



Épalinges
Commune

Réponse de la Municipalité à une interpellation

« Protection des données personnelles au sein de la commune » déposé par Mme la Conseillère communale Ardiane Pasquier

Secrétariat municipal

Nom du représentant de la Municipalité : M. le Syndic Alain Monod

Réponse à l'interpellation adoptée par la Municipalité le 28.09.2026

Table des matières

Objet de l'interpellation	2
Réponse de la Municipalité	4

Objet de l'interpellation

Lors de la séance du Conseil communal du 1^{er} septembre 2026, Mme la Conseillère communale Ardiane Pasquier a déposé l'interpellation suivante :

Cette interpellation fait suite à la réception, par l'intermédiaire de la plateforme de partage destinée aux conseillers communaux, de données personnelles concernant chacun d'entre nous.

Parmi les informations transmises figuraient notamment des données considérées comme sensibles au regard de la nouvelle Loi fédérale sur la protection des données (nLPD) et de la législation cantonale applicable (LPrD), telles que les noms, prénoms, adresses, numéros IBAN ou encore dates de naissance.

Prises individuellement ou combinées, ces informations peuvent être exploitées à des fins frauduleuses par des personnes mal intentionnées : usurpation d'identité, prise de contrôle de comptes bancaires ou accès non autorisé à certains services. En d'autres termes, l'ensemble des personnes concernées s'est retrouvé exposé à un risque en cas d'accès illicite à ces données.

Ce risque ne doit pas être sous-estimé. Selon l'Office fédéral de la cybersécurité (OFCS), plus de 64'000 cybers incidents ont été signalés en Suisse en 2025, soit en moyenne près de 180 signalements par jour / env. 8 par heure. Près de 90% des annonces concernent des particuliers, démontrant que le risque n'affecte pas uniquement les entreprises mais également les citoyens. Par ailleurs :

- nous utilisons principalement des équipements privés ;*
- nos pratiques de stockage et de protection des données sont variables ;*
- nous ne sommes pas, pour la plupart, des spécialistes de la sécurité informatique.*

Je tiens à préciser que les données concernées ont depuis été retirées de la plateforme. Cet incident soulève toutefois plusieurs questions plus larges concernant la gestion et la protection des données personnelles au sein de notre commune.

La protection des données constitue aujourd'hui un domaine essentiel et en constante évolution. En tant qu'autorité publique, notre commune est tenue de respecter strictement les dispositions légales destinées à protéger les citoyens et leurs informations personnelles.

Au-delà des éventuelles conséquences financières qu'une violation pourrait entraîner (généralement une amende de maximum 250'000 CHF par cas et par personne), l'enjeu principal demeure le respect des droits fondamentaux des habitants. La législation impose notamment les principes de proportionnalité, de finalité du traitement, de confidentialité, de minimisation et, lorsque cela est possible, d'anonymisation des données. Elle prévoit également des obligations de transparence et d'information lorsque des incidents affectent des données personnelles.

La loi encadre par ailleurs de manière stricte la gestion des violations de données, communément appelées data breaches. Selon l'article 24 de la nLPD, lors d'une violation de la sécurité des données et sous certaines conditions, le Préposé fédéral à la protection des données et à la transparence doit être informé dans les meilleurs délais. Ces obligations peuvent également s'appliquer lorsqu'une erreur humaine conduit à rendre accessibles des données personnelles à des personnes qui ne sont pas autorisées à les consulter, y compris au sein des autorités communales (dont font partie les conseillers et les membres des commissions).

Sur cette base, j'adresse les questions suivantes à notre municipalité :

- *Quelles mesures sont mises en œuvre pour limiter les risques internes liés à la consultation, à la conservation ou à la diffusion non autorisée des données personnelles ?*
- *Quels mécanismes garantissent que les données des habitants ne sont accessibles qu'aux personnes qui en ont strictement besoin dans l'exercice de leurs fonctions ?*
- *Comment les données sont-elles stockées et protégées (serveurs, solutions cloud, chiffrement, systèmes de détection et de prévention des intrusions) ? Des audits de sécurité ou des tests d'intrusion sont-ils réalisés régulièrement ?*
- *Quel protocole encadre la gestion des erreurs, incidents ou violations impliquant des données personnelles ou sensibles ?*
- *La Municipalité dispose-t-elle d'une procédure de notification au Préposé fédéral et au Préposé cantonal en cas de violation de données lorsque la loi l'exige ?*
- *Les habitants concernés sont-ils informés lorsqu'un incident de sécurité implique leurs données personnelles ?*



L'accès potentiellement étendu à certaines données sensibles, combiné aux risques croissants liés à la cybersécurité et aux obligations légales applicables en cas de violation, constitue un enjeu important tant pour les habitants que pour les membres des autorités communales.

Il apparaît dès lors nécessaire d'obtenir des clarifications sur les mesures actuellement en place ainsi que sur les éventuelles améliorations envisagées, afin de garantir un niveau adéquat de protection des données personnelles au sein de notre commune.

Je remercie la Municipalité pour ses réponses.

Réponse de la Municipalité

En préambule, la Municipalité souhaite préciser le cadre légal applicable en matière de protection des données.

Dans l'accomplissement de ses tâches publiques, la Commune est soumise à la législation cantonale en matière de protection des données, en particulier à la Loi du 11 septembre 2007 sur la Protection des Données Personnelles (ci-après : LPrD). La Loi fédérale du 25 septembre 2020 sur la Protection des Données (LPD) ne s'applique pas aux traitements de données effectués par les communes vaudoises dans l'accomplissement de leurs tâches publiques mais concerne uniquement les personnes privées ainsi que les organes fédéraux.

Par ailleurs, conformément à son champ d'application, la LPrD ne s'applique notamment pas aux délibérations du Grand Conseil et des conseils généraux et communaux, aux procédures civiles, pénales ou administratives, ainsi qu'aux données personnelles traitées en application de la législation fédérale sur le renseignement.

C'est dans ce cadre que la Municipalité répond aux différentes questions soulevées par l'interpellation.

1. Quelles mesures sont mises en œuvre pour limiter les risques internes liés à la consultation, à la conservation ou à la diffusion non autorisées des données personnelles ?

L'administration communale applique différentes mesures organisationnelles et techniques visant à limiter ces risques. Les collaborateurs sont notamment tenus au respect du secret de fonction et des règles applicables en matière de protection des données et de sécurité de l'information.

Les accès aux données et aux applications informatiques sont attribués en fonction des tâches et responsabilités exercées. Des mesures techniques de sécurisation des postes de travail, des comptes utilisateurs et des systèmes informatiques complètent ce dispositif.

2. Quels mécanismes garantissent que les données des habitants ne sont accessibles qu'aux personnes qui en ont strictement besoin dans l'exercice de leurs fonctions ?

Les droits d'accès aux applications et aux données sont définis en fonction des besoins liés à l'activité professionnelle des collaborateurs et des missions des différents services. Le principe appliqué consiste à limiter ces accès aux ressources nécessaires à l'exercice des fonctions concernées. Les droits peuvent ainsi différer selon les services, les responsabilités et les applications utilisées.

Lors de changements de fonction ou de départs de collaborateurs, les droits d'accès sont adaptés ou supprimés. La migration informatique en cours auprès de la Ville de Pully constitue également l'occasion de revoir et d'harmoniser les processus de gestion des accès.

3. Comment les données sont-elles stockées et protégées ? Des audits de sécurité ou des tests d'intrusion sont-ils réalisés régulièrement ?

Les données de l'administration sont actuellement hébergées et exploitées au moyen des infrastructures et solutions informatiques en place, qui disposent de différentes mesures de protection, notamment en matière de contrôle des accès, de sauvegarde et de sécurisation des systèmes et des réseaux.

La conservation des données est par ailleurs effectuée conformément aux dispositions légales applicables, notamment en matière de protection des données et d'archivage.

De plus, la Commune est engagée dans une migration progressive de son environnement informatique auprès de la Ville de Pully. Cette démarche vise notamment à renforcer la sécurité des systèmes et des données, à bénéficier d'une infrastructure mutualisée et à améliorer la gestion et le suivi des mesures de protection.

Durant cette phase de transition, les dispositifs existants continuent de s'appliquer et sont progressivement adaptés au nouvel environnement informatique. Certaines prestations demeurent par ailleurs assurées par des prestataires externes spécialisés.

Pour des raisons de sécurité informatique, la Municipalité ne communique pas publiquement le détail de l'architecture de ses systèmes, des dispositifs de protection déployés ou de leur configuration.

La migration en cours constitue ainsi également une opportunité de renforcer et d'harmoniser les pratiques en matière de sécurité informatique et de protection des données au sein de l'administration communale.

4. Quel protocole encadre la gestion des erreurs, incidents ou violations impliquant des données personnelles ou sensibles ?

Tout incident susceptible d'affecter la confidentialité, l'intégrité ou la disponibilité de données doit être signalé et traité selon les procédures applicables.

Lorsqu'un incident concerne des données personnelles, son ampleur, la nature des données concernées, les personnes potentiellement touchées ainsi que les conséquences et risques qui en découlent doivent être évalués. Les mesures nécessaires sont ensuite prises afin de contenir l'incident, d'en limiter les conséquences et, lorsque cela est possible, d'en déterminer la cause et d'éviter sa répétition.

5. La Municipalité dispose-t-elle d'une procédure de notification au Préposé fédéral et au Préposé cantonal en cas de violation de données lorsque la loi l'exige ?

En cas de violation de la sécurité des données, la Commune examine les obligations qui lui incombent au regard de la législation applicable et procède, lorsque les conditions légales sont remplies, aux communications requises auprès de l'autorité compétente. Il n'y a dès lors pas lieu de prévoir une notification systématique tant au Préposé fédéral qu'à l'autorité cantonale ; l'autorité compétente est déterminée en fonction du régime juridique applicable.

6. Les habitants concernés sont-ils informés lorsqu'un incident de sécurité implique leurs données personnelles ?

La survenance d'un incident impliquant des données personnelles n'entraîne pas nécessairement et automatiquement une information individuelle des personnes concernées. Chaque situation doit être appréciée en fonction des circonstances, de la nature des données concernées, de l'importance de l'incident, des risques susceptibles d'en découler pour les personnes concernées et des exigences prévues par la législation applicable.

Lorsque les conditions légales imposent ou justifient une information des personnes concernées, la Commune prend les mesures nécessaires afin de les informer de manière appropriée.

Conclusion

La Municipalité considère la sécurité de l'information et la protection des données personnelles comme des enjeux essentiels. Les mesures en place reposent à la fois sur des règles organisationnelles, une gestion des droits d'accès et différents dispositifs techniques de protection. La migration informatique en cours auprès de la Ville de Pully s'inscrit dans cette démarche et doit permettre de renforcer progressivement la sécurité des systèmes et des données, ainsi que d'harmoniser les pratiques au sein de l'administration. Cette transition constitue également l'occasion de revoir et, lorsque cela s'avère nécessaire, d'adapter les processus internes en matière de gestion des accès, de protection des données et de traitement des incidents.



La Municipalité entend ainsi poursuivre l'amélioration de ses dispositifs afin de tenir compte de l'évolution des risques, des technologies et des exigences en matière de protection des données.

Épalinges, le 28.09.2026

Au nom de la Municipalité

Le Syndic :

Alain Monod

Le Secrétaire municipal :

Damien Bally

