrer une clause de respect de la LPrD et du secret de fonction dans le contrat informatique et dans le contrat de prestation avec Unisanté. • Clarifier la question de la responsabilité du traitement entre l'OMC et Unisanté. • Centraliser la gestion des accès (entrées ET sorties).	
Position de l'OMC	Acceptée ☒ Refusée ☐
Justification (en cas de refus) : --	

- **À LA DIRECTION FINANCES ET AFFAIRES JURIDIQUES (DFAJ)**

N°13 (p.64)	Intégrer systématiquement des clauses de respect de la LPrD et du secret de fonction dans les dispositions contractuelles de délégation d'une tâche publique
Intégrer systématiquement dans les contrats de délégation d'une tâche publique impliquant le traitement de données personnelles et sensibles les clauses de respect de la LPrD et du secret de fonction.	
Position de la DFAJ	Acceptée ☒ Refusée ☐
Justification (en cas de refus) :	

- **AU SERVICE D'ÉDUCATION PHYSIQUE ET DES SPORTS (SEPS)**

N°14 (p. 66)	Gérer en interne l'envoi d'informations aux professeur·e·s d'éducation physique pour promouvoir des manifestations sportives
Gérer en interne au SEPS l'envoi à destination des enseignant·e·s en éducation physique d'informations de promotion d'un événement sportif auprès des élèves vaudois. Procéder à un envoi en copie cachée et sans communication des adresses électroniques individuelles à des prestataires externes à l'ACV.	
Position du SEPS	Acceptée ☒ Refusée ☐
Justification (en cas de refus) :	

6.4.3 REMARQUES DES ENTITÉS-MÉTIERS

- **DIRECTION GÉNÉRALE DE L'ENSEIGNEMENT OBLIGATOIRE (DGEO)**

canton de vaud

Direction générale
de l'enseignement obligatoire
et de la pédagogie spécialisée

Le Directeur général

Rue de la Barre 8
1014 Lausanne

Madame Valérie Schwaar
Magistrate – Cour des comptes
Rue Langallerie 11
1014 Lausanne

Réf. : GVI/vs

Lausanne, le 13 décembre 2021

Audit de protection des données personnelles dans l'ACV – V/projet de rapport

Madame la Magistrate,

Pour faire suite à votre projet de rapport relatif à l'objet précité et comme demandé dans votre courriel du 24 novembre dernier, je vous transmets ci-après la brève prise de position souhaitée.

L'audit met en évidence l'importance de sensibiliser les utilisateurs de nos systèmes d'information puisque le fait de disposer de documents de référence ne semble pas toujours suffisant. A l'appui de cette observation, il faut tenir compte du fait que la formation des utilisateurs est prévue de manière large et complète au moment de l'introduction des outils et lorsque des modifications substantielles sont introduites. Nous prenons acte du fait que cette sensibilisation doit être répétée de manière régulière aux utilisateurs et utilisatrices de nos systèmes d'information.

L'analyse des données sensibles et des données personnelles fait l'objet de la mise à jour d'une cartographie et des fonctions qui y ont accès, ceci afin d'identifier celles et ceux des utilisateurs qui devront recevoir les indications indispensables et nécessaires au respect de la protection de celles-ci.

En guise de remarque conclusive, je signale à toute fin utile, que le rapport distingue l'ex-SESAF et l'ex-DGEO, services désormais réunis au sein d'une structure unifiée sous l'appellation « Direction générale de l'enseignement obligatoire et de la pédagogie spécialisée » dont l'acronyme reste DGEO par souci de simplification.

En vous remerciant de la suite donnée à ce courrier, je vous prie de croire, Madame la Magistrate, à l'expression de mes sentiments les meilleurs.

Giancarlo Valceschini

***Annexe** : Recommandation n° 7 (également envoyée par courriel)*

Département de la formation, de la jeunesse et de la culture (DFJC)
Direction générale de l'enseignement obligatoire et de la pédagogie spécialisée (DGEO)
www.vd.ch/dgeo – T + 41 21 316 32 32 – Email : info.dgeo@vd.ch

- **OFFICE DE PSYCHOLOGIE SCOLAIRE (OPS)**

canton de vaud
LIBERTÉ ET PATRIE

Direction générale de l'enseignement obligatoire et de la pédagogie spécialisée (DGEO)

Direction psychologie, psychomotricité, logopédie en milieu scolaire (DPPLS)

Rue de la Barre 8
1014 Lausanne

Cour des comptes
Mme Valérie Schwaar, Magistrate
Rue Langallerie 11
1014 Lausanne

Réf. : RGR

Lausanne, le 15 décembre 2021

Prise de position sur le rapport de l'audit de protection des données personnelles dans l'ACV

Madame la Magistrate,

Pour rappel, l'office de psychologie scolaire (OPS) qui appartenait au Service de l'enseignement spécialisé et d'appui à la formation (SESAF) est devenu au 1er août 2021, la Direction psychologie, psychomotricité, logopédie en milieu scolaire (DPPLS) à la Direction générale de l'enseignement obligatoire et de la pédagogie spécialisée (DGEO).

Comme je l'ai évoqué avec vous, la question de la protection des données est au cœur de nos trois métiers, de notre fonctionnement, de nos codes de déontologie et même de nos formations.

Le nouvel outil informatique (GI-PSAF-OGEMI) prévu pour 2022 permettra de remplacer les dossiers papier par une gestion électronique des dossiers et intègre complètement la dimension de la protection des données, en à ce titre répondra à la recommandation 7.

Dans le cadre de vos deux recommandations pour l'OPS devenue DPPLS :
- nous acceptons la recommandation 7,
- nous proposons une alternative à la recommandation 8.

Les arguments sont détaillés dans le document annexé comme demandé.

En vous souhaitant une bonne réception, nous vous adressons nos respectueux messages.

Raphaël Gerber
Directeur général adjoint

Annexe
- Prise de position sur les deux recommandations

Département de la formation, de la jeunesse et de la culture (DFJC)
Direction générale de l'enseignement obligatoire et de la pédagogie spécialisée (DGEO)
Direction psychologie, psychomotricité, logopédie en milieu scolaire (DPPLS)
T +41 21 316 54 00 – Courriel : info.dppls@vd.ch – www.vd.ch/dppls

- **SERVICE DES AUTOMOBILES ET DE LA NAVIGATION (SAN)**

canton de vaud

Service des automobiles et de la navigation

Direction

Av. du Grey 110
1014 Lausanne

Cour des comptes
Mme Valérie Schwaar, Magistrate
Rue de Langallerie 11
1014 Lausanne

Réf. : DIT/SAN/PCY/EFE

Lausanne, le 14 décembre 2021

Audit de la protection des données personnelles dans l'Administration cantonale vaudoise – Consultation – Projet de rapport

Madame,

Je me réfère à votre courriel du 24 novembre 2021 m'invitant à prendre position sur les recommandations adressées à mon service dans le cadre du rapport cité en titre, dont le contenu a retenu ma meilleure attention.

De manière générale, ce rapport apporte des éléments importants et pourra servir de base pour sensibiliser encore plus les collaborateur-trice-s de mon service aux exigences de la protection des données. Les éléments de ce rapport seront notamment pris en compte dans les développements futurs.

Ainsi, le SAN a pris bonne note des différentes recommandations figurant dans le rapport ; les deux qui le concernent spécifiquement, à savoir les recommandations N° 7 et N° 9, sont acceptées.

Cela étant, certaines mesures nécessiteront des coordinations entre les différentes entités concernées, plus particulièrement entre les entités métiers et le SPEV et la DGNSI concernant les mesures N° 3 et 4 (formation) et N° 18 (cartographie des données). Il pourrait être judicieux de prévoir une telle coordination en amont.

En vous remerciant pour la bonne collaboration, je vous adresse, Madame, mes meilleures salutations.

Pascal Chatagny
Chef de service

Annexe : liste récapitulative SAN

Service des automobiles et de la navigation
www.vd.ch/san – T + 41 21 316 89 67 – info.auto@vd.ch

- **DIRECTION DE L'INSERTION ET DES SOLIDARITÉS (DIRIS) ET OFFICE CANTONAL DES BOURSES D'ÉTUDES ET D'APPRENTISSAGE (OCBE)**

canton de vaud

Direction générale de la cohésion sociale (DGCS)

Bâtiment administratif
de la Pontaise
Av. des Casernes 2
1014 Lausanne

Cour des comptes
Madame Valérie **Schwaar**
Magistrate
Rue Langallerie 11
1014 Lausanne

Direction
Référence F. Ghelfi
Tél. 021 316 51 45
e-mail : fabrice.ghelfi@vd.ch

Lausanne, le 17 décembre 2021

Audit de la protection des données personnelles dans l'Administration cantonale vaudoise – Consultation sur projet de rapport d'audit

Madame la Magistrate,

Accusant bonne réception du projet de rapport cité en titre, nous vous adressons, ci-après et dans le respect du délai aimablement prolongé par vos soins, nos déterminations y relatives.

En liminaire, il convient de souligner que les entités-métiers (dont l'OCBE et la DIRIS audités au sein de notre Direction générale) sont conscientes des obligations qui leur incombent en matière de protection et de sécurité des données personnelles. A notre sens, ceci en relation avec les constats établis en pages 33 et 34 du projet de rapport, il s'agirait plutôt en pratique de mieux expliciter le niveau de compétences et de soutien qui peut être requis des entités-cadres de l'ACV pour contribuer à l'amélioration uniforme et continue de ces principes. A titre d'exemple, si les entités-métiers doivent s'assurer que leurs sous-traitants adoptent des mesures de sécurité appropriées, il paraîtrait opportun qu'une méthodologie commune de surveillance (sorte de check-list ou autre outil standard de contrôle) puisse être définie, en vue ensuite de son adaptation selon le niveau du risque identifié.

Concernant les dispositions spéciales de la LASV en matière de collecte et de communication de données personnelles, ceci en relation avec les remarques éditées en page 40 du rapport, nous tenons notamment à vous signaler les articles 30, 31a al. 3, 38 et 39b LASV ainsi que 3c RLASV qui contiennent, entre autres, les bases légales fondant les accès aux données disponibles au moyen d'une procédure d'appel. D'autres normes (parfois même fédérales comme par exemple les articles 11 et 12 de la loi du 17 juin 2005 sur le travail au noir), légitiment par ailleurs également le traitement des données opérées par les autorités d'aides sociales.

S'agissant de l'information aux collaborateurs-trices relative à leurs obligations en matière de protection des données et aux sanctions en cas de non-respect, nous souhaiterions préciser que chaque personne ayant accès aux applicatifs de gestion des aides individuelles au sein de l'OCBE et de la DIRIS, a également accès au SI-RDU. Chacun-e d'entre elle a donc signé la déclaration de confidentialité dont il est fait mention à la page 44 du projet de rapport et a donc déjà été dûment instruite par ce biais.

Néanmoins, les efforts en matière de protection et sécurité des données ainsi que de formation et information des collaborateurs-trices seront poursuivis, notamment dans le

cadre du projet du nouveau SI Bourses dont le lancement est prévu en 2022 en vue du remplacement de l'actuelle solution, laquelle ne permet plus d'intégrer des évolutions.

En relation avec les constats établis en page 56 du projet de rapport, nous précisons en outre que, depuis le mois de juin écoulé, l'applicatif PROGRES a été remplacé par le système d'information MAORI qui permet, outre l'octroi du revenu d'insertion, de gérer le parcours de réinsertion des bénéficiaires de l'aide sociale, notamment au moyen d'un journal des évènements renseigné tant par l'assistant-e social-e que par le-la gestionnaire administratif de dossier. Un module a également été implémenté afin de permettre à la DIRIS de gérer la facturation des mesures socio-proessionnelles dispensées par ses partenaires. Nous vous confirmons par ailleurs que MAORI permet la segmentation des accès. Ceci étant dit, et pour autant que le journal social puisse être qualifié de fichier, puisque sa structure se rapporte en général uniquement au bénéficiaire RI du dossier concerné, l'annonce de ce dernier nous paraît être intégrée à celle de MAORI dans la mise à jour des fichiers de la DGCS auprès de l'APDI.

Par ailleurs, concernant le recours à la plateforme Partage.vd.ch pour l'échange d'informations entre collaborateurs-trices (page 56 du projet de rapport), il est notoire que pour une autorité d'aide sociale (comme pour les autorités sanitaires ou de poursuites pénales et administratives) le partage interne de données, par définition majoritairement sensibles, représente le corolaire nécessaire et inévitable à l'accomplissement de sa mission. L'abandon de la messagerie standard au profit d'une autre solution devrait ainsi inévitablement intégrer une dimension d'efficience. Le besoin étant notoire, il reste à définir une solution pragmatique et aussi uniforme que possible pour les entités concernées.

Enfin, nous vous soumettons, ci-après, quelques amendements au projet de rapport :

- page 10 : introduire une note de bas de page pour indiquer que l'OCBE a déclaré ses fichiers dans le cadre de la constitution du registre des fichiers DGCS (cf. note de bas de page 104, page 63) ;
- page 55 : « La Direction de l'insertion et des solidarités (DIRIS) est l'une des trois directions qui composent la Direction générale de la cohésion sociale (DGCS) :
    - Le pôle « Prévention et solidarités » s'occupe de la prise en charge des victimes de violence, de l'appui aux bénéficiaires de prestations complémentaires à l'AVS/AI hébergés en logements protégés, du soutien aux proches-aidant·e·s, de la lutte contre le surendettement et du développement des solidarités sous toutes ses formes.
    - Le pôle « Appui social et orientation » gère le fonds cantonal de lutte contre la précarité, fournit des prestations d'appui et d'orientation dans le cadre du programme de Formation pour jeunes adultes en difficulté (FORJAD), est responsable du financement des structures d'hébergement d'urgence du canton, du pilotage de la Centrale des Solidarités (« orientation accompagnée » de la population vaudoise en situation de vulnérabilité) et de la formation des assistant-e-s sociaux des régions d'action sociale.
    - Le pôle « Insertion socio-professionnelle » gère le dispositif des mesures d'insertion des bénéficiaires du RI non suivis par les ORP et les Mesures de Transition visant l'insertion des jeunes adultes émargeant au RI (suivi des bénéficiaires, bilan des mesures et facturation, gestion des relations avec les mandataires externes chargés d'assurer le suivi social des bénéficiaires, etc.) ;

Direction générale de la cohésion sociale - Département de la santé et de l'action sociale
www.vd.ch/dgcs – T +41 (0)21 316 52 21
info.dgcs@vd.ch

- page 55, 4e §: préciser que depuis juin 2021 l'application MAORI a remplacé PROGRES en introduisant un volet informatique dédié à l'appui social (y compris le journal de suivi du bénéficiaire) ;
- page 56 dernière phrase : nous proposons de supprimer purement et simplement cette phrase puisque sa formulation laisse entendre que la DIRIS a intentionnellement dissimulé le « Journal social » alors qu'il fait partie intégrante des dossiers RI et est désormais directement intégré dans le SI MAORI ;
- page 61, ch.6, 1er § : « L'Office cantonal des bourses d'étude et d'apprentissage (OCBE) est rattaché à la Direction des aides et des assurances sociales (DIRAAS), l'une des trois directions qui composent la Direction générale de la cohésion sociale (DGCS) » ;
- page 62, 1re phrase : « Les bourses ne sont pas remboursables, sauf en cas d'abandon injustifié de la formation ou d'aides perçues indument ou détournées » ;
- Page 62, 2e phrase : « Et lorsque les critères pour obtenir une bourse d'études ou d'apprentissage ne sont pas entièrement remplis, la personne peut également solliciter un prêt, sous certaines conditions » ;
- page 62, 4e § : « Les accès aux données par les gestionnaires sont segmentés. Chaque gestionnaire n'est en charge que d'un nombre limité de bénéficiaires et n'a pas accès aux données des autres ». Nous vous proposons plutôt : « Les gestionnaires travaillent sur les dossiers qui leur sont attribués via un échéancier Filemaker. L'accès aux autres dossiers est toutefois techniquement possible et se justifie, d'une part, en raison du processus de validation mis en place avant une prise de décision (contrôle interne des 4 yeux) et, d'autre part, au vu d'impératifs organisationnels permettant de pallier l'éventuelle absence d'un-e collaborateur-trice sans que le traitement de la procédure administrative en pâtisse ou soit ralenti.

Nous vous souhaitons bonne réception de la présente et vous prions de croire, Madame la Magistrate, à l'expression de notre considération distinguée.

Fabrice Ghelfi
Directeur général

Annexes : liste des recommandations acceptées par la DIRIS et l'OCBE.

Direction générale de la cohésion sociale - Département de la santé et de l'action sociale
www.vd.ch/dgcs – T +41 (0)21 316 52 21
info.dgcs@vd.ch

- **OFFICE DU MÉDECIN CANTONAL (OMC)**

canton de vaud

Direction générale de la santé

Bâtiment administratif
de la Pontaise
Av. des Casernes 2
1014 Lausanne

Cour des comptes
Mme Valérie Schwaar
Magistrate
Rue de Langallerie 11
1014 Lausanne

Le Médecin cantonal
Réf. : MGT/JDG

Lausanne, le 16 décembre 2021

Audit de la protection des données personnelles dans l'Administration cantonale vaudoise – Rapport de la Cour des comptes du 23.11.2021

Madame la Magistrate,

Je fais référence au projet de rapport d'audit concernant la protection des données personnelles dans l'ACV lequel a retenu ma meilleure attention.

L'Office du Médecin cantonal a pris connaissance des constatations n°7 et 12 et accepte les deux recommandations y relatives.

S'agissant tout d'abord de la recommandation n°7 du rapport, l'Office du Médecin cantonal est conscient de la nécessité d'identifier les données personnelles et les données personnelles et sensibles ainsi que celles relevant du secret de fonction pour établir une cartographie dans l'objectif de se conformer aux principes de la LPrD.

En ce qui concerne la recommandation n°12 portant sur la plateforme TAO, une reprise du contrat informatique par la DGNSI aura lieu dans le sens d'une signature par la DGNSI avec modification du contrat incluant désormais une clause de respect de la LPrD. La modification portera également sur la gestion des entrées et des sorties, laquelle devra être centralisée de manière complète.

Le rapport de la Cour des comptes met en évidence la nécessité d'adapter nos processus de travail aux enjeux de la protection des données. Je relève que les implications sont nombreuses notamment en termes de ressources.

Je remercie la Cour des comptes pour son travail et je vous prie d'agréer, Madame la Magistrate, l'expression de ma parfaite considération.

Dr Karim Boubaker
Médecin cantonal

Annexe : Liste récapitulative des recommandations à l'OMC complétée

Direction générale de la santé – Département de la santé et de l'action sociale
www.vd.ch/dgs – T + 41 21 316 42 26 – medecin.cantonal@vd.ch

- **DIRECTION FINANCES ET AFFAIRES JURIDIQUES (DFAJ)**

canton de vaud

Direction générale de la santé

Bâtiment administratif
de la Pontaise
Av. des Casernes 2
1014 Lausanne

Cour des comptes
Mme Valérie Schwaar
Magistrate
Rue de Langallerie 11
1014 Lausanne

Direction finances et affaires juridiques
Réf. : MAB/CGP

Lausanne, le 15 décembre 2021

Audit de la protection des données personnelles dans l'Administration cantonale vaudoise – Rapport de la Cour des comptes du 23.11.2021

Madame la Magistrate,

Le projet de rapport d'audit concernant la protection des données personnelles dans l'ACV nous est bien parvenu ; il a retenu notre meilleure attention et notre intérêt.

La DFAJ a pris connaissance de la recommandation générale et de la recommandation spécifique la concernant, et accepte ces deux recommandations. Elle s'appliquera à les mettre en œuvre aussi efficacement que possible, tout en prenant en compte les ressources à sa disposition.

En ce qui concerne le contrat de mandat mentionné sous le point 7 du rapport, consacré à la DFAJ, nous tenons à préciser que ce contrat a été élaboré dans l'urgence de la crise sanitaire en septembre 2020 afin de doter sans délai la nouvelle entité de la DGS, en charge du traçage des contacts et la gestion des quarantaines, d'un directeur Ce mandataire a depuis février 2021 pu être engagé à l'ACV comme collaborateur en contrat à durée déterminée. Nous veillerons toutefois à nous assurer que nos modèles de contrats de mandat incluent de manière systématique les clauses nécessaires en regard de la question de la protection des données personnelles.

Nous remercions la Cour des comptes pour son travail détaillé et constructif et vous prions d'agréer, Madame la Magistrate, l'expression de nos salutations les meilleures.

Chantal Grandchamp
Directrice finances et affaires juridiques

Carmen Grand
Responsable unité juridique

Annexe : Liste récapitulative des recommandations à la DFAJ complétée

- **SERVICE DE L'ÉDUCATION PHYSIQUE ET DU SPORT (SEPS)**

canton de vaud

Service de l'éducation physique et du sport

Ch. de Maillefer 35
CH-1014 Lausanne

Madame
Valérie Schwaar
Magistrate
Cour des Comptes
Rue de Langallerie 11
1014 Lausanne

Réf. : NI / bj

Lausanne, le 8 décembre 2021

Audit de protection des données personnelles dans l'ACV - Projet de rapport pour consultation officielle

Madame,

Conformément à votre demande qui nous est parvenue par courriel le 24 novembre dernier, nous vous confirmons que nous avons pris connaissance du projet de rapport intitulé « Audit de protection des données personnelles dans l'Administration cantonale vaudoise ».

En fonction de l'état de nos connaissances à propos du thème traité, nous estimons que son contenu est conforme à la réalité et qu'il n'appelle aucun commentaire particulier.

Nous vous adressons, Madame, nos salutations les meilleures.

Le chef de service

Nicolas Imhof

Annexe

- Liste récapitulative

Département de l'économie, de l'innovation et du sport
Service de l'éducation physique et du sport
T 41 21 316 39 30
info.seps@vd.ch - www.vd.ch/seps

7. LISTE DES ABREVIATIONS

ACV	Administration cantonale vaudoise
APDI	Autorité de protection des données et de droit à l'information
CCF	Contrôle cantonal des finances
CdC	Cour des comptes du canton de Vaud
CNIL	Commission nationale de l'informatique et des libertés
COGES	Commission de gestion du Grand conseil
CP	Code pénal
CSI	Conférence suisse pour l'informatique
CSIR	Centre social d'intégration des réfugiés
DFAJ	Direction finances et affaires juridiques de la DGS
DGCS	Direction générale de la cohésion sociale
DGS	Direction générale de la santé
DGEO	Direction générale de l'enseignement obligatoire
DGNSI	Direction générale de l'informatique et du numérique
DIRIS	Direction de l'insertion et des solidarités
ESUSI	E-learning « Sensibilitation à la sécurité de l'information »
FORJAD	Formation pour jeunes adultes en difficulté
GED	Gestion électronique des documents
HIN	Health Info Net
LAGAPEO	Logiciel d'aide à la gestion administrative et pédagogique de l'enseignement obligatoire
LInfo	Loi sur l'information
LIPD	Loi sur les fichiers informatiques et la protection des données
LPD	Loi fédérale sur la protection des données personnelles
LPDS	Loi sur la protection des données Schengen
LPers	Loi sur le personnel de l'Etat de Vaud
LPrD	Loi vaudoise sur la protection des données personnelles
nLPD	Loi fédérale sur la protection des données personnelles révisée
OCBE	Office cantonal des bourses d'études et d'apprentissage

OMC	**Office du médecin cantonal**
OPS	**Office de psychologie scolaire**
PFPDT	**Préposé fédéral à la protection des données et à la transparence**
PPLS	**Psychologie, psychomotricité et logopédie en milieu scolaire**
RForm	**Règlement sur la formation continue**
RGPD	**règlement général sur la protection des données (Union européenne)**
RIC	**Règlement relatif à l'informatique cantonale**
RLPers	**Règlement d'application de la LPers**
RLPrD	**Règlement d'application de la loi sur le personnel de l'Etat de Vaud**
SAN	**Service des automobiles et de la navigation**
SEPS	**Service d'éducation physique et du sport**
SI	**Système d'information**
SMSI	**Système de management de la sécurité de l'information**
SOC	**Centre opérationnel de sécurité**
SPEV	**Service du personnel de l'Etat de Vaud**
STE	**Série des traités européens**
TAO	**Traitements par agonistes opioïdes**
USSI	**Unité de sécurité des systèmes d'information**

8. ANNEXES

8.1 ANNEXE I : QUESTIONS ADRESSÉES AU PRÉALABLE AUX ENTITÉS-MÉTIERS

1. Protection des données

1.1 Dispositions de la législation sur la protection des données (LPrD)

Données traitées

Selon le Registre des fichiers, votre entité traite des données personnelles et sensibles (selon la définition de l'art. 4 al. 1 chiffres 1 et 2 LPrD[132]).

1. Existe-il un ou plusieurs documents descriptifs : liste de fichiers contenant des données personnelles, cartographie des applications, organigramme, etc. ?
2. Nous nous intéressons prioritairement à ces fichiers : *XXX (fichiers choisis pour l'entité)*
   - Des données personnelles de ces fichiers existent-elles également sous format papier ?
3. Votre entité est-elle responsable du traitement[133] de ces données ?
   - Si non, quelle est l'entité responsable du traitement ?

Conformité (Art. 5, 6 LPrD)

4. Reprenant les fiches XX et XX du Registre des fichiers, confirmez-vous que les données inscrites sont conformes ? Il s'agit notamment de la liste des bases légales, du but du fichier, du type de données et de la transmission à des tiers *(fiches en annexe à ce questionnaire)*.

Proportionnalité (Art. 7 LPrD)

5. Parmi l'ensemble des fichiers/applications avec des masques de saisie, y en a-t-il dans lesquels il est possible d'introduire des commentaires en clair ?

Archivage, destruction et communication (Art. 11, 15 et 16 LPrD)

6. Quelle est la politique d'archivage des fichiers contenant des données personnelles pour votre entité (pour l'ensemble des fichiers/applications) ?
   (S'il existe un document descriptif, merci de le transmettre lors de l'entretien)
   - Pour les données papier ?
   - Pour les données numériques ?

---

[132] Définitions selon l'art. 4 al. 1 LPrD :

On entend par :

1. ***Donnée personnelle*** : toute information qui se rapporte à une personne identifiée ou identifiable ;
2. ***Donnée sensible*** : toute donnée personnelle se rapportant
   - 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.

[133] Définition selon l'art. 4 al. 1 chiffre 8 LPrD :

Responsable du traitement : personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine le contenu, ainsi que les finalités du fichier.

7. Quelle est la politique de destruction des données/fichiers contenant des données personnelles pour votre entité (pour l'ensemble des fichiers/applications) ?
   (S'il existe un document descriptif, merci de le transmettre lors de l'entretien)
   - Pour les données papier ?
   - Pour les données numériques ?
8. Communiquez-vous ces données à des tiers (hormis la transmission à des particuliers ayant demandé avoir accès à leurs propres données (art. 25 LPrD) et la sous-traitance (art. 18 LPrD)) ?
   (S'il existe un document descriptif, merci de le transmettre lors de l'entretien)
   - Si oui, ces tiers sont-ils internes ou externes à l'ACV ?
   - Si oui, existe-t-il une base légale pour cette communication, ou répond-elle à une tâche légale ? Laquelle ?
9. Des personnes externes à votre entité ont-elles accès aux données personnelles gérées par votre entité (transmission, consultation ou modification) ?
   - Si oui, ces tiers sont-ils internes ou externes à l'ACV ?
   - Avez-vous adopté des mesures pour vous assurer que ces personnes externes respectent les dispositions en matière de protection des données ?
     (S'il existe un document descriptif, un modèle de contrat ou de déclaration de confidentialité, merci de les transmettre lors de l'entretien)

<u>Sous-traitance</u> (art. 18 LPrD)

10. Sous-traitez-vous des tâches de collecte et /ou de traitement de données personnelles, dont vous êtes responsable du traitement, à d'autres entités ?
    - Si oui, quelles tâches et pour quelles données ?
    - Si oui, ces entités sont-elles internes ou externes à l'ACV ?
    - Avez-vous adopté des mesures pour vous assurer que le sous-traitant respecte les dispositions en matière de protection des données ?
      (S'il existe un document descriptif, un modèle de contrat ou de déclaration de confidentialité, merci de le(s) transmettre lors de l'entretien)

<u>Registre des fichiers</u> (art. 19 LPrD[134])

11. Le registre des fichiers tenu par l'Autorité de protection des données et de droit à l'information est-il complet pour votre entité ?
    - Si non, quels sont les fichiers manquants ?
      (S'il existe un document descriptif, merci de le transmettre lors de l'entretien.)

<u>Problèmes rencontrés</u>

12. A votre connaissance, des cas de non-respect des dispositions sur la <u>protection</u> des données se sont-ils produits dans votre entité ces 3 dernières années (fuite, divulgation volontaire ou non de données) ?

[134] Art 19 LPrD :

1. Le Préposé cantonal à la protection des données et à l'information (ci-après : le Préposé) tient un registre des fichiers, qui est public et accessible en ligne.
2. Le Conseil d'Etat édicte les règles applicables à la tenue du registre.

1.2 Formation/information

13. Les collaborateur-trice-s de votre entité traitant des données personnelles et/ou sensibles ont-ils-elles suivi une formation en matière de protection des données ?
    - Si oui laquelle/lesquelles ?
14. Les collaborateur-trice-s de votre entité traitant des données personnelles et/ou sensibles ont-ils-elles reçu des informations en matière de protection des données ?
    - Si oui sous quelle forme ? *(S'il existe un ou des documents, merci de le(s) transmettre lors de l'entretien)*
15. Estimez-vous que leur niveau de connaissance à ce sujet est suffisant ?
16. Estimez-vous que les chef-fe-s d'entités/services bénéficient de suffisamment d'information/support en matière de protection des données ?

1.3 Mesures spécifiques à votre entité en matière de protection des données

17. Y a-t-il un-e responsable ou un-e référent-e en matière de protection des données dans votre entité ? Ou au sein de votre Direction/Département ?
18. Avez-vous établi une directive, charte, convention ou adopté des mesures spécifiques à votre entité en matière de protection des données personnelles que vous traitez ?
    (Si oui, merci de transmettre le ou les document(s) lors de l'entretien)
19. Avez-vous adopté des mesures pour vous assurer du respect des dispositions sur la protection des données dans votre entité (conformité à la LPrD) ?
    - Si oui, lesquelles ? *(S'il existe un document descriptif, merci de le transmettre lors de l'entretien)*
20. Existe-t-il des mesures spécifiques pour le personnel non soumis à la LPers (auxiliaires, temporaires, etc.)

1.4 Demandes et relations avec l'Autorité de protection des données

21. L'Autorité de protection des données (préposée) est-elle déjà intervenue dans votre entité ?
    - Si oui dans quel contexte ?
22. Avez-vous déjà sollicité l'Autorité de protection des données pour un renseignement, un conseil, une formation ?
    - Si oui dans quel contexte ?
23. Avez-vous déjà reçu des demandes d'autres autorités (par exemple du préposé fédéral à la protection des données, de policiers, de procureurs, ou de tribunaux) ?
    - Si oui dans quel contexte ?

2. Secret de fonction

24. Avez-vous défini les informations soumises au secret de fonction dans votre entité ?
    (S'il existe un document descriptif, merci de le transmettre lors de l'entretien)
25. Cas échéant, appliquez-vous le même processus de traitement et de communication que celui que vous appliquez aux données personnelles ?
    (S'il existe un document descriptif, merci de le transmettre lors de l'entretien)

3. Sécurité des données

3.1 Sécurité informatique

26. Avez-vous défini des besoins propres à votre entité en matière de sécurité informatique des fichiers contenant des données personnelles et/ou sensibles (ou autres informations soumises au secret de fonction) ? *(S'il existe un document descriptif, merci de le transmettre lors de l'entretien)*
    - Si oui, la collaboration avec la DGNSI a-t-elle permis de répondre à vos besoins ?
    - Si non, estimez-vous que les mesures de base mises en place par la DGNSI en matière de sécurité informatique suffisent à vos besoins ?
27. Avez-vous mis en place des droits d'accès aux fichiers contenant des données personnelles, différenciés selon les collaborateur-trice-s ?
    - Si oui, en fonction de quel(s) critère(s) ? *(S'il existe un document descriptif, merci de le transmettre lors de l'entretien)*
28. Hormis les droits d'accès, avez-vous mis en place des mesures/directives spécifiques à votre entité en matière de sécurité informatique visant à protéger les données personnelles ou soumises au secret de fonction ?
    (S'il existe un document, merci de le transmettre lors de l'entretien)

3.2 Sécurité physique

29. Avez-vous mis en place des mesures/directives spécifiques à votre entité en matière de sécurité physique (non informatiques) visant à protéger les données personnelles ou soumises au secret de fonction ? *(S'il existe un document, merci de le transmettre lors de l'entretien)*

3.3 Mesures organisationnelles

30. Les collaborateur-trice-s de votre entité traitant des données personnelles ont-ils-elles suivi une formation en matière de sécurité informatique ?
    - Si oui, quelle formation ?
    - Estimez-vous que leur niveau de connaissance soit suffisant ?
31. Les collaborateur-trice-s de votre entité traitant des données personnelles reçoivent-ils-elles périodiquement une information en matière de sécurité informatique ?
32. Avez-vous adopté des mesures de contrôle pour vous assurer que les mesures de sécurité visant à protéger les données personnelles dans votre entité sont efficaces ?
    (S'il existe un document descriptif, merci de le transmettre lors de l'entretien)
    - Si oui, lesquelles ?
33. Existe-t-il des mesures spécifiques pour le personnel non soumis à la LPers (auxiliaires, temporaires, etc.)

Problèmes rencontrés

34. A votre connaissance, des cas de non-respect des dispositions sur la sécurité des données se sont-ils produits dans votre entité ces 3 dernières années (fuite, divulgation volontaire ou non de données) ?
    - Si oui, comment a-t-elle été gérée ?

4. Télétravail

35. Combien de collaborateurs-trices (sans les apprenti-e-s) travaillent dans votre entité ?
36. Combien d'ETP cela représente-il au plan des postes de votre entité ?
37. Combien de collaborateur-trice-s de votre entité pratiquent le télétravail conventionné ?
38. Votre entité a-t-elle élaboré une convention de télétravail propre ?
    (S'il existe un document, merci de le transmettre lors de l'entretien)
39. Combien de collaborateur-trice-s de votre entité pratiquent le télétravail non-conventionné (hors situation COVID-19 et au minimum ½ journée par semaine) ?
40. Envisagez-vous d'élargir le télétravail dans votre entité ? Si oui dans quelle mesure ? Quelles fonctions sont concernées ? Lesquelles ne le sont pas ?
41. Les collaborateur-trice-s en télétravail utilisent-ils-elles le PC portable professionnel fourni par la DGNSI ou leur propre PC ?
    - Si oui, quelle est la proportion de l'équipe et/ou les catégories d'employés concernés ?
42. Les collaborateur-trice-s en télétravail utilisent-ils-elles leur téléphone mobile privé dans un but professionnel ?
    - Si oui, quelle est la proportion de l'équipe et/ou les catégories d'employés concernés ?
43. Estimez-vous que la pratique du télétravail accroisse significativement les risques de fuite, de perte de données personnelles ou d'informations confidentielles ?
    - Si oui, pourquoi ?
44. Avez-vous établi des directives ou adopté des mesures spécifiques au télétravail pour votre entités afin de protéger les données personnelles et sensibles (des administré-e-s) et les données soumises au secret de fonction traitées ?
    - Si non, estimez-vous que cela n'est pas nécessaire ?
    - Si non et que vous estimez néanmoins que c'est nécessaire, êtes-vous d'avis que la responsabilité d'établir des directives/guides relève des services encadrant la pratique du télétravail (SPEV, Autorité de protection des données et au droit à l'information et DGNSI) et non des entités-métiers ?
45. Estimez-vous que les mesures techniques mises en place par la DGNSI pour assurer la sécurité technique des données en télétravail sont satisfaisantes ?

5. En général

46. Estimez-vous que les responsabilités en matière de protection et de sécurité des données traitées sont clairement définies pour les différents acteurs : entité responsable du traitement, entité utilisatrice, collaborateur-trice-s, la DGNSI, Autorité de protection des données et SPEV, etc.
    - Dans les bureaux de l'ACV ?
    - En télétravail ?
47. Estimez-vous que le support des services transversaux de l'Etat (DGNSI, préposée à la protection des données, SPEV) est suffisant pour assurer la protection et la sécurité des données ?
    - Dans les bureaux de l'ACV ?
    - En télétravail ?

8.2 ANNEXE II

LE CONTEXTE INTERNATIONAL ET FÉDÉRAL DES DISPOSITIONS SUR LA PROTECTION DES DONNÉES PERSONNELLES

1. Convention de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH ; RS 0.101)

Principes fondateurs

Traité international signé par les États membres du Conseil de l'Europe le 4 novembre 1950 et entré en vigueur le 3 septembre 1953, la CEDH est entrée en vigueur pour la Suisse en 1974 et contient les principes fondateurs des dispositions sur la protection des données à l'article 8 :

> **Article 8 CEDH « Droit au respect de la vie privée et familiale »**
>
> *1 Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.*
>
> *2 Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.*

La jurisprudence décline les exigences minimales concrètes

De la jurisprudence de la CEDH découle une exigence d'établir une base légale à partir de cette disposition[135]. Elle a notamment retenu qu'il était "*essentiel de fixer des règles claires et détaillées régissant la portée et l'application des mesures et imposant un minimum d'exigences concernant, notamment, la durée, le stockage, l'utilisation, l'accès des tiers, les procédures destinées à préserver l'intégrité et la confidentialité des données et les procédures de destruction de celles-ci*" (arrêt de la CourEDH 30562/04 S. et Marper contre Royaume-Uni [GC] du 4 décembre 2008, §§ 98s.)

2. Lignes directrices de l'OCDE régissant la protection des données et les flux transfrontières des données à caractère personnel

Favoriser les échanges commerciaux tout en respectant la sphère privée

Afin d'harmoniser les niveaux de protection des données en vigueur dans chaque pays, l'OCDE a élaboré en 1980, des lignes directrices qui ont été révisées en 2013 et qui ont un statut de recommandations. Elles ont pour but d'instaurer une réglementation nationale assurant l'échange de données au plan international en évitant les entraves au commerce tout en préservant les droits fondamentaux.

[135] Source : Arrêt CDAP, GE.2019.0214

Huit principes concrets

Ces lignes directrices, qui s'appliquent aux données du secteur public et privé, comprennent huit principes : la limitation de la collecte, la qualité des données, la finalité, la limitation de l'utilisation, les garanties de sécurité, la bonne foi, la participation individuelle et la responsabilité.

3. Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, du Conseil de l'Europe (RS 0.235.1)

Premier texte contraignant au niveau international

Adoptée par le Conseil de l'Europe le 28 janvier 1981 et ratifiée par la Suisse le 2 octobre 1997, cette Convention, nommée aussi directive STE 108 fonde le cadre juridique international en matière de protection des données, dans le respect des lignes directrices OCDE. Son champ d'application couvre les traitements de données personnelles intervenant dans les secteurs public et privé. C'est le premier traité international en matière de protection des données ; ses normes sont juridiquement contraignantes et sont à transposer dans les législations nationales. Au 31 décembre 2020, 55 Etats (dont 8 non-membres du Conseil de l'Europe) l'ont ratifiée.

Instauration d'une autorité indépendante de contrôle

Un protocole additionnel à cette Convention a été adopté en 2001 et est entré en vigueur pour la Suisse le 1er avril 2008. Parmi les nouveautés, on note l'institution d'une autorité indépendante pour assurer le respect des principes liés à la protection des données et la mise en place de règles pour les flux transfrontières des données, qui ne sont autorisés que si le pays de destination prévoit un niveau de protection approprié des données (si le pays n'est pas signataire de la Convention).

Plusieurs révisions et renforcement progressif des dispositions

La Convention a fait l'objet d'une révision totale afin de tenir compte de l'évolution technologique et de renforcer les pouvoirs de l'autorité de contrôle en lui accordant le droit de rendre des décisions contraignantes soumises à recours et de prononcer des sanctions administratives. Les obligations du responsable du traitement sont également renforcées. Son protocole d'amendement (STE 223) a été adopté le 18 mai 2018. La Suisse l'a signé en octobre 2019 et devrait le ratifier avec l'entrée en vigueur de la nLPD. On parle souvent de Convention 108+ ou de « Convention modernisée pour la protection des personnes à l'égard du traitement des données à caractère personnel ».

4. Le cadre légal européen

L'Union Européenne (UE) a adopté en 2016 un cadre législatif moderne et conforme aux dispositions de la Convention 108+ comprenant deux documents principaux :

- **le règlement (UE) 2016/679** « *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* » en en abrégé « règlement général sur la protection des données » ou RGPD ;

- **la directive (UE) 2016/680** « *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données* », qui constitue un développement de l'acquis Schengen[136]. Elle est souvent abrégée de manière officieuse la directive « Police-Justice ».

Ce cadre légal impacte directement la législation de la Confédération et des cantons, en particulier la Directive Police-Justice qui devait être reprise dans le cadre des accords de Schengen en 2018.

4.1 Le règlement UE 2016/679 (RGPD)

La Suisse et ses cantons doivent aligner leur législation sur le RGPD

Bien que le RGPD ne concerne pas directement la Suisse qui n'est pas membre de l'UE, les dispositions de l'UE imposent que, pour tout transfert de données personnelles entre une entité soumise au RGPD et une entité située hors UE, le pays où se trouve cette entité présente un niveau de protection « adéquat » en matière de protection des données personnelles. Pour des raisons économiques, la Confédération et les cantons ont tout intérêt à être reconnus comme adéquats, sous peine d'entraves aux échanges de données avec les pays de l'UE[137].

Entré en vigueur en mai 2018, le RGPD remplace la directive 95/46/CE, adoptée en 1995. Cette dernière constituait le premier texte de loi de l'UE européen en matière de protection des données. Le RGPD est directement applicable dans l'ensemble de l'Union sans nécessiter de transposition dans les différents États membres. Aligné sur le standard de base des dispositions de la Convention 108+, le RGPD contient des clauses beaucoup plus détaillées que cette dernière et vise à la fois le renforcement et la modernisation des dispositions, afin notamment de tenir compte de l'évolution technologique et de la numérisation des données.

Tâches nouvelles pour les responsables de traitement et rôle accru de l'autorité de contrôle

Le RGPD s'applique aux données à caractère personnel gérées par les secteurs privé et public, relatives à des personnes identifiables résidant dans un pays de l'UE. Font exception à ce règlement, les données traitées par la police et la justice qui sont régies par la Directive (UE)2016/680, ainsi que celle qui ne relèvent pas du champ d'application du droit de l'Union européenne telles que les activités de sûreté de l'Etat ou de défense nationale. Il ne concerne pas non plus les données personnelles traitées par les individus à titre privé, ni les données concernant des personnes morales.

[136] L'acquis Schengen est un ensemble de règles et règlements, intégrés dans le droit de l'Union européenne, qui règlent la zone dite « espace de liberté, de sécurité et de justice » et les relations entre les États qui ont signé la Convention de Schengen.

[137] Même si les collectivités publiques vaudoises qui sont les entités soumises à la LPrD, ne sont, en règle générale, pas soumises au RGPD (cf. Memo HDC Sylvain Métille à l'intention de l'APDI « Champ d'application du RGPD aux entités vaudoises », 13.02.2018), la législation qui s'y applique doit néanmoins être reconnue comme adéquate par l'UE. En effet cette dernière, pour juger du caractère adéquat ou non de la législation en matière de protection des données, examine l'ensemble des dispositions du pays et non uniquement celles relatives aux entités échangeant des données avec un pays de l'UE.

Ce règlement prévoit également une application extraterritoriale : une entité privée ou publique qui traite les données de résidents UE qu'elle vise - à qui elle offre des biens et services ou analyse le comportement (en vue d'une prospection) - doit appliquer le RGPD pour ces traitements de données. Les nouveautés apportées par le RGPD sont nombreuses et d'importance. Parmi les principales qui impacteront la législation suisse, on peut citer[138] :

- l'élargissement de la définition **des données sensibles** aux données génétiques et biométriques ;
- l'encadrement strict du traitement de données résultant d'un profilage[139] ;
- la **responsabilité renforcée des sous-traitants :** le règlement leur étend en effet une large partie des obligations imposées aux responsables de traitement ;
- l'obligation d'appliquer **la protection des données dès la conception et par défaut** et le renforcement de l'application de mesures de protection et de sécurité tout au long du traitement. Dans ce but, de nouveaux outils sont prévus dont les principaux sont :
  - la tenue d'un registre des traitements comprenant des données personnelles ;
  - la **notification des violations de la sécurité** aux autorités et aux personnes concernées ;
  - la nomination d'**un·e délégué·e à la protection des données** pour les responsables de traitement et leurs sous-traitants (obligatoire dans le secteur public) ;
  - les **analyses d'impact** relatives à la protection des données pour tous les traitements à risque : portant sur des données sensibles, traitées à large échelle et profilage (évaluation systématique et approfondie d'aspects personnels des personnes physiques).
- **le renforcement des droits de la personne** concernée notamment par le droit à la portabilité des données, le droit à l'oubli (effacement des données), le droit à réparation des dommages matériel ou moral, le droit de saisir une autorité de contrôle ou judiciaire, etc. ;
- **le renforcement des sanctions et le pouvoir accru de l'autorité de contrôle** qui peut désormais : prononcer un avertissement, mettre en demeure l'entreprise, imposer une amende, limiter temporairement ou définitivement un traitement, suspendre les flux de données, ordonner de satisfaire aux demandes d'exercice des droits des personnes, ordonner la rectification, la limitation ou l'effacement des données.

En outre, le plafond des amendes administratives est relevé à 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, de 2% jusqu'à 4% du chiffre d'affaires annuel mondial.

4.2 La directive (UE) 2016/680 : directive « Police-Justice »[140] du développement de l'acquis Schengen

Si le RGPD n'a pas de caractère véritablement obligatoire pour la Suisse, tel n'est pas le cas de la directive (UE) 2016/680, la Suisse étant signataire de l'Accord de Schengen[141].

[138] Source principale : CNIL « Règlement européen sur la protection des données : ce qui change pour les professionnels », 2018.
[139] Définition : cf. note de bas de page n°149
[140] Le nom complet de la directive est : DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.
[141] L'Accord de Schengen favorise la libre circulation des personnes grâce à la suppression des contrôles de personnes aux frontières internes. Un renforcement de la sécurité interne est assuré par les contrôles aux frontières externes de l'espace Schengen et par une coopération transfrontalière en matière de justice et police renforcée entre les Etats. La Suisse adhère au système d'information de

Cette directive s'applique aux transferts de données à travers les frontières des pays de l'Union européenne et fixe des normes minimales pour le traitement des données à des fins policières au sein de chaque Etat signataire des Accords Schengen. N'étant pas directement applicable pour les Etats, elle doit être transposée en droit interne.

Cette directive est calquée sur la structure du RGPD, tout en visant des domaines différents, exclus du périmètre RGPD. Elle a pour objectif de favoriser la libre circulation des données dans le secteur de la police et de la justice ainsi que la coopération judiciaire et policière entre les Etats signataires, tout en protégeant les libertés et droits fondamentaux des personnes physiques et, en particulier, leur droit à la protection des données.

A l'instar du RGPD, il est prévu d'instituer une autorité de contrôle indépendante chargée de vérifier le respect des règles édictées par la directive (qui peut être la même que celle prévue par le RGPD). Cette directive encadre en outre les flux transfrontières des données dans le cadre des finalités visées.

Par contre, par rapport au RGPD, les droits des personnes concernées sont fortement tempérés en raison du contexte répressif ou judiciaire régulé dans lequel des règles particulières relatives au profilage sont également prévues[142].

L'audit n'examinant pas directement des entités relevant de cette directive, la police et la justice étant hors périmètre, nous ne détaillerons donc pas ici ces dispositions.

5. Le cadre légal fédéral

Le cadre légal fédéral relatif à la protection des données conditionne à des degrés divers le contexte légal se rapportant aux entités publiques vaudoises. Même si la LPD ne concerne pas directement les entités publiques vaudoises qui sont soumises à la LPrD, elle influe toutefois cette dernière qui ne peut contenir des dispositions qui s'en écartent trop. En effet certaines entités, qui sont soumises à la fois au droit fédéral et au droit vaudois, doivent respecter les deux types de dispositions. Comme le mentionne l'EMPL de mars 2007 relatif à la LPrD, « *par conséquent, une uniformité entre les règles applicables au traitement des données par les autorités fédérales d'une part, et par les autorités cantonales d'autre part, est souhaitable.* » De plus, le citoyen vaudois s'attend à un niveau de protection similaire imposé aux autorités cantonales, qui doivent en outre respecter les Conventions 108 et 108+.

C'est pourquoi il est important de comprendre le droit fédéral et son évolution.

5.1 La Constitution fédérale du 18 avril 1999 (RS 101)

La Constitution fédérale contient un article relatif à la protection des données personnelles. Le premier alinéa s'inspire directement de l'art. 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH).

Schengen (SIS), une base de données informatisée contenant plusieurs dizaines de millions des renseignements sur les personnes et les objets recherchés (source : *EMPL de la loi vaudoise sur la protection des données*, mars 2007).

[142] Source : *La protection des données dans le secteur de la « police » et de la « justice »,* Éditions Larcier, 16.11.2018

« Protection de la sphère privée » (Art. 13 Cst)

1 Toute personne a droit au respect de sa vie privée et familiale, de son domicile, de sa correspondance et des relations qu'elle établit par la poste et les télécommunications.

2 Toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent.

5.2 Première loi fédérale sur la protection des données en 1992 (LPD ; RS 235.1)

Loi commune au secteur public fédéral et au secteur privé

En 1992 une première loi fédérale sur la protection des données, basée sur les principes modernes prévoyant l'institution d'une autorité indépendante de surveillance, a vu le jour[143]. Les travaux préparatoires à cette législation ont duré près de dix ans. A noter qu'un certain nombre de pays européens avaient déjà adopté de telles dispositions, le premier étant la Suède en 1973, suivi par l'Allemagne en 1977, la France, l'Autriche, la Norvège et le Danemark en 1978 et la Grande-Bretagne en 1984.

Il avait été décidé d'établir une loi commune pour l'administration fédérale et le secteur privé. Les administrations cantonales et communales furent exclues du périmètre.

Dotée de 39 articles, cette disposition se conforme aux exigences de la Convention 108. La Commission européenne a reconnu que la législation suisse garantissait un niveau adéquat de protection des données[144].

Dispositions du Code civil et directives fédérales insuffisantes

Avant cette législation, la protection des données dans le secteur privé était régie uniquement par l'article 28 al. 1 du Code civil, entré en vigueur en 1985 : « *Celui qui subit une atteinte illicite dans sa personnalité peut agir en justice pour sa protection contre toute personne qui y participe* ». Cette disposition qui définit uniquement le principe général de la protection de la personnalité était cependant largement insuffisante pour réglementer ce domaine, même si la jurisprudence a contribué à l'élaboration de certaines définitions, dont le caractère illicite d'un traitement[145].

Concernant l'administration fédérale, le Conseil fédéral avait édicté le 16 mars 1981 des *« Directives applicables au traitement de données personnelles dans l'administration fédérale* ». Ce texte posait quelques jalons juridiques de la protection des données en obligeant notamment l'administration à renseigner les personnes concernées. Il ne couvrait cependant pas tous les aspects à traiter.

[143] Entrée en vigueur en 1993.

[144] JO L 215 du 25.8.2000, p. 1 (source : *Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales*, 15 septembre 2017).

[145]« *La jurisprudence est d'avis qu'un traitement de données est illicite s'il porte atteinte à un aspect de la vie de l'individu, à son indépendance morale ou à son crédit social. »* (source : *Message concernant la loi fédérale sur la protection des données (LPD)* du 23 mars 1988).

Contexte et objectifs précisés

Le message accompagnant la loi retrace le contexte et précise son objectif[146] . Il s'agit de garder à l'esprit que la protection des données ne doit pas entraver l'activité économique ou étatique, mais établir certaines règles afin d'assurer la protection de la personnalité des individus dont les données sont traitées ou tout au moins d'en limiter les atteintes.

Périmètre exclu de la loi

Le champ d'application de la loi ne s'étend pas aux procédures juridictionnelles devant les autorités judiciaires, aux procédures pénales, aux procédures d'entraide judiciaire, ni aux registres publics. En effet, les lois de procédure protègent déjà la personnalité. Le dédoublement de dispositions portant sur le même périmètre a donc été jugé inutile.

Introduction des principes constituant le cœur de la protection des données

La loi consacre les principes fondamentaux de la protection des données qui se retrouvent dans toutes les législations modernes et qui sont présentés dans le chapitre introductif, que sont la licéité du traitement, leur exactitude, la proportionnalité, la sécurité et la finalité. Le message relatif à la loi précise encore que « *… Ajoutés au principe gouvernant la communication des données à l'étranger, ces principes forment le noyau dur de la protection des données* ».

Outre ces principes, la législation fédérale introduit les éléments principaux suivants :

- **institution d'un·e préposé·e à la protection des données**, autorité indépendante, dont les tâches relatives au secteur public sont notamment :
    - La surveillance de l'application de la législation par les organes fédéraux ;
    - L'établissement de recommandations aux organes fédéraux, en cas de non-respect de la législation, et le cas échéant une demande de décision de la part de l'organe responsable contre laquelle le·la préposé·e peut déposer un recours ;
    - La sensibilisation, l'information et l'assistance auprès des organes fédéraux en matière de protection des données ;
    - L'examen des projets d'actes législatifs fédéraux.
- **droit d'accès des individus à des informations concernant leurs propres données** traitées par les organes fédéraux, selon le principe de l'autodétermination informationnelle ;
- obligation des organes fédéraux de **déclarer tous les fichiers contenant des données personnelles** qu'ils détiennent au·à la préposé·e à la protection des données qui tient à jour un registre des fichiers publics, afin de favoriser ce droit d'accès des individus à leurs propres données ;
- **possibilité de recourir** à la loi sur la procédure administrative pour quiconque a un intérêt légitime, d'exiger de l'organe fédéral qu'il s'abstienne de procéder à un traitement illicite, rectifie des données inexactes, etc. ;

[146]« *Le but d'une loi sur la protection des données n'est pas de stopper le développement des technologies de l'information, ni même de limiter les possibilités qu'elles offrent. Ces technologies ont incontestablement fait leurs preuves ; et ce, dans des domaines aussi divers que les sciences, l'économie ou l'administration. Les progrès dont on leur est redevable ne sauraient être remis en cause ; bien au contraire, il faut qu'ils se poursuivent. Néanmoins, il est impératif de consacrer certains principes directeurs garantissant qu'aucun traitement de données inutile ou indésirable ne vienne menacer l'épanouissement de la personnalité des individus. A moins que l'ordre juridique n'en dispose autrement, chacun doit pouvoir déterminer la valeur qu'il attache à ses propres données et l'utilisation qu'il souhaite qu'on en fasse* » (source : *Message concernant la loi fédérale sur la protection des données (LPD)* du 23 mars 1988).

- distinction entre les **données personnelles sensibles** (selon la définition page 13) et les profils de personnalités devant bénéficier de mesures de protection renforcées, et les données personnelles non sensibles ;
- obligation pour chaque organe fédéral de désigner **un·e délégué·e à la protection des données** (disposition prévue par l'ordonnance fédérale).

Plusieurs révisions depuis 1993

La LPD a subi plusieurs révisions depuis son entrée en vigueur en 1993.

La principale a eu lieu en 2006, avec le renforcement de la transparence dans le traitement des données personnelles pour les personnes concernées et l'obligation de les informer lors de la collecte de données sensibles et de profils de personnalité. Le·la préposé·e dispose désormais du pouvoir de faire recours contre les décisions prises par la Chancellerie ou les départements suite à ses recommandations.

5.3 Loi sur la protection des données Schengen (LPDS)

La Suisse, de par son adhésion à l'Accord Schengen, est liée à l'obligation de légiférer en matière de protection des données sur les domaines de justice et police, exclus du champ de la LPD, sur le modèle de la directive (UE) 2016/680.

Dans le projet de révision de la LPD, il était prévu d'intégrer également les domaines de la justice et de la police afin de réunir les dispositions relatives à la protection des données dans une seule loi. Dans l'attente de cette révision, il a cependant été décidé de légiférer sur le domaine Schengen : la loi sur la protection des données Schengen (LPDS), entrée en vigueur le 1er mars 2019, est donc la transposition de cette directive européenne pour la Confédération[147]. La LPDS ne s'applique toutefois pas aux domaines de la justice et de la police relevant des cantons qui sont tenus d'établir leur propre base légale. Elle sera abrogée lors de l'entrée en vigueur de la LPD révisée.

5.4 Révision complète de la LPD en 2021 (pas encore en vigueur)

Cinq ans après l'évaluation de la LPD ayant conclu à la nécessité de réviser la loi en profondeur et après plusieurs années d'intenses travaux, un premier projet a été mis en consultation en 2016. Ce dernier a appelé de nombreux commentaires et modifications. Le parlement a finalement adopté le 25 septembre 2020 la version finale de la LPD révisée, soit dix ans plus tard.

La nouvelle loi reprend la plupart des dispositions du droit européen …

L'objectif de cette révision est en premier lieu d'assurer la compatibilité de la législation suisse avec le droit européen. Cela implique tout d'abord de pouvoir ratifier la Convention 108+ et de garantir que la Commission européenne maintienne sa décision d'accorder à la Suisse le statut de pays offrant un niveau de protection des données adéquat. Cette condition est nécessaire à la libre circulation des données entre l'Union européenne et la Suisse.

Reprenant les éléments figurant dans la LPD, le projet intègre la plupart des principales nouveautés du RGPD détaillées sous le point 3.1.2.1 comme :

[147] Au niveau fédéral, la LPDS s'applique dès lors que des données personnelles sont traitées par exemple dans le cadre de l'accomplissement des tâches légales de l'OFJ dans le domaine de l'entraide judiciaire internationale en matière pénale, dans le cadre des activités du domaine de direction coopération policière internationale de fedpol, des enquêtes de la police fédérale judiciaire dans les domaines relevant de la compétence de la Confédération ainsi que lors de l'échange d'informations de police avec les autorités de poursuite pénale d'autres pays, ou avec des organismes internationaux tels que INTERPOL et Europol.

- **l'élargissement de la définition des données sensibles** aux données génétiques et biométriques (art. 5 let. c LPD) ;
- l'introduction des notions de « **profilage**[148] » et de « **profilage à risque élevé**[149] » ;
- l'**obligation d'annoncer les violations de la sécurité** des données (art. 25 LPD) ;
- la **responsabilité renforcée des sous-traitants** notamment en matière de sécurité (art. 8 LPD et tous les articles du chapitre 3 « Obligations du responsable du traitement et du sous-traitant ») ;
- l'obligation d'appliquer la **protection des données dès la conception et par défaut** (art. 7 LPD), qui implique notamment la nécessité de procéder à **une analyse d'impact** (art. 22 al. 3 LPD)[150] pour les traitements à risque ;
- l'obligation de tenir un **registre des activités de traitement** (art. 12 LPD)[151] ;
- le **renforcement des pouvoirs de l'autorité de contrôle**, désormais habilitée à prononcer des décisions.

… mais s'en écarte au niveau des sanctions

Par contre, contrairement au RGPD, l'autorité de contrôle n'est pas dotée de la compétence d'imposer des sanctions. Le volet pénal est cependant renforcé. Le plafond du montant des amendes, rehaussé à CHF 250'000 reste toutefois beaucoup plus faible que celui prévu par le RGPD (10 à 20 millions d'euros ou de 2 à 4% du chiffre d'affaires mondial).

Des dispositions plus compliquées à appliquer que celles de la précédente loi

Avec les nouvelles dispositions, l'application de la loi sur la protection des données s'est complexifiée. Elle nécessite, pour les entités gérant des données personnelles, de disposer de compétences accrues en matière de protection et de sécurité des données.

Le responsable du traitement doit en effet toujours distinguer les données personnelles non sensibles des données personnelles sensibles et leur appliquer un traitement approprié et différencié comme avec la précédente loi. En plus, il est tenu d'identifier les données ou les combinaisons de données présentant « un risque élevé » pour la personnalité ou les droits fondamentaux de la personne concernée, ces dernières étant assimilées à des données sensibles quant aux mesures à leur appliquer et nécessitant une analyse d'impact (art. 24 LPD). Cette démarche implique que le responsable du traitement procède à une analyse approfondie et régulière des données dont il a la charge en regard des risques qui les concernent.

[148] Le profilage est défini comme toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique (art. 5 lettre f. LPD).

[149] Le profilage à risque élevé est défini comme tout profilage entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique. (art. 5 lettre f LPD). Le profilage à risque élevé est assimilé à des données sensibles au niveau des mesures de protection à leur appliquer.

[150] « *Lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, le responsable du traitement procède au préalable à une analyse d'impact relative à la protection des données personnelles (art. 22 al. 1 LPD). L'analyse d'impact contient une description du traitement envisagé, une évaluation des risques pour la personnalité ou les droits fondamentaux de la personne concernée, ainsi que les mesures prévues pour protéger sa personnalité et ses droits fondamentaux* ».

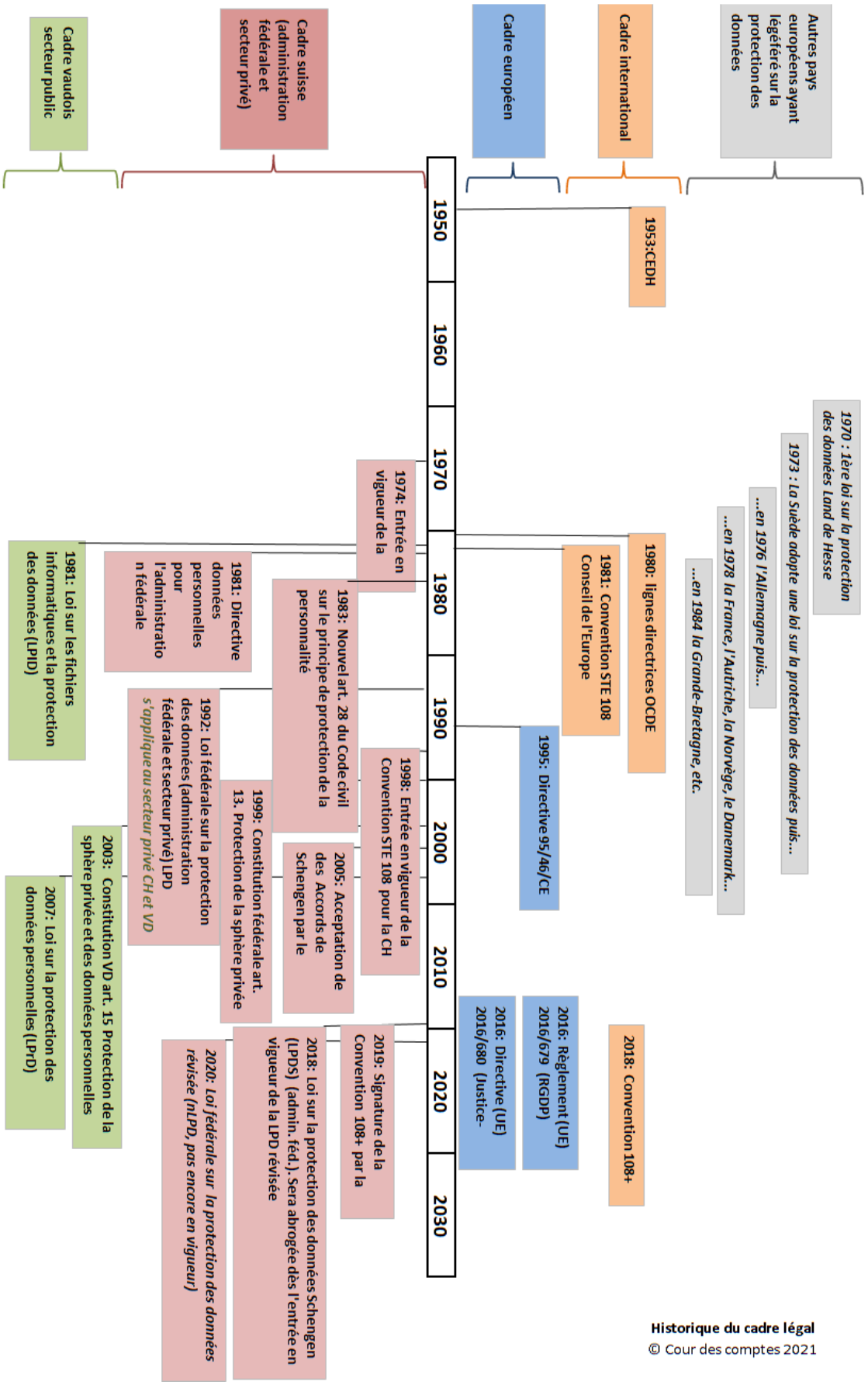
[151] Ce registre doit contenir notamment : l'identité du responsable du traitement, la finalité du traitement, une description des catégories de personnes concernées et des catégories de données personnelles traitées, les catégories de destinataires, dans la mesure du possible, le délai de conservation des données personnelles ou les critères pour déterminer la durée de conservation, dans la mesure du possible, une description générale des mesures visant à garantir la sécurité des données, en cas de communication de données personnelles à l'étranger, le nom de l'État concerné et les garanties prévues.

Le principe de protection des données, dès la conception et par défaut, implique que tout projet traitant de données personnelles doit comporter un volet analytique en la matière et ce, dès le début.

La responsabilité des entités gérant des données personnelles s'étend également aux sous-traitant auxquels des données personnelles sont confiées, ce qui implique l'établissement de clauses contractuelles adéquates.

La mise sur pied d'un registre des activités de traitement (art. 12 LPD) nécessite l'élaboration d'une documentation beaucoup plus détaillée des données et des traitements réalisés, que pour le registre des fichiers exigés par la précédente législation.

8.3 ANNEXE III : HISTORIQUE DU CADRE LÉGAL



Historique du cadre légal
© Cour des comptes 2021

8.4 ANNEXE IV : EXEMPLE D'ACCORD DE CONFIDENTIALITÉ POUR L'ACCÈS À UNE APPLICATION SENSIBLE

canton de vaud

Demande d'accès au Système d'Information RDU

Ce document constitue la demande d'accès au SI RDU. La personne demandant l'accès, signe l'accord de confidentialité et son supérieur hiérarchique, respectivement, pour les apprentis-ies son formateur responsable, valident la demande.

A) Accord de confidentialité et de protection des données concernant le SI RDU

OBJET
Cet accord de confidentialité précise les points sur lesquels les personnes accédant aux données du SI RDU doivent s'engager en matière de sécurité et de traitement des données. Le traitement des données contenues dans le SI RDU est régi principalement par la LHPS et par la loi cantonale sur la protection des données personnelles, la loi sur l'information et la loi sur personnel de l'Etat de Vaud. Les prescriptions contenues dans ce document précisent et s'ajoutent par ailleurs à celles déjà applicables en ce domaine selon les lois fédérales et cantonales, le droit pénal (et en particulier le droit pénal des mineurs pour les apprentis-les mineurs-es), le droit civil, en particulier les art. 97 et suivants, ainsi que 337 et 346 du code des obligations et les art. 143, 143bis, 144, 144bis, 147 et 179novies du code pénal. Pour les apprentis-ies, sont applicables en plus les autres lois spéciales et les directives de service les concernant (Loi sur la formation professionnelle notamment).

PRESCRIPTIONS
Toute personne qui consulte et utilise le SI RDU prend l'engagement de:

- ne pas révéler, utiliser, transmettre ou divulguer à des tiers non expressément autorisés des faits ou des informations auxquelles elle aurait accès;
- n'accéder qu'aux données nécessaires à l'accomplissement de ses tâches ; toute recherche effectuée sur une personne qui n'est pas concernée par le traitement d'un dossier est ainsi passible de sanctions;
- garder le secret, y compris après la fin de son engagement, sur les informations dont elle a eu connaissance dans l'exercice de sa fonction et qui doivent rester secrètes en raison de la loi ou d'un intérêt public ou privé prépondérant
- ne pas réaliser de copie non autorisée de données, même à des fins de tests;
- ne pas chercher à connaître le(s) mot(s) de passe d'un autre utilisateur ni tenter d'accéder à des programmes ou des données informatiques pour lesquels elle n'a pas d'autorisation formelle;
- conserver de manière confidentielle le (ou les) mot(s) de passe qu'elle utilise ou dont elle est responsable dans le cadre de ses fonctions normales et changer ceux-ci au minimum tous les 30 jours;
- changer immédiatement tous les mots de passe dont elle sait que leur intégrité ou leur confidentialité est compromise;
- informer l'organe de gestion du SI RDU dans les plus brefs délais de toute violation des prescriptions ci-dessus ou d'un comportement inapproprié dont elle aurait connaissance.

RESPONSABILITE ET SANCTIONS
En outre, le non respect des obligations légales et des prescriptions ci-dessus peut être considéré par l'employeur comme faute grave, pouvant entraîner la résiliation immédiate du contrat de travail pour justes motifs, en vertu de la loi sur le personnel de l'Etat, des réglementations intercommunales et communales sur le personnel et du Code des obligations (art. 337, 346). Ce non respect entrainera l'application de sanctions conformément à la loi (loi cantonale sur la protection des données personnelles, loi cantonale sur l'information, Code pénal) et le cas échéant une demande de dédommagement pour le tort causé (loi cantonale sur la responsabilité de l'Etat, des communes et de leurs agents), ainsi que la législation applicable aux apprentis-les. Le droit d'être entendu est garanti dans le cadre des procédures susmentionnées.

L'utilisation conforme aux prescriptions du SI RDU fait l'objet de contrôles réguliers par analyse des accès effectués et du contenu des recherches. Toute infraction sera dénoncée à l'employeur et le cas échéant les droits d'accès au SI RDU révoqués. Les modalités des contrôles sont précisées par voie de directive établie par l'organe de gestion du SI RDU.
L'accès au SI RDU est subordonné à la signature du présent document.

ACCEPTATION
Par sa signature, la personne désignée ci-dessous (le cas échéant l'apprenti-ie) certifie qu'elle a pris connaissance des dispositions exposées
ci-dessus et qu'elle s'engage à les respecter dans le cadre de son utilisation du SI RDU.

Désignation de l'entité: . . . . . .

Le/la soussigné-e (collaborateur-trice, apprenti-ie):

Nom . . . . . Prénom . . . . . .

Lieu et date. . . . . Signature . . . . . .

B) Demande validée par (supérieur-e hiérarchique, formateur-trice responsable)

Nom . . . . . Prénom . . . . . .

Fonction . . . . . .

Lieu et date . . . . . Signature . . . .

Le service responsable peut porter le présent accord dûment signé à la connaissance des parents de l'apprenti-ie mineur-e.