

ANNEXE DE LA DELIBERATION 2022 27
CHARTRE INFORMATIQUE du SAVM



Rappel des textes législatifs :

- Règlement n°2016/679 du 27 avril 2016, dit « règlement général sur la protection des données » ou « RGPD »
- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi « Informatique et Libertés » ou « LIL », modifiée

SOMMAIRE

Préambule.....	3
1. Système d'information et de communication	4
2. Utilisateurs	4
3. Responsable du système d'information et de communication	4
4. Responsabilité et engagement du SAVM	5
5. Utilisation de l'outil informatique	5
6. Confidentialité des paramètres d'accès	5
7. Règles de sécurité et protection des ressources sous la responsabilité de l'utilisateur	6
8. Règles spécifiques aux utilisateurs en télétravail	7
9. Accès à Internet	7
10. Messagerie électronique	8
11. Accès distant	9
12. Téléphonie	10
13. Départ d'un utilisateur	10
14. Traçabilité	11
15. Protection des données	11
16. Conditions d'administration du système d'information	11
17. Responsabilité et sanctions	12
18. Information des agents	12
19. Évolution de la charte informatique	12
20. Entrée en vigueur de la charte informatique	12

Préambule

Le règlement général de protection des données (RGPD) est un texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union Européenne. Il est entré en application le 25 mai 2018. Il s'inscrit dans la continuité de la loi informatique et liberté établissant des règles sur la collecte et l'utilisation des données sur le territoire français. Il a été conçu autour de 3 objectifs :

- **renforcer les droits des personnes ;**
- **responsabiliser les acteurs traitant des données ;**
- **crédibiliser la régulation** grâce à une coopération renforcée entre les autorités de protection des données.

Le Syndicat met en œuvre un système d'information et de communication nécessaire à l'exercice de ses compétences, comprenant notamment un réseau informatique et téléphonique.

Les agents, dans le cadre de leurs missions, sont conduits à accéder aux outils informatiques et aux moyens de communications mis à leur disposition et à les utiliser.

Cette charte est avant tout un code de bonne conduite et intègre la mise en place du Règlement Général de Protection des Données « RGPD ».

Elle définit les conditions d'accès et les règles d'utilisation des moyens informatiques et des outils de communication du Syndicat Autolib' Velib' Métropole (SAVM).

L'objet de cette charte est de préciser la responsabilité des utilisateurs, en conformité avec la législation, afin d'instaurer un bon usage des ressources informatiques et des services Internet, quel que soit le lieu de travail, y compris en télétravail.

L'enjeu de cette charte est donc de renforcer le niveau d'information et améliorer le comportement de chaque utilisateur dans le but de :

- Respecter les contraintes réglementaires (CNIL, Référentiel Général de Sécurité...),
- Protéger le système d'information du Syndicat contre les menaces qui évoluent sans cesse,
- Informer les utilisateurs, tant sur le plan du bon usage des ressources informatiques et de communication, que sur le plan de la protection des données qu'ils sont amenés à manipuler.

Pour être toujours à jour, cette charte sera régulièrement réactualisée en fonction des évolutions du système d'information, de la réglementation, pour faire face aux nouvelles menaces, mais aussi pour s'adapter à la politique de sécurité du Syndicat.

Le non-respect des obligations imposées par la présente charte peut conduire l'utilisateur à se voir sanctionné, conformément à la réglementation en vigueur.

1. Système d'information et de communication

La présente charte s'applique en cas d'utilisation du système d'information et de communication du Syndicat Autolib' Velib' Métropole (SAVM). Le système d'information et de communication est notamment constitué des éléments suivants :

- ◆ Le poste de travail (PC, Mac, écran),
- ◆ Les appareils raccordés au poste de travail (imprimante, scanner, vidéoprojecteur...),
- ◆ Les équipements réseau (connectique, réseaux sans fil, vidéoprojecteur...),
- ◆ Les appareils partagés (imprimante réseau, copieurs...),
- ◆ Les appareils mobiles (PC portables, Smartphones, ...),
- ◆ La messagerie unifiée (messages écrits ou vocaux, calendrier, tâches, contacts),
- ◆ Les outils du web (site Internet...),
- ◆ Le téléphone (fixe et mobile),
- ◆ Les réseaux sociaux.

Pour des raisons de sécurité du réseau, le matériel personnel des agents connecté au réseau du SAVM, ou contenant des informations à caractère professionnel est également considéré comme faisant partie du système d'information et de communication.

2. Utilisateurs

Sauf mention contraire, la présente charte s'applique à l'ensemble des utilisateurs du système d'information et de communication du SAVM, quel que soit leur statut, qu'ils soient agents du SAVM, membres des collectivités, ou encore salariés d'une société sous-traitante. Les règles énoncées par la présente charte sont également applicables aux utilisateurs occasionnels tels que les invités ou les visiteurs.

Les agents veillent à faire respecter les règles posées par la présente charte à toute personne à laquelle ils permettraient d'accéder au système d'information et de communication.

3. Responsable du système d'information et de communication

Le Président est responsable du contrôle du bon fonctionnement du système d'information et de communication. Il veille à l'application des règles de la présente charte. Il est assisté par le prestataire informatique désigné (cf annexe 1). Le prestataire du système d'information et de communication est assujéti à une obligation de confidentialité sur les informations qu'il est amené à connaître.

4. Responsabilité et engagement du SAVM

Le SAVM porte à la connaissance de l'utilisateur la présente charte. Il doit mettre en œuvre les mesures pour assurer la sécurité du système d'information et la protection des utilisateurs.

Le SAVM facilite l'accès des utilisateurs aux ressources du système d'information. Les ressources mises à leur disposition sont à usage professionnel mais le Syndicat est tenu de respecter la vie privée de chacun.

Un délégué à la Protection des Données (« Data Protection Officer » ou « DPO » en anglais) externalisé a été désigné par le SAVM (cf annexe 1). L'utilisateur pourra s'adresser à la Direction de l'Administration Générale (DAG) pour tout complément d'information sur l'application de la Charte informatique.

L'utilisateur est responsable, en toutes circonstances, de l'usage qu'il fait du système d'information auquel il a accès.

L'arrêté de recrutement et le contrat de travail devront prévoir expressément l'obligation de respect de la charte.

L'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat. Il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède.

Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie. Le non-respect de ses obligations ou tout abus dans l'utilisation des ressources mises à sa disposition engage la responsabilité de l'utilisateur et peut donner lieu à des procédures disciplinaires ou des poursuites pénales.

Sans préjuger des poursuites ou procédures engagées, le SAVM peut limiter, par mesure conservatoire, l'usage du système d'information pour l'utilisateur concerné.

5. Utilisation de l'outil informatique

L'utilisation des outils informatiques et des moyens d'information et de communication mis à la disposition des agents doit être exclusivement professionnelle, sauf autorisation préalable de la Direction.

Si une telle autorisation devait être accordée, l'usage personnel qui en résulterait devrait être occasionnel et raisonnable, tant dans la fréquence que dans la durée, conforme à la législation en vigueur et ne pas porter atteinte à la sécurité et à l'intégrité du système d'information, des données professionnelles ou à caractère personnel traitées au sein du SAVM, ou encore à l'image du SAVM, et plus largement à celle de la fonction publique.

6. Confidentialité des paramètres d'accès

L'accès aux sessions des appareils informatiques, ainsi que ceux des logiciels et applications sont protégés par des paramètres de connexion requérant un identifiant et un mot de passe. Ces paramètres sont personnels à l'utilisateur et doivent être gardés confidentiels.

Ces éléments doivent être mémorisés par l'utilisateur et ne pas être conservés, sous quelque forme que ce soit. Ils ne doivent pas être transmis à des tiers ou être aisément accessibles. Ils doivent être saisis par l'utilisateur à chaque accès et ne pas être conservés en mémoire dans le système d'information.

Lorsqu'ils sont choisis par l'utilisateur, les mots de passe doivent respecter un certain degré de complexité, conformément aux recommandations de l'ANSSI, et être modifiés régulièrement.

L'utilisateur est responsable de son compte et de son mot de passe, et de l'usage qu'il en fait. Il ne doit pas masquer son identité sur le réseau local ou usurper l'identité d'autrui en s'appropriant le mot de passe d'un autre.

7. Règles de sécurité et protection des ressources sous la responsabilité de l'utilisateur

L'utilisateur est chargé de signaler au responsable du système d'information et de communication toute violation ou tentative de violation suspectée de son compte informatique et, de manière générale, tout dysfonctionnement.

Il est responsable quant à lui des ressources qui lui sont confiées dans le cadre de l'exercice de ses fonctions. Il doit concourir à la protection des dites ressources, en faisant preuve de prudence.

En cas d'absence, même temporaire, il est impératif que l'utilisateur verrouille l'accès au matériel qui lui est confié ou à son propre matériel, dès lors que celui-ci contient des informations à caractère professionnel. Il appartient à l'utilisateur de veiller à la sécurité du matériel utilisé et à son innocuité.

L'utilisateur doit effectuer des sauvegardes régulières des fichiers dont il dispose sur le matériel mis à sa disposition.

L'utilisateur **s'engage à respecter les règles de sécurité suivantes :**

- Ne jamais confier son mot de passe,
- Ne pas masquer sa véritable identité (tout utilisateur doit être identifiable),
- Ne pas usurper l'identité d'autrui,
- Retenir son mot de passe, ne pas l'écrire en clair, ni sur papier, ni dans un fichier,
- Ne jamais demander son identifiant ni son mot de passe à un collègue ou à un collaborateur,
- Verrouiller son ordinateur dès que l'on quitte son poste de travail,
- Signaler à la DAG toute violation ou tentative de violation suspectée de son compte réseau,
- Signaler à la DAG, d'une manière générale, tout dysfonctionnement constaté sur les logiciels et équipements faisant partie du système d'information,
- Respecter l'intégrité et la confidentialité des données confiées et gérées dans le cadre de ses missions,
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des données sans autorisation ou habilitation des personnes responsables de ces données,
- Toute copie de données sur un support externe est soumise à l'accord du supérieur hiérarchique et doit respecter les règles définies dans la présente charte,
- Ne pas installer de logiciels ou de module complémentaire sur les navigateurs sans autorisation de la DAG,
- Ne pas télécharger ou copier de contenu illicite sur son poste de travail,
- Ne pas connecter d'équipement personnel sans prendre l'attache de la DAG.

Les intervenants extérieurs doivent s'engager à faire respecter la présente charte par leurs propres salariés et éventuelles entreprises sous-traitantes, ce qui implique que les marchés publics, contrats ou conventions signés entre le SAVM et tout tiers ayant accès aux données, aux programmes informatiques ou autres moyens, doivent comporter une clause rappelant cette obligation.

Chaque utilisateur accède aux outils informatiques nécessaires à l'exercice de son activité professionnelle dans les conditions définies ci-après par le SAVM.

Il doit en toutes circonstances veiller au respect de la législation, qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, les données personnelles, les systèmes de traitement automatisé de données, le droit à l'image des personnes, l'exposition des mineurs aux contenus préjudiciables.

A l'exception des ordinateurs portables mis à la disposition des agents, et des téléphones portables aucun matériel ni logiciel informatique appartenant au SAVM ne peut en être sorti sans autorisation préalable de la Direction.

8. Règles spécifiques aux utilisateurs en télétravail

On entend par « équipements nomades » tous les moyens techniques mobiles (ordinateur portable, téléphones mobiles ou smartphones, clé USB, etc.) que le SAVM met à la disposition des utilisateurs nomades (contrôleurs) ou en télétravail.

Quand cela est techniquement possible, ils doivent faire l'objet d'une sécurisation spécifique, au regard de la sensibilité des documents qu'ils peuvent stocker, notamment par le chiffrement du contenu.

L'utilisation de tout équipement nomade, même limitée à quelques fonctions (messagerie, navigation Internet, consultation de documents, stockage de données), comporte des risques particuliers pour la confidentialité des informations professionnelles, notamment en cas de perte ou de vol de ces équipements. Quand ces appareils ne sont pas utilisés pendant quelques minutes, ils doivent donc être verrouillés automatiquement par un moyen adapté (code chiffré ou modèle graphique) en plus du code PIN, de manière à prévenir tout accès non autorisé aux données qu'ils contiennent. L'utilisateur en assure la garde et la responsabilité.

Il doit informer la DAG en cas d'incident (perte, vol, dégradation), et fournir à la direction de l'Administration Générale et des RH les informations nécessaires à la déclaration de vol ou au dépôt de plainte.

9. Accès à Internet

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à Internet. Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé par le responsable du système d'information et de communication. Celui-ci est habilité à imposer des configurations du navigateur et à restreindre le téléchargement de certains fichiers.

L'utilisateur est informé que les traces de la navigation sont temporairement archivées. En effet, à la demande d'une autorité judiciaire ou administrative, l'administrateur du proxy devra fournir les informations de la navigation web.

Le Syndicat se réserve le droit :

- de contrôler le contenu de toute page Web hébergée sur ses serveurs en vue de s'assurer du respect des conditions d'utilisation des services énoncées par la présente Charte.
- de suspendre l'usage du service d'hébergement des pages Web par un utilisateur en cas de non-respect de la Charte et notamment dans l'hypothèse où l'utilisateur aurait diffusé sur ses pages Web un contenu manifestement illicite.

L'utilisateur s'engage à respecter les règles suivantes :

- Interdiction de consulter ou télécharger du contenu de sites web à caractère pornographique, pédophile ou tout autre site illicite ou contraire aux bonnes mœurs.
- Interdiction de télécharger des fichiers musicaux ou vidéo, sauf obligation professionnelle.
- Pour participer à des forums, l'utilisateur doit disposer d'autorisations internes afin de s'exprimer au nom du Syndicat.
- Les téléchargements de contenu illicite sont interdits (contrefaçon de marque, copie de logiciels commerciaux, etc.).
- Une utilisation ponctuelle et raisonnable pour un motif personnel est admise. Elle ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.
- Le contenu des sites consultés ne doit pas être contraire à la loi, de nature à troubler l'ordre public ou bien encore mettre en cause l'intérêt ou la réputation du SAVM.
- L'usage des réseaux sociaux et des messageries personnelles est soumis aux mêmes règles de tolérance. Les options de maintien de la connexion et tout autre dispositif permettant une connexion permanente sont interdits, sauf pour un usage strictement professionnel.
- Chaque utilisateur doit être attentif aux risques de manquement à son obligation de réserve et de discrétion professionnelle lorsqu'il diffuse des messages sur un réseau social.

10. Messagerie électronique

Chaque agent dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique attribuée par la DAG.

Les messages électroniques reçus font l'objet d'un contrôle antivirus et d'un filtrage des courriels indésirables. Les agents sont invités à signaler tout dysfonctionnement constaté dans le dispositif de filtrage.

Les messages électroniques sont conservés pendant une durée de 5 ans. Passé ce délai, ils sont systématiquement supprimés, sauf disposition légale ou réglementaire contraire.

L'envoi de messages électroniques obéit aux mêmes règles que l'envoi de correspondances postales. Les messages électroniques ont la même portée qu'un courrier manuscrit et peuvent rapidement être communiqué à des tiers.

L'utilisateur doit donc prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information, de limiter l'envoi de messages non sollicités et de ne pas engager sa responsabilité civile ou pénale ou celle du Syndicat.

Avant tout envoi, il est impératif de vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises.

En cas d'envoi à une pluralité de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non-sollicités.

Il doit également dissimuler les destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires.

En cas d'envoi à une liste de diffusion, il est impératif de vérifier la liste des destinataires avant l'envoi. La vigilance des utilisateurs doit redoubler en présence d'informations à caractère personnel et/ou confidentiel. Les messages doivent dans ce cas être cryptés, conformément aux recommandations de l'ANSSI.

Le risque de retard, de non remise et de suppression automatique des messages électroniques doit être pris en considération pour l'envoi de correspondances importantes.

Les messages importants doivent être envoyés avec un accusé de réception et être, le cas échéant, doublés par des envois postaux.

Afin de ne pas surcharger les serveurs de messagerie, il est attendu de chaque utilisateur une gestion des messages (suppression, archivage, effacement périodique) et de la taille des pièces jointes envoyées.

L'utilisateur doit veiller au respect des lois et règlements. Les correspondances électroniques ne doivent comporter aucun élément illicite, tel que des propos diffamatoires, injurieux, contrefaisants ou, d'une manière plus générale, contrevenants aux dispositions statutaires relatives aux droits et obligations du fonctionnaire.

Les échanges électroniques avec des tiers ont la même valeur juridique que les échanges papier. Un message électronique peut donc être une preuve ou un début de preuve, engageant l'utilisateur ou le SAVM.

11. Accès distant

Deux types d'accès sont possibles :

11.1- Avec tout appareil relié à Internet, les agents du SAVM peuvent accéder à leur messagerie à distance

Il convient de s'assurer que le poste à partir duquel l'agent établit la connexion dispose bien des protections indispensables (anti-virus, pare-feu activé, ...),

Lorsque l'utilisation de la messagerie doit être interrompue, il est indispensable de se déconnecter.

En fin de session, il faut également veiller à se déconnecter et effacer les fichiers qui auraient été copiés sur l'ordinateur local (ou tout autre appareil) utilisé par l'agent.

11.2 Avec un smartphone qui dispose de logiciel spécifique

Les appareils fournis par le SAVM sont paramétrés par la DAG accompagnée du prestataire informatique, il est interdit d'en modifier la configuration.

L'usage d'équipements personnels est soumis à autorisation du SAVM qui communiquera les données de connexion mais ne garantira ni support, ni assistance.

Tous ces appareils, qu'ils soient propriété du SAVM ou personnels, doivent être protégés pour interdire l'accès à la messagerie en cas de perte ou de vol.

Lors d'une connexion à la messagerie du SAVM depuis Internet, les utilisateurs doivent être attentifs aux conseils de prudence ci-dessus afin de garantir la confidentialité des messages.

Les agents bénéficiant du dispositif de télétravail doivent se conformer, en plus de ces règles, aux dispositions particulières qui leur sont communiquées dans le cadre de l'organisation du télétravail.

12. Téléphonie

Chaque utilisateur dispose de moyens de téléphonie destinés à l'exercice de son activité professionnelle.

Il peut s'agir, soit de téléphones fixes, soit pour certains cas liés aux fonctions et/ou aux missions, de téléphones mobiles.

L'utilisation du téléphone à titre privé est admise à condition qu'elle demeure ponctuelle et raisonnable.

Il n'y a aucune restriction d'utilisation des téléphones fixes (zones d'appel, numéros surtaxés...).

Le SAVM s'interdit de mettre en œuvre un suivi individuel de l'utilisation des services de télécommunications.

Aucune statistique globale n'est réalisée sur l'ensemble des appels entrants et sortants, notamment pour vérifier les consommations.

En cas d'utilisation manifestement anormale, le SAVM, sur demande du directeur général, peut accéder aux numéros complets des relevés individuels.

13. Départ d'un utilisateur

Lors de son départ, ou lorsque la durée prévisible d'une absence est supérieure à 12 mois, l'utilisateur doit restituer au SAVM les matériels nomades mis à sa disposition. Le poste de travail fixe et le téléphone doivent être laissés à leur place habituelle.

Il doit préalablement :

- Vérifier qu'aucune donnée professionnelle ne subsiste sur ces équipements, sans avoir été sauvegardée ou transmise à un autre agent (ces données risquent d'être définitivement perdues lors de la reconfiguration du ou des appareils concernés)
- Effacer tous ses fichiers et données privées (après en avoir effectué éventuellement une sauvegarde)
- Signaler tout problème affectant le matériel qu'il avait à sa disposition.

La copie pour conservation de documents professionnels, à l'occasion d'un départ, ne peut se faire qu'avec l'autorisation expresse du supérieur hiérarchique.

L'accès de cet utilisateur au système d'information est bloqué à la date de cessation effective de ses fonctions au SAVM, sauf dérogation exceptionnelle et motivée accordée par le directeur général.

Les conditions de suppression des comptes et des données personnelles de l'utilisateur concerné sont précisées dans une procédure annexe. Dans certains cas exceptionnels, la direction générale peut accorder une dérogation à ces règles sur demande du supérieur hiérarchique.

14. Traçabilité

Les opérations que doit exécuter le prestataire informatique font l'objet d'une traçabilité garantie par les dispositions suivantes :

- L'administrateur dispose d'un compte nominatif sur tous les systèmes dont il a la charge, y compris les systèmes administrés pour le compte des partenaires
- Lorsqu'une intervention de maintenance informatique ou de support doit être effectuée sur le poste d'un utilisateur, l'administrateur peut accéder à distance sur le poste en question.

Ce type d'intervention est toutefois soumis à l'information et l'accord préalable de chaque utilisateur concerné.

15. Protection des données

Le règlement n°2016/679 dit « règlement général sur la protection des données » du 27 avril 2016 définit les conditions dans lesquelles des traitements de données personnelles peuvent être opérés au sein de l'UE.

L'annexe 2 présente les modalités dans lesquels les traitements de données doivent être réalisées au sein du SAVM.

16. Conditions d'administration du système d'information

Pour des nécessités de maintenance et de gestion, l'utilisation des ressources matérielles ou logicielles, les échanges via le réseau, ainsi que les rapports des télécommunications peuvent être analysés et contrôlés dans le respect de la législation applicable, et notamment de la loi Informatique et Libertés.

L'utilisateur est informé que pour effectuer la maintenance, le prestataire informatique dispose de la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition, et qu'une maintenance à distance est précédée d'une information de l'utilisateur.

Pour des nécessités de maintenance et de gestion technique, l'utilisation des services et notamment des ressources matérielles et logicielles, ainsi que des échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et notamment dans le respect des règles relatives à la protection de la vie privée et au respect des communications privées.

Le Syndicat se réserve, dans ce cadre, le droit de recueillir et de conserver les informations nécessaires à la bonne marche du système. Il se réserve la possibilité de procéder à un contrôle des sites visités afin d'éviter l'accès par ces derniers à des sites illicites ou requérant l'âge de la majorité.

Le Syndicat assure une traçabilité sur l'ensemble des accès aux applications et aux ressources informatiques qu'elle met à disposition pour des raisons d'exigence réglementaire de traçabilité, de prévention contre les attaques et de contrôle du bon usage des applications et des ressources.

Par conséquent, les applications du SAVM, ainsi que les réseaux, messagerie et accès internet intègrent des dispositifs de traçabilité permettant le contrôle si besoin de :

- L'identifiant de l'utilisateur ayant déclenché l'opération,
- L'heure de la connexion,
- Le logiciel ou programme utilisé.

Le prestataire informatique respecte la confidentialité des données et des traces auxquelles il est amené à accéder dans l'exercice de ses fonctions, mais peut être amené à les utiliser pour mettre en évidence certaines infractions commises par les utilisateurs.

17. Responsabilité et sanctions

L'utilisateur est responsable de son utilisation des outils d'information et de communication mis à sa disposition.

Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager sa responsabilité et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés.

18. Information des agents

La présente charte est affichée publiquement. Elle est communiquée individuellement à chaque agent.

Le prestataire informatique est à la disposition des agents pour leur fournir toute information concernant l'utilisation des nouvelles technologies de l'information et de la communication.

Il informe les utilisateurs régulièrement sur l'évolution des limites techniques du système d'information et sur les menaces susceptibles de peser sur sa sécurité.

19. Évolution de la charte informatique

La présente charte peut être amenée à évoluer, notamment en raison des évolutions législatives et réglementaires.

20. Entrée en vigueur de la charte informatique

La présente charte est applicable à compter du 13 décembre 2022.

Annexe 1

Désignation et Coordonnées

Responsable du contrôle du bon fonctionnement
du système d'information et de communication

Le Président du SAVM

Prestataire informatique

I P E

Délégué à la Protection des Données
(« Data Protection Officer » ou « DPO » en anglais)

DPO consulting

Annexe 2

Traitements de données à caractère personnel au sein du SAVM

I - PROTECTION DES DONNEES A CARACTERE PERSONNEL

Une **donnée personnelle** est décrite par la CNIL comme « toute information se rapportant à une personne physique identifiée ou identifiable ». Il existe 2 types d'identifications :

- identification directe (nom, prénom etc.) ;
- identification indirecte (identifiant, numéro etc.).

Lorsqu'une opération ou un ensemble d'opérations portant sur des données personnelles sont effectuées, on considère qu'il s'agit de **traitement de données personnelles**. La CNIL donne les actions suivantes à titre d'exemple du traitement des données :

- tenue d'un fichier de ses clients ;
- collecte de coordonnées de prospects via un questionnaire ;
- mise à jour d'un fichier de fournisseurs.

Article 1 : confidentialité des données

Le règlement n°2016/679 dit « règlement général sur la protection des données » du 27 avril 2016 définit les conditions dans lesquelles des traitements de données personnelles peuvent être opérés. Il institue au profit des personnes concernées par les traitements de données des droits que le présent règlement invite à respecter, tant à l'égard des utilisateurs que des tiers.

Les agents sont soumis à une obligation de discrétion qui leur impose d'assurer la confidentialité des données qu'ils détiennent.

Un comportement exemplaire est exigé dans toute communication orale ou écrite, téléphonique ou électronique, que ce soit lors d'échanges professionnels ou au cours de discussions relevant de la sphère privée.

Article 1.1 : accès aux données par les agents

L'accès par les agents aux informations et documents conservés doit être limité à ceux qui leur sont propres, ainsi que ceux publics ou partagés.

Il est ainsi interdit de prendre connaissance des informations détenues par d'autres agents, même si ceux-ci ne les ont pas explicitement protégées. Cette règle s'applique en particulier aux données couvertes par le secret professionnel, ainsi qu'aux conversations de type courrier électronique dont l'agent n'est ni directement destinataire, ni en copie.

Article 1.2 : Responsable de traitements et délégué à la protection des données

Le Président est responsable des traitements de données à caractère personnel. Le responsable de traitements veille au sein du Syndicat à la bonne application des règles issues du règlement général sur la protection des données.

Un délégué à la protection des données (cf annexe 1) a été désigné afin d'accompagner le SAVM dans sa mise en conformité et afin de piloter la bonne application de ces règles.

II - REPONSES AUX DEMANDES D'USAGE DES DROITS DES PERSONNES CONCERNEES PAR LES TRAITEMENTS DE DONNEES

Article 2.1 : Droits des personnes concernées par les traitements de données

Les personnes concernées par les traitements de données personnelles, quels qu'ils soient, disposent de droits leur permettant de garder la maîtrise des informations les concernant. Ainsi, toute personne peut :

- Accéder à l'ensemble des informations la concernant ;
- Connaître l'origine de ces informations ;
- En obtenir une copie ;
- Exiger que ses données soient rectifiées, complétées, mises à jour ou, selon les cas, supprimées.

Article 2.2 : Droit à l'information des personnes concernées par les traitements de données

Les agents ont l'obligation d'informer toute personne du recueil de ses données à caractère personnel, de ses droits ainsi que des moyens par lesquels cette personne pourra user de ses droits sur ces données.

Article 2.3 : Demandes d'usage des droits des personnes

Les personnes concernées par les traitements de données à caractère personnel peuvent faire usage de leurs droits sur simple demande, soit par écrit, soit en personne.

Les agents recevant une telle demande ont pour obligation de contrôler par tous moyens de l'identité du demandeur.

Article 2.4 : Instruction des demandes d'usage des droits des personnes

Les agents recevant une demande d'usage des droits des personnes concernées par un traitement de données ont pour obligation de transmettre cette demande au service chargé de la mise en œuvre du traitement.

Ce service aura alors pour obligation de répondre à cette demande dans un délai maximum d'un mois à compter de la date de présentation de la demande.

A défaut de pouvoir identifier le service chargé de la mise en œuvre du traitement, les agents peuvent transmettre la demande d'usage des droits de la personne concernée par le traitement au délégué à la protection des données qui sera alors chargé de procéder à son instruction dans les mêmes délais et selon la même procédure.

La réponse devra se faire de manière compréhensible. Toute abréviation, sigle ou code devra faire l'objet de précisions, notamment aux moyens d'un lexique ou d'une notice explicative.

Article 2.5 : Refus de la demande d'usage des droits des personnes

La demande pourra être refusée pour des motifs légitimes, notamment le respect d'une obligation légale. Peuvent également être refusées les demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique.

Tout refus devra alors faire l'objet d'une justification. Le demandeur devra être également informé des voies et délais de recours permettant de contester cette décision.

Si le Syndicat ne dispose d'aucune donnée sur la personne qui exerce son droit d'accès, une réponse précisant ce fait devra être apportée dans le délai d'un mois.

Article 2.6 : Réponses aux demandes d'usage des droits des personnes

Toute demande et toute réponse devront faire l'objet d'une traçabilité. Tout service instruisant une telle demande ou procédant à une telle réponse devra procéder à son inscription dans le registre des demandes d'usage des droits sur les données à caractère personnel.

Ce registre est tenu et mis à jour avec l'aide du délégué à la protection des données.

III - VIOLATIONS DE DONNEES A CARACTERE PERSONNEL

Article 3.1 : Constatation des violations de données

Toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une manière, ou l'accès non autorisé à de telles données constitue une violation de données à caractère personnel.

Tout agent amené à constater une telle violation de données a l'obligation d'en informer immédiatement le délégué à la protection des données.

Article 3.2 : Documentation de la violation de données

Conjointement avec le délégué à la protection des données, l'agent devra, dans un délai maximum de 48 heures :

- Déterminer la nature de la violation ;
- Déterminer la catégorie et le nombre approximatif de personnes concernées par les données faisant l'objet de la violation ;
- Déterminer la catégorie et le nombre approximatif de données concernées ;
- Décrire les conséquences probables de la violation de données ;
- Déterminer et décrire les mesures prises pour atténuer les effets de la violation et éviter que celle-ci ne se reproduise.

L'ensemble de ces éléments devront faire l'objet d'une traçabilité et d'une inscription dans le registre des violations de données.

Ce registre est tenu et mis à jour avec l'aide du délégué à la protection des données.

Article 3.3 : Notification des violations de données auprès de la CNIL

Toute violation de données susceptible de porter atteinte à la vie privée des personnes concernées par les données touchées par la violation doit faire l'objet d'une notification auprès de la CNIL aux moyens d'une plate-forme sécurisée sur son site internet (www.cnil.fr).

Cette notification devra être réalisée conjointement avec le délégué à la protection des données dans un délai maximal de 72 heures suivant la violation de données ou, à défaut, dans un délai maximal de 72 heures suivant la constatation de la violation de données.

En cas d'impossibilité de réunir toutes les informations susmentionnées dans l'article 3.2 dans un tel délai, une notification initiale devra être déposée dans ledit délai, suivie d'une notification complémentaire dès que l'ensemble des éléments seront réunis.

Toute notification effectuée hors délai devra être justifiée.

Article 3.4 : Notification des violations de données auprès des personnes concernées

Toute violation de données susceptible de porter une atteinte excessivement élevée à la vie privée des personnes concernées par les données touchées par la violation devra, en outre de la notification mentionnée à l'article 3.3, faire l'objet d'une notification auprès des personnes concernées.

La notification devra *a minima* contenir et exposer, en des termes clairs et précis, la nature de la violation, les conséquences probables de la violation, les coordonnées du délégué à la protection des données et les mesures prises pour remédier à la violation et en limiter les conséquences.

La notification devra être complétée, si nécessaire, de recommandations à destination des personnes pour atténuer les effets négatifs potentiels de la violation et leur permettre de prendre les précautions qui s'imposent, tel qu'un changement de mot de passe ou la vérification de l'intégrité des données de leur compte utilisateur.

Cette notification devra être réalisée en collaboration avec le délégué à la protection des données dans les meilleurs délais.

Article 3.5 : Traçabilité des notifications de violations de données

La notification de la violation de données auprès de la CNIL et, le cas échéant, la notification aux personnes concernées devront faire l'objet d'une traçabilité et être inscrites dans le registre des violations de données.

Annexe 3

Formulaire à compléter

Nom – Prénom :

Grade :

Direction/service :

Déclare que la charte informatique du SAVM m'a été remise, m'engage à en prendre connaissance et à m'y conformer.

Fait le

SIGNATURE