*Fribourg, le 7 janvier 2025*

*L’ATPrDM est d’avis que l’organe législatif est compétent pour adopter un règlement de protection des données et de la sécurité de l’information. Pour cette raison, elle met à disposition un règlement-type détaillé (cf. ci-dessous) qui laisse une marge de liberté pour des modifications et des éventuelles réductions.*

**Règlement-type de protection des données et de sécurité des données**

L’Assemblée communale/Le Conseil général …

Vu :

* La loi du 12 octobre 2023 sur la protection des données (LPrD ; RSF 17.1),
* Le règlement du 29 juin 1999 sur la sécurité des données personnelles (RSD ; RSD 17.15),
* La loi du 25 septembre 1980 sur les communes (LCo ; SRF 140.1),
* Les principes de protection des données de la commune,

décrète :

**1 Généralités**

Art. 1 Buts

Le présent règlement détaille les buts, définis dans la politique de protection des données, et décrit les marches à suivre afin de garantir le traitement des données personnelles conformément à la loi cantonale sur la protection des données et d’assurer la sécurité des données. Il vise à assurer les buts de sécurité de confidentialité, d’intégrité, de disponibilité et de traçabilité et ainsi que de garantir un fonctionnement conforme à la protection des données.

Dans un souci de transparence vis-à-vis des utilisateurs-trices, de promotion d'une utilisation responsable et sécurisée du système d'information et de communication, il définit les règles d'utilisation de ces ressources ainsi que les moyens de contrôle et de surveillance de cette utilisation.

Art. 2 Champ d’application

Le présent règlement s’applique :

1. à tous les employé-e-s de la commune, quel que soit leur statut ; **il fait partie intégrante de leur contrat de travail**. Les employé-e-s l’acceptent par la signature du contrat ;
2. aux mandataires externes et leurs auxiliaires ; il fait partie du contrat de mandat respectivement d’entreprise signé par la commune ;
3. aux élus communaux et élues communales, sous réserve des dispositions de la législation spéciale, notamment la loi sur les communes.

Art. 3 Systèmes d’information et de communication

Le système d’information et de communication (SIC) de la commune comprend tous les dispositifs techniques et organisationnels permettant de collecter, de traiter, de stocker et de transmettre des informations et des données personnelles entre différents utilisateurs ou différentes utilisatrices ou systèmes.

Le/la responsable de la sécurité de l’information (RSI) de la commune tient un inventaire de tous les composants. Celui-ci doit être mis à jour en permanence.

Art. 4 Responsabilités

La commune est responsable de la protection des données personnelles et de la sécurité de l’information et adopte les mesures nécessaires.

Cette tâche incombe au secrétaire communal ou à la secrétaire communale ou à la personne désignée spécialement par le conseil communal en qualité de responsable de la sécurité de l’information et de la protection des données.

Art. 5 Objectifs de sécurité et confidentialité

Le personnel communal est tenu de garantir la confidentialité, l’intégrité, la disponibilité et la traçabilité des données personnelles qu’il traite (collecte, conservation, utilisation, transformation, communication, enregistrement, archivage ou destruction).

Le personnel communal est soumis au secret de fonction. L’obligation subsiste même après la fin des rapports de travail.

Les sous-traitants externes sont soumis aux mêmes règles de confidentialité dans l'exécution de leur contrat avec la commune.

En matière de confidentialité, les élus communaux et élues communales sont tenus aux mêmes règles en application de la législation spéciale, notamment la loi sur les communes.

**2 Protection des données et sécurité des données**

Art. 6 Traitement des données personnelles

Les données personnelles doivent être traitées selon les exigences légales.

Lors du traitement des données personnelles et des données sensibles, les objectifs de sécurité de la confidentialité, de l’intégrité, de la disponibilité et de la traçabilité doivent être garantis.

Art. 7 Propriétaire des données

Si la commune est propriétaire des données, elle est responsable de l'implémentation, de la mise en œuvre et de la formation des mesures de sécurité de l'information et de protection des données nécessaires afin de garantir les objectifs de sécurité.

Art. 8 Communication et transmission de données

Les données ne peuvent être transmises ou communiquées qu'à des personnes et organes autorisés. Voir à ce sujet la fiche d'information de l'ATPrDM sur la communication par courrier électronique (e-mail) de données personnelles et sensibles (<https://www.fr.ch/etat-et-droit/transparence-et-protection-des-donnees/themes-en-matiere-de-protection-des-donnees> / sous la rubrique « Bonnes pratiques »).

Les données personnelles ne peuvent être transmises à des tiers ou à l'étranger que si la personne responsable a vérifié la communication et que les conditions légales prévues aux articles 14 et suivants de la LPrD sont remplies.

Art. 9 Traitement des données à l’étranger

Les données personnelles ne peuvent être traitées qu'en Suisse ou dans un État garantissant un niveau de protection adéquat (cf. la liste exhaustive des Etats dans l’annexe 1 de l'ordonnance fédérale du 31 août 2022 sur la protection des données (OPDo ; RS 235.11 ; [www.fedlex.admin.ch/eli/cc/2022/568/fr](http://www.fedlex.admin.ch/eli/cc/2022/568/fr)).

Les données personnelles ne peuvent être transmises à un tiers et à l'étranger que si la personne responsable a vérifié que les conditions légales prévues aux articles 14 et suivants de la LPrD, notamment celles de l’article 15, sont remplies.

Art. 10 Clear desk policy

Dans les locaux accessibles au public, il est indispensable de mettre en place des mesures actives de protection des données personnelles.

Les règles suivantes s'appliquent notamment aux postes de travail :

Les employé-e-s sont tenu-e-s de verrouiller leur ordinateur lorsqu'ils quittent leur poste de travail, même brièvement. Un verrouillage automatique de l'écran après une certaine période d'inactivité doit être mis en place.

Les documents confidentiels doivent être mis sous clé même en cas d'absence de courte durée et à la fin du travail.

Les demandes d'impression de documents confidentiels adressées à une imprimante centrale doivent être accompagnées d’un code d'impression ou être récupérées immédiatement.

A la fin du travail, les ordinateurs doivent être éteints et mis hors tension.

Art. 11 Cryptage

Les données personnelles sensibles doivent être cryptées par des moyens appropriés (cryptage du contenu), tant lors de leur stockage que lors de leur transmission.

La commune, en tant qu'organe responsable pour la protection des données, met à disposition l'infrastructure nécessaire à cette fin.

Art. 12 Classification des données

En fonction de son contenu, chaque document, physique ou électronique, est à classifier selon les catégories suivantes : « accessible au public (1er degré) », « à usage interne (2ème degré) » ou « confidentiel ou secret (3ème degré) », conformément au règlement du 29 juin 1999 sur la sécurité des données personnelles (RSD, RSF 17.15).

Art. 13 Procédure de connexion et d’authentification

La commune garantit par une procédure d’authentification que seulement les personnes autorisées, les services et applications disposant des droits correspondants peuvent accéder aux ressources de la commune.

L'authentification simple se fait en général avec un nom d'utilisateur personnel ou d’utilisatrice personnelle et un mot de passe secret.

Pour renforcer la sécurité, une troisième information (empreinte digitale, badge, SMS) peut être demandée, spécialement pour l’accès aux données sensibles.

Les employé-e-s ne peuvent utiliser que leur compte d’utilisation personnel respectivement leur login ou des comptes fonctionnels qui leur sont attribués. Ils ou elles sont responsables des accès qui sont effectués avec leur compte.

Si la confidentialité des paramètres d’accès a été compromise pour une raison quelconque (vol, perte, communication par erreur), cela doit être immédiatement signalée au responsable de la sécurité d’information.

Art. 14 Mots de passe

Le nom d'utilisateur et le mot de passe personnel sont utilisés pour l'identification des utilisateurs et des utilisatrices par l'infrastructure SIC. Le mot de passe est strictement personnel et ne doit être en aucun cas communiqué, y compris aux collègues.

Le mot de passe doit respecter les conditions suivantes :

* il doit comporter au moins 11 caractères et être suffisamment complexe (des chiffres, des caractères spéciaux, des majuscules et des minuscules ;
* les mots de passe triviaux tels que "EEEEEEEE" et "12345678" sont interdits ;
* le mot de passe ne doit pas contenir de noms ou de données personnelles, comme la date d’anniversaire, les numéros de téléphone ou d’immatriculation de voiture ;
* le mot de passe personnel doit être modifié à intervalles réguliers (au minimum 2 fois par an) ;
* les mots de passe ne doivent pas être répétés ni incrémentés (par exemple, mot\_de\_passe23, mot\_de\_passe24) ;
* si le mot de passe risque d’être connu par d'autres personnes, il doit être changé immédiatement ;
* le mot de passe ne doit pas être conservé sur le lieu de travail sans être crypté, que ce soit sous forme papier ou électronique.

Les directives doivent être appliquées sur le plan technique et organisationnel.

Art. 15 Destruction de dossiers et de supports de données

Les documents confidentiels ne doivent pas être jetés dans les corbeilles à papier ou les poubelles ordinaires. Seuls les conteneurs spécialement prévus à cet effet doivent être utilisés pour leur élimination.

Les supports de données contenant des données personnelles qui ne sont plus utilisés, doivent être éliminés/effacés de manière appropriée. Un simple effacement n'est pas suffisant.

Art. 16 Sécurité physique

L'accès aux bureaux où sont traitées des données personnelles, n'est autorisé qu'aux employé-e-s de la commune dans le cadre de l'accomplissement de leurs tâches. Des systèmes de sécurité appropriés doivent être mis en place (tels que des plans de fermeture, badge etc.).

L'accès de tierces personnes (tels que des techniciens ou du personnel de nettoyage) doit être autorisé par le responsable de la sécurité de l'information. Selon la nature des tâches et des activités, des mesures de protection spécifiques doivent être définies et mises en œuvre (telles que l’accompagnement personnel, la fermeture des armoires à dossiers, la déconnexion des systèmes, etc.).

Art. 17 Postes de travail informatiques et composants

Les employé-e-s, les élu-e-s et les mandataires sont responsables des données, des ressources matérielles et des logiciels qui leurs sont confiés dans l'exercice de leurs fonctions. Ils doivent les traiter avec prudence et vigilance et sont tenus de signaler tout dysfonctionnement, incident, anomalie ou perte.

La configuration des postes de travail informatiques (PC) ainsi que tous les périphériques mis à disposition par la commune ne doivent pas être modifiés par les utilisateurs et les utilisatrices. Seuls les logiciels, achetés et installés par la commune, peuvent être utilisés. Sont notamment interdits, mais pas exclusivement, les opérations suivantes :

* toute installation non autorisée de logiciels par les utilisateurs ;
* toute utilisation de logiciels sans licence ;
* la désinstallation ou la modification des logiciels et des composants matériels installés par la commune ;
* le raccordement d'appareils privés à l'infrastructure SIC, notamment d'appareils privés de traitement, de stockage ou de transmission de données, étant précisé que l'installation d'une connexion sans fil (WLAN, Bluetooth, etc.) au réseau communal est également considérée comme un raccordement.

Art. 18 Stockage des données

Les données doivent être stockées sur les systèmes mis à disposition par la commune (par exemple, serveur interne, cloud privé de la commune). Les employé-e-s sont tenu-e-s de sauvegarder les données professionnelles uniquement sur ces systèmes. Toute copie ou enregistrement de données personnelles en dehors des espaces prévus à cet effet dans l'infrastructure communale (lecteurs réseau) et des solutions cloud proposées par ICT, est interdit. Cette interdiction s'applique en particulier au stockage des services de stockage en ligne, tels que Dropbox, Google Docs, Google Drive, OneDrive, etc.

Si des appareils mobiles sont utilisés pour certains processus de travail en dehors des locaux communaux, les données doivent ensuite être réenregistrées le plus rapidement possible sur l'infrastructure communale et effacées localement.

Art. 19 Violation de la sécurité des données personnelles

En cas de violation de la sécurité des données personnelles (par exemple, virus, e-mail de phishing, vol de mot de passe), l'employé doit immédiatement en informer son ou sa supérieur-e hiérarchique et le/la responsable de la sécurité de l'information.

La commune veille à ce que la liste des contacts et les procédures à suivre en cas d'incident de sécurité soient à jour et disponibles pour chaque employé. Voir le portail d’annonce de violation de la sécurité des données de l'ATPrDM et les explications à ce sujet sur le site Internet <https://www.fr.ch/etat-et-droit/transparence-et-protection-des-donnees/annonce-de-violation-de-la-securite-des-donnees>

Art. 20 Utilisation d’internet par le personnel communal

En principe, l’accès à Internet doit être réservé à des fins professionnelles.

Une utilisation occasionnelle à des fins privées est tolérée. Dans le cadre de l’utilisation tolérée, l’internet peut être utilisé comme moyen d'information, mais l’accès à des contenus purement récréatifs, tels que des jeux ou des vidéos, n'est pas autorisée. La commune est autorisée à limiter ou à bloquer l'accès aux offres Internet dont l'utilisation n'est pas autorisée ou qui, selon l'expérience, entraînent une utilisation excessive.

Le fait qu’un site soit accessible ne signifie pas que cet accès est autorisé.

L'activité Internet des utilisateurs et utilisatrices est enregistrée.

Art. 21 Courrier électronique (e-mail)

Principe : Les e-mails ne garantissent ni la confidentialité ni l'exactitude de l'expéditeur, du destinataire ou du contenu. Par conséquent, en principe, aucune donnée sensible ne doit être envoyée par e-mail sans un cryptage sécurisé du contenu.

Chaque employé-e dispose, pour ses besoins professionnels, d'une adresse électronique standardisée et personnelle (adresse e-mail) qui lui est attribuée par le responsable de la sécurité de l'information. L'adresse est attribuée et activée à son arrivée et désactivée à son départ.

Les e-mails entrants et leur contenu sont filtrés par un système antivirus et antispam. Le cryptage du contenu des e-mails sortants (y compris leurs pièces jointes) qui contiennent des données personnelles sensibles, est assuré.

Malgré les mesures de sécurité, il n'est pas exclu que des employé-e-s reçoivent des e-mails infectés. Il est de la responsabilité de l'utilisateur ou de l'utilisatrice de ne pas ouvrir les e-mails manifestement douteux, ainsi que leurs liens et pièces jointes.

Le système de messagerie est uniquement destiné à des fins professionnelles.

Les employé-e-s ne doivent pas transférer les e-mails vers leur adresse privée ou vers d'autres adresses e-mail externes qu'ils contrôlent.

En cas d'absence supérieure à un jour, les employé-e-s doivent configurer une réponse automatique indiquant leur absence, ainsi que les coordonnées de leur remplaçant-e.

L'ensemble des e-mails ainsi que leur contenu qui se trouvent dans le système de messagerie de la commune, sont considérés comme professionnels et appartiennent à la commune.

Avant de quitter la Commune, l’employé-e doit remettre les affaires en cours de traitement ou qui sont en suspens ainsi que les e-mails. Les courriels électroniques à contenu personnel, par exemple avec des collègues de travail, doivent être supprimés. Au plus tard le dernier jour de travail, le compte e-mail de l’employé-e quittant le service sera bloqué. Les expéditeurs qui envoient des e-mails à l'adresse e-mail bloquée seront automatiquement informés que l'adresse du destinataire n'est plus valide.

Art. 22 Télétravail

Le télétravail est soumis à autorisation.

L’accès à distance aux ressources informatiques en dehors du bureau ou du réseau de la commune nécessite l’autorisation préalable du ou de la supérieur-e hiérarchique. Cela vaut également pour le home-office ou le télétravail.

Pour l'accès à distance, il faut en principe utiliser les ordinateurs ou les téléphones portables fournis par la commune.

Si l'utilisation de téléphones portables privés est autorisée, une solution de sécurité appropriée (conteneur) doit être installée sur les appareils mobiles privés avec le consentement de la personneconcernée. Cette solution doit être configurée de manière à ce que les données professionnelles (e-mails, documents, images, etc.) ne soient traitées que dans ce conteneur.

Dans le cadre du télétravail, les données personnelles ne peuvent être stockées que sur les supports de stockage autorisés et contrôlés par le service informatique de la commune.

Les mesures de sécurité et de comportement décrites dans le présent règlement s'appliquent également au home-office ou au télétravail, y compris la notification des violations de la sécurité et les procédures correspondantes.

Art. 23 Contrôle des activités et violation du présent règlement

La gestion et la sécurité des systèmes d'information font l'objet d'une surveillance régulière. Cette surveillance est en principe anonyme et non ciblée.

En cas de soupçon de violation du règlement, des investigations approfondies peuvent être menées avec l'accord du/de la supérieur-e ou du/de la responsable de la sécurité de l'information de la commune. Les informations ainsi obtenues sont transmises dans leur intégralité au/à la supérieur-e hiérarchique, qui met en œuvre les mesures appropriées.

En cas de violations (volontaires ou par négligence) du présent règlement, les sanctions pénales ou disciplinaires prévues par la législation supérieure ou communale sont réservées.

**3 Formation et sensibilisation**

Art. 24 Objectif

Afin de garantir la compréhension et le respect des règles de protection des données et de sécurité de l’information, la commune met en place un programme de formation et de sensibilisation. La participation à la formation continue et à la sensibilisation est obligatoire pour l’ensemble du personnel communal et les élu-e-s.

Il appartient au Conseil communal de convenir avec les mandataires externes des obligations y relatives si cela s’avère nécessaire.

**4 Dispositions finales**

Art. 25 Modification du règlement

La sécurité des systèmes d'information est un enjeu permanent et évolutif.

Ce règlement sera régulièrement mis à jour en fonction des changements technologiques et organisationnels.

Art. 26 Entrée en vigueur

Le présent règlement entre en vigueur dès son adoption par l’assemblée communale/par le conseil général, sous réserve de son approbation par la Direction des institutions, de l’agriculture et des forêts.

07.01.2025 – v2.6