

COMMUNE D'ATTALENS

Directives sur la protection des données

Le Conseil communal,

Edicte :

Table des matières

1.	Principes de base	3
Art. 1.1	Objectif	3
Art. 1.2	Champ d'application	3
Art. 1.3	Définitions	3
2.	Principe de base	3
3.	Bases légales	3
4.	Portée du traitement des données	4
5.	Objectifs de protection des données	4
5.1	Protection de la personnalité	4
5.2	Garantie de la sécurité des données	5
6.	Confidentialité	5
7.	Systèmes d'information et de communication SIC	5
8.	Traitement des données personnelles	5
8.1	Propriétaire des données	5
9.	Mesures techniques et organisationnelles	6
9.1	Communication et transfert de données	6
9.2	Traitement des données à l'étranger	6
9.3	Politique de bureau propre (clear desk policy)	6
9.4	Cryptage	6
9.5	Classification des données	6
9.6	Procédure de connexion et authentification	7
9.7	Mots de passe	7
9.8	Destruction de dossiers et de supports de données	7
9.9	Sécurité physique	8
9.10	Postes de travail informatiques	8
9.11	Stockage des données	8
9.12	Violation de la sécurité des données personnelles	8
9.13	Formation et sensibilisation	8
9.14	Utilisation d'Internet	9
9.15	E-mails	9
9.16	Télétravail	10
10.	Contrôle des activités et violation des présentes directives/instructions	10
11.	Droits des personnes concernées	10
12.	Dispositions finales	10

1. Principes de base

Art. 1.1 Objectif

Le présent document définit les directives/instructions relatives à la protection des données et à la sécurité de l'information que le personnel communal doit respecter dans le cadre de l'accomplissement de ses tâches au sein de la commune.

Ces directives/instructions sur la protection des données et la sécurité de l'information édictées par le conseil communal ont pour but de donner aux employé-e-s des lignes directrices pour un traitement des données personnelles conforme à la loi.

Les objectifs principaux de cette directive sont les suivants :

- garantir la protection des données et le respect du secret de fonction ;
- assurer la confidentialité, l'intégrité et la disponibilité de l'infrastructure SIC ;
- garantir une utilisation de l'infrastructure informatique conforme.

Art. 1.2 Champ d'application

Ces lignes directrices s'adressent au personnel communal. Elles servent de recommandations aux contractants externes dans le cadre de la délégation contractuelle de tâches.

Art. 1.3 Définitions

- données : toutes les informations et tous les contenus traités par la commune
- données personnelles : toutes les informations se rapportant à une personne identifiée ou données personnelles : toutes les informations se rapportant à une personne identifiée ou identifiable (voir <https://www.fr.ch/etat-et-droit/gouvernement-et-administration/informations-importantes-sur-la-protection-des-donnees>) ;
- données personnelles sensibles : catégories de données bénéficiant d'une protection renforcée en vertu de la loi, dont la liste exhaustive est établie à l'article 4 alinéa 1 lettre c LPrD (voir <https://www.fr.ch/etat-et-droit/gouvernement-et-administration/informations-importantes-sur-la-protection-des-donnees>) ;
- infrastructure SIC : l'ensemble des installations, appareils, équipements et services de la commune utilisés pour le traitement électronique des données, y compris les données elles-mêmes ;
- traitement : toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés – notamment la collecte, l'enregistrement, la conservation, l'exploitation, la modification, la communication, l'interconnexion, l'externalisation, l'effacement, l'archivage ou la destruction.

2. Principe de base

Le personnel communal s'engage à traiter avec diligence les informations et les données personnelles traitées dans la commune.

3. Bases légales

La commune est responsable de la protection des données personnelles qu'elle traite ou fait traiter.

Les données personnelles doivent être traitées conformément au droit cantonal, notamment :

- la Loi cantonale 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 ; RSF 17.15) ;
- la Loi cantonale du 7 décembre 2010 sur la vidéosurveillance (LVid, RSF 17.3) ;

- l'Ordonnance cantonale du 23 août 2011 sur la vidéosurveillance (OVid ; RSF 17.31) ;
- la Législation spéciale, notamment la loi cantonale du 25 septembre 1980 sur les communes (LCo ; RSF 140.1) ;
- la Loi cantonale du 23 mai 1986 sur le contrôle des habitants (LCH ; RSF 114.21.1).

En outre, la Loi fédérale révisée sur la protection des données du 25 septembre 2020 (LPD ; RS 235.1) et l'Ordonnance du 31 août 2022 sur la protection des données (OPDo ; RS 235.11) s'appliquent aux éventuels prestataires de services externes.

La commune ou les personnes responsables de l'externalisation du traitement des données veillent à ce que les prestataires de services externes s'engagent à traiter les données conformément aux dispositions relatives à la protection des données, notamment les articles 18 ss LPrD. Cela comprend notamment la conclusion de contrats, la sélection soignée des sous-traitants, l'inclusion dans le contrat de clauses de confidentialité, ainsi que la surveillance des sous-traitants (p. ex. contrôle d'accès, octroi contractuel d'un droit de contrôle et d'audit, etc.).

4. Portée du traitement des données

L'employé-e ne peut traiter que les données personnelles nécessaires à l'accomplissement de ses tâches légales, de manière durable, sécurisée et fiable.

La commune déclare ses différentes activités de traitement dans le registre des activités de traitement de l'ATPrDM. Celui-ci peut être consulté sous la rubrique [Registre de traitement | Etat de Fribourg](#) du site Internet de l'ATPrDM.

5. Objectifs de protection des données

5.1 Protection de la personnalité

L'objectif principal de la protection des données est de protéger la personnalité et les droits fondamentaux des personnes dont les données font l'objet d'un traitement.

Le traitement doit se conformer strictement aux dispositions légales ou, le cas échéant, au consentement de la personne concernée. Il en découle les conséquences suivantes :

- Les employé-e-s connaissent les règles de protection des données applicables à leur domaine d'activité ; si ce n'est pas le cas, il convient de se renseigner auprès du ou de la supérieur-e hiérarchique.
- Le traitement des données personnelles est restrictif et ne comprend que les données personnelles nécessaires à l'accomplissement des tâches (principes d'économie de données et de proportionnalité).
- Chaque employé-e n'a accès aux données que dans la mesure où cela est nécessaire à l'accomplissement de ses tâches (contrôle de l'accès et de l'utilisation).
- Le traitement est contrôlable et transparent à tout moment.
- Les droits des personnes dont les données personnelles sont traitées doivent être garantis (droit d'accès, de rectification, d'effacement, de restitution des données, de blocage des données pour les renseignements à des personnes privées) ; en cas de doute, il convient de se renseigner auprès du ou de la supérieur-e hiérarchique/ou le ou la secrétaire communale.
- La communication de données à des fins commerciales est strictement interdite.

5.2 Garantie de la sécurité des données

La commune prend les mesures techniques et organisationnelles nécessaires pour garantir la sécurité des données et de son infrastructure TIC.

Les employé-e-s sont régulièrement informé-e-s des mesures techniques et organisationnelles visant à assurer la sécurité des données et sont formé-e-s en conséquence (cf. également le point 9.9 ci-après).

6. Confidentialité

Le personnel communal est soumis au secret de fonction. Il est tenu de garantir la confidentialité des données personnelles tout au long du cycle de vie du traitement des données (collecte, conservation, utilisation, transformation, communication, enregistrement, archivage ou destruction). Cette obligation subsiste même après la fin des rapports de travail.

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

7. Systèmes d'information et de communication SIC

Le système d'information et de communication (SIC) de la commune comprend 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 systèmes.

Un SIC est principalement composé de ces éléments :

- Des technologies de l'information (TI) : elles comprennent tous les appareils techniques et les applications de traitement de l'information, tels que les ordinateurs, les serveurs, les logiciels et les bases de données.
- Des technologies de la communication : elles comprennent toutes les technologies et tous les réseaux qui permettent l'échange d'informations, comme l'Internet, la téléphonie et d'autres réseaux de télécommunications.
- D'une organisation : les règles, processus et structures qui garantissent que les informations sont traitées et échangées de manière sûre, efficace et efficiente.

Le 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.

8. Traitement des données personnelles

Les informations et les données personnelles doivent être traitées conformément aux exigences légales. Le traitement des données personnelles et des données sensibles repose sur les objectifs de sécurité suivants : confidentialité, intégrité, disponibilité et traçabilité.

8.1 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 pour garantir les objectifs de sécurité.

9. Mesures techniques et organisationnelles

9.1 Communication et transfert 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 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 l'étranger que si la personne responsable a vérifié que les conditions légales prévues aux articles 14 et suivants de la LPrD.

9.2 Traitement des données à l'étranger

Les données personnelles ne peuvent être traitées qu'en Suisse ou dans un Etat garantissant un niveau de protection adéquat. Il existe une liste exhaustive de ces Etats (cf. 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).

Les données personnelles ne peuvent être transmises 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.

9.3 Politique de bureau propre (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 à la fin du travail ou en cas d'absence de courte durée.
- 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.

9.4 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 de traitement, met à disposition l'infrastructure nécessaire à cette fin.

9.5 Classification des données

Conformément à l'article 9 RSD, tout document physique ou électronique doit être classé selon les catégories suivantes :

- accessible au public (1^{er} degré) ;
- pour usage interne (2^e degré) ou
- confidentiel ou secret (3^e degré).

9.6 Procédure de connexion et authentification

Connexion au système : les employés s'authentifient au système avec leurs données de connexion personnelles, qui doivent être traitées de manière confidentielle.

Le système utilise ces informations pour vérifier si les utilisateurs disposent d'une autorisation d'accès et, en cas de contrôle positif, autorise l'utilisateur conformément à son rôle et à ses autorisations.

Grâce à l'authentification, la commune s'assure que seules les personnes, services et apps autorisés et disposant des droits correspondants peuvent accéder aux ressources communales.

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

Pour renforcer la sécurité, une troisième information (empreinte digitale, badge, SMS) peut être demandée.

La perte des données de connexion susmentionnées doit être immédiatement signalée au responsable de la sécurité et/ou au supérieur hiérarchique.

9.7 Mots de passe

Le nom d'utilisateur et le mot de passe personnel sont utilisés pour l'identification des utilisateurs par l'infrastructure SIC (voir 9.6). 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 ces conditions :

- Il doit comporter au moins 12 caractères et être suffisamment complexe incluant 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.
- Le mot de passe personnel doit être modifié à intervalles réguliers.
- 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.

Pour plus d'informations, voir la fiche d'information de l'ATPrDM sur la communication par 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 »).

9.8 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.

9.9 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, etc.

L'accès de tierces personnes, comme 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.

9.10 Postes de travail informatiques

La configuration des postes de travail informatiques de la commune ne doit pas être modifiée par les utilisateurs. Seuls les logiciels achetés et installés par la commune peuvent être utilisés. Sont notamment interdits, mais pas exclusivement, les opérations suivantes :

- toute installation arbitraire de logiciels par les utilisateurs ;
- toute utilisation de logiciels sans licence ;
- la désinstallation ou la modification des logiciels 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.

9.11 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, etc.). 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.

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.

9.12 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, etc.), l'employé doit immédiatement en informer son ou sa supérieur-e hiérarchique et/ou le 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>

9.13 Formation et sensibilisation

La commune forme régulièrement son personnel à la protection des données et à la sécurité de l'information et attire son attention sur les programmes. La participation à la formation continue et à la sensibilisation est obligatoire pour l'ensemble du personnel communal. Le conseil communal ou la personne chargée de cette tâche détermine la fréquence et la durée de la formation continue.

Les frais de formation continue correspondants sont pris en charge par la commune.

9.14 Utilisation d'Internet

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

Une utilisation occasionnelle à des fins privées est tolérée.

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.

9.15 E-mails

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, selon 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 (avec 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 de l'entreprise 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.

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.

En cas de départ, l'employé-e doit remettre à la commune les affaires en cours ainsi que les e-mails y afférents.

Avant de quitter l'entreprise, l'employé-e doit remettre les affaires en cours de traitement ou qui sont en suspens. Les e-mails 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 l'entreprise 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.

9.16 Télétravail

L'accès aux ressources informatiques en dehors du bureau ou du réseau de la commune requiert l'accord préalable du/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 des personnes concernées. 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.

10. Contrôle des activités et violation des présentes directives/instructions

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 des règles, 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 et traite les informations conformément à la protection des données.

11. Droits des personnes concernées

Les droits des personnes concernées par le traitement doivent être respectés (art. 27 ss LPrD).

Les demandes concernant leurs données doivent être transmises au/à la secrétaire communal-e compétent-e, le cas échéant à la personne qu'il/elle a désignée (cf. organisation interne).

12. Dispositions finales

La sécurité des systèmes d'information est une évolution soutenue et en constante progression.

Ces lignes directrices sont régulièrement adaptées aux évolutions techniques et organisationnelles.

Les directives ont été adoptées et entrent en vigueur le 1^{er} janvier 2026.

Adopté par le Conseil communal dans sa séance du 15 décembre 2025.


Laurent Menoud
Syndic




Serge Praz
Administrateur communal