

Commune Attalens

Formation du 13 janvier 2026

- **Protection et sécurité des données**
- **Cyberattaques**
- **IA**

Programme

- **Formation** initiale à la protection des données et à la sécurité des données
 - Information sur la **directive sur la protection des données**
 - **Accord de confidentialité** type à signer par l'employé-e
 - Rappel de la procédure à appliquer en cas de **cyberattaque** ou violation des données
 - Utilisation de l'**intelligence artificielle**
- 

Formation initiale à la protection des données et à la sécurité des données

L'autorité cantonale de la transparence, de la protection des données et de la médiation a publié une [brochure](#) de formation à la protection des données.

Brochure de formation initiale à la protection des données et à la sécurité des données

acf-fgv

association des communes fribourgeoises
freiburger gemeindeverband



ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence, de la protection des données
et de la médiation ATP+DM

Kantonale Behörde für Öffentlichkeit, Datenschutz
und Mediation ÖDSMB

03 Principes de la sécurité des données



Confidentialité

Assurez-vous que les informations ne sont accessibles
qu'aux personnes autorisées.



Intégrité

Veillez à ce que les informations soient exactes
et complètes.



Disponibilité

Garantissez que les informations soient disponibles
lorsqu'elles sont nécessaires.

04 Obligations et responsabilités



Employé-e-s et mandataires externes

Respecter les politiques et procédures de sécurité des données.

Utiliser des mots de passe robustes et sécurisés.

Signaler tout incident ou anomalie (violation de la sécurité des données).

Ne pas divulguer des informations à des personnes ou organisations non autorisées. Vous êtes liés au **secret de fonction** respectivement au **secret professionnel** pour les mandataires externes.



Elu-e-s communaux-ales

Appliquer les mêmes règles de confidentialité que les employé-e-s.

Suivre les dispositions spécifiques de la législation sur les communes.



Responsables de la sécurité des données

Assurer la mise en œuvre des politiques de sécurité des données.

Former et sensibiliser les employé-e-s et les élu-e-s.

Répondre aux incidents de sécurité (violation de la sécurité des données).

05 Bonnes pratiques quotidiennes



Gestion des accès

Utilisez des mots de passe complexes.

Ne partagez pas vos identifiants.

Utilisez l'authentification multi-facteurs.



Sécurité physique

Verrouillez votre poste de travail en cas d'absence.

Sécurisez les documents sensibles.



Utilisation des outils de travail

Utilisez uniquement les logiciels et équipements autorisés.

Évitez d'utiliser des dispositifs personnels pour des tâches professionnelles sans autorisation.

06 Gestion des incidents (violation de la sécurité des données)



Détection d'un incident

Soyez vigilant aux comportements inhabituels du système et aux emails suspects.

Signalez immédiatement tout incident.



Procédure de signalement

Informez le service informatique ou le responsable de la sécurité, ainsi que cas échéant, la préposée à la transparence et à la protection des données.



Réponse aux incidents

Prenez des mesures immédiates pour limiter les dommages.

Collaborez avec le service informatique pour résoudre le problème.

8. Conclusion



Nous vous remercions de votre engagement à suivre ces directives et à protéger les données et la sécurité des données. Votre rôle est crucial pour assurer la sécurité et la confidentialité des informations sensibles.

Pour toute question ou demande d'information supplémentaire, n'hésitez pas à contacter le service informatique ou les responsables de la sécurité des données.

Note : Cette brochure fait partie intégrante de votre formation initiale. Veuillez lire attentivement chaque section et suivre les directives énoncées pour garantir la protection des données et la sécurité des données au sein de la commune.

Information sur la directive sur la protection des données

Le Conseil communal a validé la mise en place de la [Directive sur la protection des données](#), la formation et convention pour le personnel.

COMMUNE D'ATTALENS

Directives sur la protection des données

Le Conseil communal,

Edicte :

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 sous-traitants 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 antispham. 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

Accord de confidentialité à signer par l'employé-e

Le Conseil communal a validé la mise en place de la Directive sur la protection des données, la formation et convention pour le personnel.

A retourner signé à RH → 20 janvier 2026

Accord de confidentialité – convention

Dans le cadre de son activité, le ou la collaboratrice-trice peut être amené-e à accéder aux informations confidentielles et données personnelles traitées par l'employeur, en plus des informations couvertes par le secret de fonction au sens de l'article 320 du Code pénal suisse du 21 décembre 1937 (CP ; RS 311.0).

Définitions :

1. Les **informations confidentielles** sont toutes les informations y compris les données personnelles qui sont soumises au secret de fonction et qui ne peuvent pas être divulguées à des tiers non autorisés, sous réserve de base légale ou une autre instruction.
2. On entend par **données personnelles** toutes les informations se rapportant à une personne identifiée ou identifiable (art. 4 al. 1 let. a de la Loi cantonale sur la protection des données du 12 octobre 2023, LPrD ; RSF 17.1).
3. Les **données personnelles sensibles** sont les données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales, les données sur la santé, la sphère intime ou l'origine raciale ou ethnique, les données génétiques et biométriques identifiant une personne physique de manière univoque, les données sur des mesures d'aide sociale, des poursuites ou les données sur les sanctions pénales et administratives (art. 4 al. 1 let. c LPrD).

La communication de ces données est soumise aux termes et conditions ci-après :

- Respecter les conditions de protection des données et à garder le secret sur les informations dont il-elle aura connaissance et à ne dévoiler aucune information dont il-elle aura connaissance dans l'exercice de ses fonctions.
- Traiter les données personnelles uniquement aux fins prévues pour l'accomplissement de ses tâches professionnelles, à ne pas les réutiliser et à ne les transmettre ou à n'en faire un quelconque autre usage.
- Ne pas consulter les systèmes d'informations à sa disposition à des fins autres que celles relatives à l'accomplissement de ses tâches professionnelles, y compris médias et réseaux sociaux.
- Ne faire état d'aucun nom, dossier ou affaire dont il-elle aurait eu connaissance dans le cadre de son travail.
- N'effectuer aucune copie et photo des données auxquelles il-elle aura accès et de ne pas les prélever ou les télécharger.

Par la présente, le ou la collaboratrice-trice confirme avoir pris connaissance des obligations susmentionnées, des directives sur la protection des données et s'engage à les respecter.

CONSEIL COMMUNAL D'ATTALENS


Laurent Menoud
Syndic


Serge Praz
Administrateur communal

Lu et accepté par l'employé-e

Nom et prénom : _____

Date et signature : _____

Rappel de la procédure à appliquer en cas de cyberattaque ou violation des données

Comme déjà communiqué à fin 2023, une procédure a été rédigée pour réagir correctement à des événements inattendus et assurer la continuité des opérations communales.

Ce document s'adresse à tout le personnel utilisant l'infrastructure informatique de la Commune d'Attalens.

Version du 02.12.2025 dans [Youdoc\0 AdminGen\022 SecGen\0220 SecGen\0220.04 IT\03 PrestatLogiciels\Divers](#)

Procédure en cas de cyberattaque ou violation de la sécurité des données pour l'administration communale d'Attalens

Cette procédure a pour but de réagir correctement à des événements inattendus et assurer la continuité des opérations communales.

Ce document s'adresse à tout le personnel utilisant l'infrastructure informatique de la Commune d'Attalens.

Version du 02.12.2025

Doc sous [Youdoc\0_AdminGen\022_SecGen\0220_SecGen\0220.04_IT\03_PrestatLogiciels\Divers](#)

Etapes et actions	Qui
1. Identification de l'incident	
Si détection ou soupçon d'une cyberattaque ou de violation de la sécurité des données, informer immédiatement l'administrateur communal (021 947 33 75) ou remplaçant (chef du service technique 021 947 55 71) et le prestataire informatique (VG Technologies 021 943 50 50).	impliqué.e
Documenter toutes les observations pertinentes, y compris l'heure exacte, la nature de l'incident et les systèmes potentiellement affectés. Si possible avec des photos ou saisies d'écran.	impliqué.e
2. Isolation de l'incident	
D'entente avec le prestataire informatique, déconnecter les systèmes compromis du réseau pour éviter une propagation ultérieure, éteindre l'ordinateur, retirer la prise réseau de la machine.	impliqué.e + prestataire informatique
Changer les mots de passe pour tous les comptes utilisateurs et administrateurs sur les systèmes affectés.	impliqué.e + prestataire informatique

3. Notification aux parties concernées	
Informer le syndic, le Conseil communal et les autres parties prenantes de la situation.	administrateur communal
Si des données personnelles ou sensibles ont été compromises, informer les autorités compétentes conformément à la réglementation en vigueur (police) et annoncer à l'Autorité cantonale de la transparence, de la protection des données et de la médiation ATPrDM via le formulaire en ligne	administrateur communal
Au besoin, mettre en place une cellule de crise avec le syndic, l'administrateur et le prestataire informatique.	administrateur communal
4. Évaluation et analyse	
Rassembler les journaux et les données pertinentes pour évaluer la nature et l'ampleur de l'incident.	prestataire informatique
Utiliser des outils de diagnostic et de surveillance pour identifier la source et la méthode d'attaque.	prestataire informatique
5. Éradication	
Une fois la source de l'incident identifiée, supprimer tous les éléments nuisibles.	prestataire informatique
S'assurer d'avoir corrigé toutes les vulnérabilités qui ont permis l'attaque.	prestataire informatique
6. Restauration	
Restaurer les systèmes à partir de sauvegardes connues pour être propres et sûres.	prestataire informatique
Mettre à jour et patcher tous les logiciels et systèmes pour prévenir des incidents futurs.	prestataire informatique
7. Communication	
Si nécessaire, préparer un communiqué pour informer le public, les résidents et autres parties prenantes de la situation, des mesures prises et des recommandations pour éviter d'autres incidents.	syndic + administrateur communal
S'assurer de répondre aux questions et préoccupations de manière transparente et ouverte.	syndic + administrateur communal
8. Revue post-incident	
Organiser une réunion avec toutes les parties impliquées pour discuter de l'incident, des mesures prises et des leçons apprises.	administrateur communal

Utilisation de l'intelligence artificielle

Info dans la [News 7/2025](#) - IA- intelligence artificielle

L'intelligence artificielle prend de plus en plus de place dans notre société et jusqu'à nos places de travail. Son utilisation présente des avantages indéniables mais également de très grands risques, notamment pour la sécurité des données.

Obligation de respecter la [directive de l'Etat de Fribourg](#) lors de l'éventuelle utilisation de l'intelligence artificielle générative. Elle prévoit les 7 règles en bref :

- **Ne pas introduire de données sensibles, confidentielles, secrètes ou sous le coup du secret professionnel dans un logiciel d'IA.**
- **Ne pas introduire de données personnelles dans les outils d'IA.**
- **Être conscient de la responsabilité d'utilisation de l'IA : celui ou celle qui y a recours est seul-e responsable de son contenu et de sa conformité aux normes légales.**
- **Retravailler les résultats générés par l'IA et les analyser de manière critique pour éviter les biais et les informations incomplètes ou erronées.**
- **Vérifier les sources des informations.**
- **Indiquer de manière transparente l'utilisation de l'IA (même partielle).**
- **Ne pas porter atteinte à l'image de la Commune d'Attalens**

Intelligence artificielle générative pour les tâches administratives

Directive sur l'utilisation

L'utilisation de l'IA générative dans l'administration cantonale n'en étant qu'à ses débuts, cette directive doit être régulièrement revue au fil du temps et adaptée à la pratique.

Lors de l'utilisation d'outils d'IA générative pour des tâches administratives, il convient de tenir compte des points suivants :

I. Définition

Le terme IA désigne la vaste discipline consistant à développer des logiciels capables de simuler l'intelligence humaine. Plus exactement, l'IA fait référence aux technologies et algorithmes utilisés pour apprendre à des systèmes à exécuter des tâches intellectuelles.

L'intelligence artificielle générative (IA générative) est un sous-domaine de l'intelligence artificielle (AI) qui se concentre sur la création de nouveaux contenus, tels que des images, des textes, des vidéos, de la musique, etc. Le terme « générative » fait référence à la capacité de ces systèmes à générer de nouvelles données qui ressemblent à des données existantes.

II. Objectif et champ d'application

Cette directive offre aux collaborateurs et collaboratrices de l'administration cantonale une orientation pour une utilisation de l'IA de manière sûre et conforme au droit suisse. Elle s'applique aux collaborateurs et collaboratrices de toutes les Directions et établissements de l'Etat de Fribourg, selon le champ d'application de l'ordonnance du Conseil d'Etat sur la gouvernance de la digitalisation et des systèmes d'information de l'Etat, qui utilisent et mettent en œuvre des outils d'IA générative dans le cadre de leur activité professionnelle.

III. Quels outils d'IA générative sont concernés ?

Les outils d'IA générative concernés par la présente directive comprennent toutes les applications qui soutiennent les tâches administratives de recherche et de rédaction. Il s'agit par exemple de générateurs de texte tels que Copilot, de programmes de traduction tels que DeepL ou Microsoft Translator, ou de générateurs d'images tels que DALL-E. Ces outils analysent les entrées faites par les utilisateurs et génèrent sur cette base des sorties telles que des textes, des images ou du code de programme.

IV. Utilisation d'outils d'IA générative

Il n'y a presque pas de limites à l'imagination en matière d'applications de l'IA générative. Les outils d'IA générative peuvent être utilisés de diverses manières comme soutien dans le travail quotidien, notamment pour :

- > rédaction de résumés d'information accessibles au public ;
- > brainstorming sur un thème ;
- > aides à la formulation pour les textes déjà existants, les courriels sans données personnelles ni contenu confidentiel ;
- > traductions ;

- > compilation de séries de diapositives ou de résumés de vidéos disponibles sur Internet (par exemple : conférences de presse sur Youtube).

Il convient notamment de ne pas l'utiliser :

- > dans le cadre du traitement d'un dossier personnel d'un citoyen ou d'une citoyenne ;
- > pour la préparation de décisions juridiquement contraignantes ;
- > dans l'élaboration de documents sur la base d'informations dont la divulgation pourrait porter préjudice à l'Etat.

En règle générale, il faut partir du principe que l'output issu des outils correspondants doit être évalué de manière critique par l'utilisateur ou l'utilisatrice selon le cas d'application et doit être retravaillé.

V. Restrictions et protection des données

Lors de l'utilisation d'outils d'IA, aucune information sensible, confidentielle ou secrète, ni aucune donnée personnelle, y compris pseudonymisée, ne doit être introduite. Même les données anonymisées peuvent, dans certaines circonstances, permettre de tirer des conclusions sur les personnes et doivent donc être analysées et utilisées de manière très restrictive. L'utilisation de l'IA ne doit en aucun cas porter préjudice à l'image de l'Etat.

VI. Exigences légales

L'utilisation d'outils d'IA est soumise à la législation fédérale et cantonale, notamment en ce qui concerne la confidentialité, la sécurité des informations et la protection des données. Celles-ci comprennent notamment (sous une forme non exhaustive) :

- > la protection des données personnelles conformément à la loi sur la protection des données (loi fédérale sur la protection des données LPD, RS 235.1 et loi cantonale sur la protection des données LPrD RSF 17.1) ;
- > le respect du secret de fonction ou du secret professionnel (loi sur le personnel de l'Etat LPers RSF 122.70.1 ;
- > le respect des règles de confidentialité métier spécifiques ;
- > le droit d'auteur et le droit de propriété intellectuelle.

VII. Responsabilité et examen des résultats

Les collaborateurs et collaboratrices sont responsables de la saisie et de l'utilisation des outils d'IA et de leurs résultats, ainsi que de toutes les conséquences juridiques qui en découlent. L'exactitude et l'exhaustivité de tous les résultats générés et les sources doivent être vérifiées de manière critique avant leur utilisation ou leur diffusion (par exemple par le biais du contrôle des 4 yeux). Les résultats éthiquement discutables ou biaisés doivent être identifiés et leur réutilisation évitée. La dignité, l'éthique et l'intérêt public doivent toujours être garantis.

Il convient en outre de noter que deux phénomènes peuvent se produire dans les outils d'IA, qui rendent l'examen des utilisateurs si important, en particulier :

Biais : l'ensemble de données utilisé par le modèle s'inscrit dans un contexte spatial et historique et ne représente pas toujours toute la diversité et neutralité attendues. Un biais est dû à une sur-représentation d'une donnée d'entraînement (données occidentales ou orientales, genre, ethnie, etc.). L'IA étant le reflet des données, cela peut fausser les résultats obtenus à l'aide de l'IA, qui doivent être corrigées par l'utilisateur ou l'utilisatrice. Toute personne doit être protégée contre toute discrimination ou stigmatisation. L'utilisation d'outils d'IA ne saurait aller à l'encontre de ce droit fondamental, et la vérification des résultats doit en tenir compte.

Hallucinations : il s'agit d'un résultat formulé de manière convaincante par une IA, qui ne semble pas être justifié par les données d'entraînement du modèle et qui peut être objectivement faux. De tels résultats doivent être détruits et il faut parvenir à un résultat d'une autre manière.

VIII. Etiquetage et transparence

L'utilisation des outils d'IA doit être transparente. Les résultats qui sont repris sans révision substantielle doivent être signalés en conséquence. Une mention doit indiquer de manière transparente le générateur d'IA utilisé, la version de celui-ci et l'étendue de son utilisation.

Les 7 règles en bref :

1. Ne pas introduire de données sensibles, confidentielles, secrètes ou sous le coup du secret professionnel dans un logiciel d'IA.
2. Ne pas introduire de données personnelles dans les outils d'IA.
3. Etre conscient de la responsabilité d'utilisation de l'IA : celui ou celle qui y a recours est seul-responsable de son contenu et de sa conformité aux normes légales.
4. Retravailler les résultats générés par l'IA et les analyser de manière critique, pour éviter les biais et les informations incomplètes ou erronées.
5. Vérifier les sources des informations.
6. Indiquer de manière transparente l'utilisation de l'IA (même partielle).
7. Ne pas porter atteinte à l'image de l'Etat de Fribourg.

Adopté en séance du Conseil d'Etat le 18 novembre 2024.

Des questions ???



Bon café!

