



**Réponse de la Municipalité à l'interpellation de Mme Angélique Chatton et consorts
déposée le 9 septembre 2022**

« Risques cybers et protection des données personnelles »

Lausanne, le 7 novembre 2024

Rappel de l'interpellation

« Dans les lignes directrices relatives à la transformation numérique de la Ville de Lausanne, figure le principe de « responsabilité et transparence en matière de captation des données personnelles en application de la LPrD ». Cette interpellation questionne la Municipalité sur la manière dont cela est mis en œuvre en pratique.

Le nombre de cyberattaques ne cesse d'augmenter et touche tous les secteurs. En Suisse, leur nombre a augmenté de 65% entre 2020 et 2021¹. Les institutions publiques n'y font pas exception comme le montrent les récents vols de données dans les communes de Rolle et Montreux ou encore à l'Université de Neuchâtel. Les cyberattaques exposent les organisations qui en sont victimes à différents types de risques :

- risque d'image ;
- risque réglementaire en cas de défaillance grave de l'encadrement des risques cybers étant en dernière instance de la responsabilité du conseil d'administration qui est chargé d'exercer la haute direction de la société et d'établir une organisation appropriée selon le Code suisse des obligations ;
- risque de chantage par les pirates informatiques ;
- risque de paralysie des systèmes d'information et ses potentiels effets en cascade.

Dès lors, disposer d'une connaissance complète et précise des données personnelles traitées et de leurs flux (de la création à la destruction) est essentielle :

- afin de les protéger de manières adéquates vis-à-vis des cyberattaques ;
- en cas de cyberattaque, de pouvoir rapidement identifier les données volées ou corrompues et de prendre les mesures appropriées dans les meilleurs délais.

L'administration communale et ses prestataires sont soumis à la loi cantonale sur la protection des données (LPrD) pour l'encadrement des données personnelles. Les entreprises privées, quant à elles, seront soumises à la nouvelle loi fédérale sur la protection des données (nLPD) dès son entrée en vigueur d'ici début 2023. Ces deux lois visent à prévenir le traitement abusif des données relatives aux personnes et à protéger leur personnalité ainsi que leur sphère privée.

¹ <https://www.ictjournal.ch/etudes/2022-01-11/en-suisse-les-cyberattaques-augmentent-davantage-que-dans-le-monde>.

Le récent audit de l'Administration cantonale vaudoise par la Cour des comptes du canton a mis en évidence des lacunes dans la mise en application de la LPrD² :

- peu d'entités de l'Administration ont procédé à une identification exhaustive des données personnelles traitées ;
- aucune analyse complète en regard des exigences de la LPrD n'a été réalisée ;
- les entités de l'Administration n'ont pas ou peu entamé de réflexion sur la conservation des données personnelles qu'elles gèrent, les stockant le plus souvent indéfiniment sans les avoir anonymisées ».

Introduction

Les risques cyber et la protection des données personnelles sont des préoccupations importantes pour la Municipalité. Dès la fin de l'année 2017, la Municipalité a répondu par son rapport-préavis N° 2017/56 « Dispositif communal de mise en œuvre des mesures liées à la protection des données personnelles » à deux postulats de M. Pierre-Antoine Hildbrand et consorts en créant une commission à la protection des données, suivie plus tard par un poste de responsable de la protection des données permettant de piloter la mise en conformité des traitements de données sous l'autorité de cette commission.

La sécurité des systèmes d'information est une démarche qui est en constante évolution pour faire face aux évolutions technologiques et aux menaces sans cesse grandissantes. Depuis cinq ans, la Ville a mis en place un Système de management de la sécurité de l'information (SMSI)³ offrant un cadre de gouvernance (politiques, directives, processus, etc.) et un pilotage par les risques. Le SMSI et le renforcement des mesures de sécurité ont été réalisés dans le cadre du préavis N° 2015/73 « Renforcement de la sécurité des Systèmes d'Information pour la période 2016-2019 ». Le nouveau préavis N° 2023/47 « Pilotage de la sécurité des systèmes d'information et de la protection des données pour la période 2023-2026 » poursuivra la montée en maturité dans ces domaines.

Il convient de noter que les domaines de la sécurité de l'information, des risques cyber et de la protection des données constituent des points d'examen obligatoire et potentiellement bloquant lors du choix d'une nouvelle solution informatique, ce processus s'effectuant en parallèle des évaluations techniques auxquelles les équipes informatiques procèdent.

² <https://www.vd.ch/toutes-les-autorites/cour-des-comptes/recherche-dans-les-publications-de-la-cour-des-comptes/news/15376i-rapport-n-74-la-protection-des-donnees-personnelles-dans-ladministration-cantonale-vaudoise>.

³ Un SMSI désigne un ensemble de politiques et de processus visant à gérer la sécurité de l'information et à atténuer les risques de cyber sécurité via une approche d'amélioration continue.

Réponse aux questions posées

La Municipalité répond comme suit aux questions posées :

Question 1 : Dans sa vision et principes de la transformation numérique, la Ville de Lausanne se fixe un principe de « responsabilité et transparence en termes de captation des données personnelles en application de la LPrD ». Dans la pratique, comment ces principes sont-ils cadrés et mis en œuvre ? Plus spécifiquement :

- Une analyse complète en regard des exigences de la LPrD (notamment, en lien avec le registre des fichiers) a-t-elle été réalisée ?
- Une identification exhaustive des données personnelles traitées par l'administration de la ville a-t-elle été réalisée ?
- Une politique de conservation claire des données personnelles a-t-elle été définie ? Est-elle mise en œuvre ?

La Ville de Lausanne a validé la mise en place d'un dispositif de gouvernance intitulé Système de gestion de la protection des données (SGPD). Ce dispositif (dont le pendant en matière de sécurité de l'information est le SMSI précédemment cité) définit dans le domaine de la protection des données personnelles un cadre de gouvernance (politiques, directives, processus, etc.) et se base sur un pilotage par les risques et la conformité. Le SGPD comprend notamment une activité d'inventaire des exigences légales auxquelles la Ville est soumise, ainsi qu'un inventaire des données personnelles traitées par l'administration, quelles que soient leurs formes.

Considérant la taille de la Ville et l'ensemble des services fournis à la population, une quantité très importante de données personnelles est traitée au sein du système d'information. La Ville ne peut donc passer à une situation de conformité en peu de temps. Le programme de déploiement du SGPD va se dérouler sur une période de trois à quatre ans.

À ce jour, quatre services de la Ville ont déjà été mis en conformité avec la LPrD, et les données personnelles qu'ils traitent sont déclarées à la Préposée à la protection des données, qui est chargée de tenir un registre public et accessible en ligne (art. 19 LPrD).

Il est à noter que l'inventaire des traitements déclarés et les premières évaluations effectuées ont également pris en compte des exigences de la nouvelle loi sur la protection des données (nLPD), entrée en vigueur le 1^{er} septembre 2023.

Ce travail se poursuit actuellement auprès des 12 services de la Ville les plus concernés par le traitement de données personnelles et sensibles. La démarche d'inventaire des traitements de données et de déclaration à l'Autorité de protection des données et de droit à l'information (APDI) se fait en parallèle avec ces 12 services depuis septembre 2023.

À ce jour, la Ville de Lausanne a soumis au Canton la déclaration de trois services supplémentaires pour validation et publication sur le registre de fichiers tenu par l'APDI.

Pour les neuf autres services, l'état d'avancement est variable et estimé à 60% de réalisation. Plusieurs traitements de données ont été déclarés au Canton et sont en attente de validation par celui-ci.

Par ailleurs, d'autres services volontaires pour leur mise en conformité ont entamé les démarches pour déclarer leurs traitements de données personnelles.

L'inventaire des traitements de la Ville est la condition nécessaire pour effectuer des travaux de mise en conformité complémentaires, par exemple les durées de conservation des données comme l'exige la LPrD.

Question 2 : Plus largement, comment la gouvernance des données s'inscrit-elle dans la gouvernance documentaire énoncée dans le préavis N° 2016/06 ?

Une politique de gouvernance documentaire dans le prolongement du préavis N° 2016/06 « Mise en œuvre d'une gouvernance documentaire pour la Ville de Lausanne » a été adoptée par la Municipalité en 2021. Cette politique formalise le principe d'introduire des règles de conservation des documents et données exploités dans le cadre des activités quotidiennes des services de la Ville, dans le respect des exigences juridiques propres à la protection des données selon le programme SGPD. Les responsables du programme SGPD et de la gouvernance documentaire unissent donc actuellement leurs efforts et œuvrent ensemble à la cohérence des deux programmes.

Question 3 : Quelles ressources (audit, certifications, tests d'intrusion, etc.) sont mises en œuvre pour prévenir les risques cybers ?

La Ville met en œuvre plusieurs moyens de prévention et compte améliorer l'existant par l'utilisation de technologies complémentaires :

- le SMSI mentionné plus haut a permis de mettre en œuvre une gestion des risques de sécurité, ces derniers faisant l'objet d'un suivi régulier et d'un rapport annuel à la Municipalité ;
- le processus de gestion de projets informatiques intègre les évaluations préalables ainsi que les jalons de contrôle et de validation pour la sécurité et la protection des données ;
- des audits de sécurité sont réalisés régulièrement et vont être systématisés à l'avenir, avec un programme d'audit annuel. Dans le cadre des projets informatiques, des tests d'intrusion ou Pentest⁴ sont systématiquement réalisés avant la mise en production des applications accessibles via internet et des applications considérées comme critiques pour le bon fonctionnement de la Ville ;
- un plan de formation et de sensibilisation accessible et mieux adapté aux différents profils des collaboratrices et collaborateurs est prêt à être déployé (fin 2023-début 2024) et sera obligatoire pour tout le personnel de la Ville. Cet axe sera majeur car la personne utilisatrice, devenue le maillon faible, est particulièrement ciblée par les pirates et attaquants ;
- les bonnes pratiques de sécurisation et de recherches de vulnérabilités sont mises en œuvre à tous les niveaux pour éliminer d'éventuelles faiblesses ;
- les journaux d'événements des systèmes sont surveillés, et en particulier ceux de tous les systèmes de sécurité.

⁴ Lors d'un test d'intrusion, le testeur adopte la position de l'attaquant potentiel (hacker). Le principal but de cette manœuvre est de trouver des vulnérabilités exploitables en vue de proposer un plan d'actions permettant d'améliorer la sécurité du système d'information, afin notamment d'empêcher des pirates informatiques de compromettre l'informatique de la Ville.

Le préavis N° 2023/47 « Pilotage de la sécurité des systèmes d'information et de la protection des données pour la période 2023-2026 » prévoit de renforcer les actions en cours et d'automatiser le processus de surveillance des événements dits de sécurité.

Question 4 : Par ailleurs, comment la Municipalité s'assure-t-elle que les dispositifs nécessaires à la mise en conformité de la nLPD soient mis en place au sein des entreprises dont elle est actionnaire majoritaire ? Quelles ressources (audit, certifications, tests d'intrusion, etc.) sont mises en œuvre par ces dernières pour prévenir les risques cybers ?

Les entreprises dont la Ville est actionnaire majoritaire sont soumises à la nLPD au même titre que toute autre entreprise dans le canton de Vaud. Il leur appartient en tant qu'entités indépendantes de s'assurer de leur conformité par rapport aux obligations légales.

La Municipalité estime avoir ainsi répondu aux questions de Mme Angélique Chatton et consorts.

Ainsi adopté en séance de Municipalité, à Lausanne, le 7 novembre 2024.

Au nom de la Municipalité

Le syndic
Grégoire Junod



Le secrétaire
Simon Affolter

