

DIRECTIVE SUR LA PROTECTION DES DONNÉES

TABLE DES MATIÈRES

1	Préambule.....	1
2	Définitions.....	1
3	Champ d'application	2
4	Directives sur la protection des données.....	2
4.1	Gouvernance.....	2
4.1.1	Registre des données sensibles	2
4.1.2	Gestion des risques.....	2
4.1.3	Gestion des violations de données.....	2
4.1.4	Confidentialité et sensibilisation des collaborateurs.....	3
4.1.5	Gestion du changement.....	3
4.2	Traitements.....	3
4.2.1	Légalité et minimisation des données.....	3
4.2.2	Conservation et exactitude des données.....	4
4.2.3	Demandes des personnes concernées	4
4.2.4	Gestion des sous-traitants.....	4
4.2.5	Communications de données	5

1 PRÉAMBULE

Le but de ce document est de définir au niveau tactique les exigences permettant de protéger les données personnelles traitées par la Commune de Rolle (ci-après « la Commune ») conformément aux principes de mise en œuvre défini dans la Politique de protection des données.

2 DÉFINITIONS

Les définitions utiles se trouvent dans la Politique de protection des données personnelles.



3 CHAMP D'APPLICATION

Ce document s'applique à l'ensemble du domaine d'application du Système de gestion de la protection des données de la Commune tel qu'établi dans la politique dédiée (PPD).

4 DIRECTIVES SUR LA PROTECTION DES DONNÉES

4.1 GOUVERNANCE

4.1.1 Registre des données sensibles

Un registre des données sensibles liste les données sensibles traitées par chaque service, les types de supports, ainsi que leur localisation, afin de s'assurer que les mesures adéquates soient mises en œuvre conformément à l'analyse des risques. Le Greffe est responsable de mettre à jour ce registre en présence d'une nouvelle activité de traitement, respectivement de le réviser au minimum tous les deux ans, avec la participation de chaque service.

4.1.2 Gestion des risques

L'analyse des risques en matière de protection des données est effectuée conjointement par le Greffe et le Secteur informatique, ce dernier étant responsable de l'analyse des risques sous l'angle de la sécurité des données conformément à la Politique de sécurité de l'information. L'analyse des risques liste les risques identifiés, en fonction de la probabilité et gravité de leur survenance, et les mesures mises en œuvre pour les traiter. L'analyse des risques est revue au minimum tous les deux ans et validée par la Municipalité.

4.1.3 Gestion des violations de données

Une équipe d'intervention en cas de violation de données est constituée. Sa mission consiste à fournir une réponse immédiate, efficace et compétente à toute violation de données supposée ou réelle affectant la Commune. Le processus d'intervention en cas de violation de données est lancé lorsque quiconque constate qu'une violation présumée de données s'est produite, et que tout membre de l'équipe d'intervention en est informé. Il existe une procédure détaillant le déroulement des actions et les tâches respectives de chaque membre de l'équipe d'intervention.

L'équipe d'intervention est composée des fonctions suivantes :

- Municipalité: Syndic ou son remplaçant
- Technique: Responsable informatique
- Secrétaire municipal ou son remplaçant
- Chef du Service des finances et de l'informatique

Si nécessaire, les membres de l'équipe peuvent également faire appel à des prestataires externes (par exemple en matière de cybersécurité ou de communication de crise).

L'équipe doit mettre en œuvre les mesures suivantes :

- Analyser l'incident et déterminer s'il s'agit d'une violation de données, si nécessaire en collaboration avec le prestataire externe.
- Notifier dès que possible la force de réaction cantonale de la DGNSI et les autorités compétentes.



- Coordonner les opérations avec les différents intervenants et leur fournir les informations utiles.
- Veiller à ce que les personnes concernées soient correctement informées, si nécessaire.

La **Municipalité** est responsable des décisions d'ordre stratégique et financier, ainsi que de la communication interne et externe.

4.1.4 Confidentialité et sensibilisation des collaborateurs

Le **Responsable des RH** s'assure que tout collaborateur, même temporaire, ayant accès aux données personnelles, ait signé un engagement de confidentialité par le biais du contrat de travail, la charte de protection des données, ainsi que la charte informatique s'il doit accéder aux systèmes de la Commune par le biais d'un document indiquant qu'il a bien pris connaissance du règlement du personnel dont ces chartes font partie intégrante.

Le **Responsable des RH** et le **Greffé** organise chaque année une séance de sensibilisation à la protection des données à l'attention des collaborateurs, en collaboration avec le **Responsable informatique** pour les thématiques de sécurité.

4.1.5 Gestion du changement

Une procédure de gestion du changement est mise en place, afin de s'assurer que les exigences de protection des données soient appliquées par défaut et dès la conception en présence de nouveaux traitements de données ou de modifications substantielles de traitements existants par la Commune. Tout changement majeur ou à risque, notamment en présence de traitement de données sensibles, doit être validé par la **Municipalité**.

Les rôles sont répartis comme suit :

- Le **responsable informatique** est responsable d'analyser tout changement au niveau du système d'information de la Commune ayant un impact sur le traitement des données et la sécurité de l'information, en remplissant la checklist dédiée.
- Les **Chefs de service** sont responsables d'analyser tout nouveau traitement ou collecte de données, par exemple en présence d'une nouvelle prestation de leur service, en remplissant la checklist dédiée et de transmettre cette dernière au Greffé.

Le changement ne peut être appliqué avant que la procédure d'analyse et de validation n'ait été complétée, sous réserve d'une urgence justifiée.

4.2 TRAITEMENTS

4.2.1 Légalité et minimisation des données

Les **Chefs de service** sont responsables de s'assurer que les traitements de données au sein de leur service aient lieu uniquement si:

- une base légale l'autorise;
- leur traitement sert à l'accomplissement d'une tâche publique; ou
- la personne concernée y a consenti ou a rendu ses données accessibles à tout un chacun.

Si le consentement de la personne concernée est nécessaire, à savoir en l'absence d'une base légale ou de l'accomplissement d'une tâche publique, le consentement est enregistré et conservé par le service concerné au

moment de la collecte de données ou du changement de finalité (si des données déjà en possession de la Commune sont utilisées dans un autre but qu'initialement).

Les **Chefs de service** s'assurent également que seules soient collectées et traitées les données nécessaires pour atteindre le but poursuivi ou accomplir la tâche publique concernée (minimisation des données). En particulier, ils respectent les éventuelles directives ou recommandations des services de l'Etat.

4.2.2 Conservation et exactitude des données

Les données sont détruites ou rendues anonymes dès qu'elles ne sont plus nécessaires à la réalisation de la tâche pour laquelle elles ont été collectées, sous réserve des dispositions légales spécifiques, notamment en matière d'archivage. Pour ce faire, une procédure de gestion du cycle de vie des données règle la conservation des données du stockage initial au sort final.

Un calendrier de conservation des documents et données est mis en place, respectivement tenu à jour par le **Greffé** avec la participation des **services**. Ce calendrier définit les durées de conservation des différents types de documents par service, ainsi que leur sort à l'échéance de la durée de conservation.

Chaque **collaborateur** est tenu:

- de stocker les documents et données conformément à la procédure précitée et de respecter les durées fixées dans le calendrier de conservation;
- s'il a accès à la GED, de renseigner une durée de conservation pour tout document qu'il y ajoute, conformément au calendrier de conservation ;
- de conserver uniquement les versions définitives des documents et de supprimer toutes versions de travail ou copies dès qu'elles ne sont plus nécessaires ;
- de corriger immédiatement les données personnelles dès qu'il apprend ou constate qu'elles ne sont pas à jour ou exactes.

La **Municipalité** s'assure et octroie le temps nécessaire aux services pour qu'un tri des documents par service ait lieu au minimum une fois par an, sous la coordination du **Greffé**.

4.2.3 Demandes des personnes concernées

Toute demande d'une personne concernée fondée sur la LPrD, par exemple une demande d'accès à ses propres données, est transmise au **Greffé**, sous réserve d'une demande pouvant être traitée directement par le Contrôle des habitants. Le **Greffé** est responsable de réunir les données personnelles concernées et de répondre à la demande, si nécessaire par le biais d'une décision formelle de la **Municipalité**.

4.2.4 Gestion des sous-traitants

Tout prestataire ou entité externe à l'administration communale traitant des données personnelles pour le compte de la Commune, à savoir tout sous-traitant, doit signer un contrat en vertu duquel il est soumis au secret de fonction et s'engage à respecter les règles en matière de protection des données.

Chaque **Chef de service** est responsable, pour tout sous-traitant avec lequel le service concerné souhaite collaborer, de :

- s'assurer que le sous-traitant présente des garanties et des compétences suffisantes en matière de protection des données (absence d'incidents, etc.) ;

- de soumettre le modèle de contrat validé par la Municipalité au sous-traitant, étant entendu que ce dernier ne peut commencer à traiter les données pour le compte de la Commune tant qu'il n'a pas signé ce contrat ; et
- s'assurer qu'aucune donnée couverte par le secret de fonction ne soit transférée en dehors de Suisse.

Le Greffe s'assure que le contrat ait bien été signé avant de soumettre la collaboration ou le contrat de prestations (c'est-à-dire l'accord principal prévoyant le traitement de données) pour validation municipale. Il tient également à jour une liste des sous-traitants de la Commune et centralise les contrats.

4.2.5 Communications de données

Les Chefs de service s'assurent que tout transfert ou communication de données de leur service à des tiers externes à l'administration communale ait lieu uniquement aux conditions prévues par la législation applicable, qu'il s'agisse de la LInfo ou de lois spécifiques aux métiers du service. Les listes, notamment d'adresses, contenant des données personnelles ne sont transmises qu'après la signature par le demandeur d'un document par lequel il s'engage à utiliser les données uniquement aux fins annoncées.

En présence d'une demande LInfo complexe ou portant sur des données sensibles ou délicates, la demande est transmise au Greffe pour analyse et décision municipale. Cas échéant, les données personnelles sont caviardées, afin de protéger la personnalité des personnes concernées.

Approuvé par la Municipalité dans sa séance du 25 septembre 2023

Au nom de la Municipalité

La Syndique



Monique Choulat Pugnale



La Secrétaire



Tu Wüst