



## REPONSE DU CONSEIL D'ETAT

### à l'interpellation Denis Dumartheray et consorts au nom du groupe UDC - Protection des données personnelles (LPrD) – non-respect des dispositions de la loi (23\_INT\_29)

#### **Rappel de l'intervention parlementaire**

*À la suite des déboires des communes de Rolle et de Montreux, qui ont été victimes de cyberattaques en automne 2021, la Municipalité de Gilly a demandé des garanties à son fournisseur informatique d'applications-métier hébergées.*

*En effet, selon la Loi sur la protection des données (LPrD), chaque commune est considérée comme « Responsable de Traitement » et se doit de prendre les mesures nécessaires pour s'assurer de la conformité à la protection des données de ses sous-traitants.*

*A cet effet, une check-list pour « contrat de sous-traitance de solution informatique externalisée » est fournie par le Canton de Vaud via son site.*

*La commune de Gilly a initié une demande en ce sens en octobre 2021 auprès de son prestataire, qui n'a pas daigné fournir les documents requis par la Loi, malgré de multiples rappels.*

*Afin de faire avancer le dossier, la Municipalité a sollicité l'aide de la Préposée cantonale à la protection des données, dès décembre 2021.*

*Cela fait désormais 16 mois que nous nous battons en vain pour obtenir satisfaction auprès de notre fournisseur, qui est l'un des prestataires reconnus et implantés auprès de nombre de petites communes vaudoises.*

*Entre temps, le dossier a été clos et auprès de l'autorité cantonale et dénoncé auprès de l'autorité fédérales (ce qui est dans l'ordre des choses puisque ce prestataire est une entreprise privée dépendant donc directement du PFPDT, alors qu'une commune dépend directement de l'autorité cantonale).*

*Toutefois, la Préposée a également précisé « Finalement, nous nous permettons de vous rappeler qu'il appartient à la Commune de Gilly, en sa qualité de responsable du traitement, de prendre les mesures nécessaires pour s'assurer de la conformité à la protection des données. En cas de sous-traitance, le responsable du traitement demeure en effet le premier responsable du traitement des données à l'égard des personnes concernées. Or, la situation en souffrance est difficilement admissible sur le principe. Des mesures doivent être mises en place pour y remédier. »*

*Il est donc urgent que nous puissions tous agir pour obtenir les garanties écrites imposées par la LPrD conformément aux point 4 à 13 de la check-list pour « contrat de sous-traitance de solution informatique externalisée » fournie par le Canton, auprès des fournisseurs de services hébergés des communes vaudoises.*

*Va-t-on attendre une attaque de grande ampleur sur les serveurs des fournisseurs hébergeant les applications-métiers de communes vaudoises, comme vécue récemment par Winbiz, paralysant des milliers d'entreprises et mettant en danger les données personnelles de dizaines de milliers de personnes au bas mot, pour agir ?*

*Dès lors, j'ai l'honneur de poser les 2 questions suivantes :*

- De quelle manière l'exécutif d'une commune de la taille de Gilly (1'480 habitants environ au 31.12.2022) peut-il remédier à cette situation, si l'Autorité cantonale est impuissante ?*
- Comment le Conseil d'État peut-il soutenir les communes qui aujourd'hui sont dans le même cas de figure que la commune de Gilly afin d'obtenir le respect Loi du 11 septembre 2007 sur la protection des données personnelles ? (LPrD)*

## Réponse du Conseil d'Etat

Le Conseil d'Etat souhaite tout d'abord rappeler que, l'autonomie communale dans le canton de Vaud est un pilier de l'organisation politique et administrative, permettant aux communes de gérer des questions locales spécifiques tout en respectant le cadre législatif défini par le canton et la Confédération.

Cette autonomie est garantie par la Constitution vaudoise, à son article 76 CstVD : « *les communes sont autonomes, sous réserve des compétences que la Constitution et la loi attribuent à l'Etat* ». Les communes vaudoises ont ainsi le droit, mais également la responsabilité, de gérer leurs propres affaires dans les domaines qui leur sont propres, comme l'urbanisme, l'éducation, et la fiscalité locale. La législation cantonale définit pour chaque domaine le périmètre de l'autonomie des communes, leurs compétences, leur organisation administrative, et leur gestion financière. Elle s'appuie sur les principes définis dans la Constitution cantonale. Le canton peut toutefois développer dans certains domaines des outils permettant aux communes d'accomplir plus facilement leurs obligations légales (p. ex : règlements-types, aide-mémoire pour les autorités communales).

### ***De quelle manière l'exécutif d'une commune de la taille de Gilly (1'480 habitants environ au 31.12.2022) peut-il remédier à cette situation, si l'Autorité cantonale est impuissante ?***

La loi du 11 septembre 2007 sur la protection des données personnelles (LPrD) prévoit la possibilité, pour les entités qui lui sont soumises, de confier à un tiers un traitement de données. Outre les conditions légales de l'art. 18 LPrD, il incombe également au responsable du traitement, ici l'autorité communale concernée, de veiller au respect des règles légales applicables en la matière. Cette obligation inclut entre autres de *prendre des mesures appropriées pour garantir la sécurité des fichiers et des données personnelles, soit notamment contre leur perte, leur destruction, ainsi que tout traitement illicite*.

Dès lors, s'agissant d'un contrat de prestations privé entre la Municipalité et son fournisseur informatique, la commune peut, sous réserve des conditions contractuelles, résilier le contrat lorsque les modalités ne sont pas respectées.

La conclusion d'un contrat de prestations informatiques offre au responsable du traitement la possibilité de détailler, avec le prestataire, non seulement les règles nécessaires au respect des exigences légales de protection des données personnelles mais également les modalités de collaboration entre les parties au contrat. Le responsable du traitement doit donc veiller à ce que le fournisseur, ici informatique, offre une prestation réellement apte à garantir la sécurité des données transmises. La sécurité est notamment garantie par l'inscription, dans le contrat, de mesures organisationnelles et techniques supplémentaires et par la vérification subséquente par le responsable du traitement de leur mise en œuvre par le sous-traitant (gouvernance). Ces mesures sont le résultat de l'auto-évaluation faite par l'autorité communale quant à son choix de faire traiter des données par un tiers.

Concrètement, il peut être utile, pour qu'une commune vaudoise obtienne les garanties écrites des fournisseurs d'hébergement, qu'elle exige des clauses contractuelles strictes, des audits réguliers et la fourniture de documents, conformément à l'article 18 de la LPrD et aux directives cantonales. La liste ci-après, non exhaustive, de points à régler dans un contrat est recommandée :

- **Droit de regard et d'audit** : insérer des clauses permettant à la commune de vérifier sur place (audits) ou via des rapports que le fournisseur respecte ses engagements.
- **Disponibilité des services** : inclure des garanties de niveau de services (SLA) notamment en ce qui concerne leur disponibilité.
- **Détermination des parties qui exécutent les services** : étendre les clauses contractuelles à toute autre entité du fournisseur ou à ses sous-traitants.
- **Sécurité des données** : demander des preuves des mesures de sécurité techniques (chiffrement, sauvegardes) et organisationnelles (formation, procédures d'urgence).
- **Traitement des incidents** : définir clairement les procédures de notification et de gestion des incidents de sécurité et des violations de données.

- **Lieu de stockage** : préciser où les données sont stockées (Suisse/UE idéalement).
- **Droit de résiliation** : prévoir des clauses de résiliation en cas de manquement grave aux obligations LPrD.
- **Demander des attestations** : exiger des certifications (ISO 27001, etc.) ou des rapports d'audit indépendants.
- **Exiger des garanties écrites** : faire confirmer explicitement chaque point de la check-list<sup>1</sup> mentionnée par l'interpellant par écrit dans le contrat.

Le canton met à disposition des communes un modèle de contrat en la matière<sup>2</sup>.

En ce qui concerne la surveillance des sous-traitants d'entités publiques cantonales ou communales en matière de protection des données, celle-ci a soulevé des questions à la suite du cas de la Commune de Gilly, notamment sous l'angle de la répartition des compétences entre le Préposé fédéral à la protection des données et la transparence (PFPDT) et les autorités cantonales de protection des données. En effet, certains cantons, à l'instar du Canton de Vaud, ne prévoient pas expressément la possibilité pour l'autorité cantonale de protection des données d'ouvrir une procédure de surveillance à l'encontre du sous-traitant. Un processus a en conséquence été mis en place pour régler la problématique dans le cas où une situation similaire devait se reproduire. Cette question sera au demeurant traitée dans le cadre de la révision de la LPrD. En effet, le projet de loi, actuellement soumis à consultation, prévoit la possibilité pour l'autorité d'ouvrir, d'office ou sur dénonciation, une enquête contre un responsable du traitement, possibilité qui fait actuellement défaut. Cette nouveauté permet au canton d'être en conformité avec les exigences du droit supérieur.

***Comment le Conseil d'État peut-il soutenir les communes qui aujourd'hui sont dans le même cas de figure que la commune de Gilly afin d'obtenir le respect Loi du 11 septembre 2007 sur la protection des données personnelles ? (LPrD)***

L'Etat ne peut pas prendre le contrôle des données des entreprises ou des communes pour les protéger. Cependant, il a développé des modules de formation et de prévention, qu'il met à leur disposition, permettant de réduire certains risques. Ce sont des éléments importants pour diminuer l'exposition des entreprises et des communes. Il est également en appui en cas de crise, pour des interventions urgentes.

En ce qui concerne plus particulièrement la thématique des cyberattaques, le canton a rencontré en novembre 2021 les faïtières des communes pour leur proposer un catalogue d'interventions possibles en cas d'attaques, une liste des bonnes pratiques, des formations pour leur personnel et la mise à jour de l'application développée avec la Chambre vaudoise du commerce et de l'industrie pour sensibiliser les entreprises à ces problèmes, pour correspondre à leurs besoins.

En janvier 2024 est entrée en vigueur une convention « cybersecurité », signée entre l'Union des communes vaudoises (UCV) et l'Association de communes vaudoises (AdCV) d'une part, et le canton de Vaud d'autre part<sup>3</sup>. Celle-ci prévoit la mise à disposition d'une force d'intervention cantonale pour soutenir les communes et associations intercommunales contre les cyberattaques. Elle couvre les prestations suivantes :

- Préparatifs AVANT une cyberattaque (conseils spécialisés sur site ou à distance, formation, veille)
- Gestion de crise PENDANT une cyberattaque (numéro d'urgence, cellule de crise, équipe de réponse technique, coordination de la communication)

<sup>1</sup>[https://www.vd.ch/fileadmin/user\\_upload/themes/etat\\_droit/protection\\_des\\_donnees\\_et\\_transparence/fichier\\_pdf/Check-list\\_pour\\_un\\_contrat\\_de\\_sous-traitance\\_informatique.pdf](https://www.vd.ch/fileadmin/user_upload/themes/etat_droit/protection_des_donnees_et_transparence/fichier_pdf/Check-list_pour_un_contrat_de_sous-traitance_informatique.pdf)

<sup>2</sup>[https://www.vd.ch/fileadmin/user\\_upload/organisation/dinf/dsi/fichiers\\_pdf/Contrats/ACTDP\\_Accord\\_de\\_traitement\\_donn%C3%A9es\\_personnelles.pdf](https://www.vd.ch/fileadmin/user_upload/organisation/dinf/dsi/fichiers_pdf/Contrats/ACTDP_Accord_de_traitement_donn%C3%A9es_personnelles.pdf)

<sup>3</sup> [https://www.vd.ch/fileadmin/user\\_upload/organisation/dinf/dsi/fichiers\\_pdf/securite/Cybersecurite-CON-CAN-COM.pdf](https://www.vd.ch/fileadmin/user_upload/organisation/dinf/dsi/fichiers_pdf/securite/Cybersecurite-CON-CAN-COM.pdf)

- Plan d'amélioration APRES une cyberattaque (retour d'expérience en vue de tirer des enseignements, plan d'actions d'amélioration / correctives).

En contrepartie de cette prestation, l'UCV verse 410'000 francs par an au canton. A noter que les communes conservent une totale autonomie sur la gestion de leur informatique – il peut ainsi y avoir 300 systèmes différents dans le canton.

Enfin, l'Etat de Vaud met sur son site internet et via son application mobile de nombreuses informations en lien avec la protection des données et la cybersécurité<sup>4</sup>.

Ainsi adopté, en séance du Conseil d'Etat, à Lausanne, le 24 juin 2026.

La présidente :

*C. Luisier Brodard*

Le chancelier :

*M. Staffoni*

---

<sup>4</sup> <https://www.vd.ch/etat-droit-finances/protection-des-donnees-et-droit-a-linformation/protection-des-donnees#c2065648>  
<https://www.vd.ch/dadn/dgnsi/cybersecurite>