Charte de Sécurité et de Confidentialité pour l'accès aux Données Personnelles par le Prestataire

Juin 2025

Préambule

Dans le cadre de son engagement continu envers la protection des données personnelles des personnes concernées et la conformité avec les normes législatives en vigueur, notamment le Règlement Général sur la Protection des Données (RGPD) et autres réglementations locales pertinentes, le Prestataire a établi cette Charte de Sécurité et de Confidentialité. Cette Charte régit les conditions d'accès et d'utilisation aux données personnelles par le Prestataire, WAVENSYS, un prestataire engagé pour fournir au Client des solutions et équipements de radiocommunication, de vidéosurveillance et de caméras piétons.

La nature sensible des données manipulées dans le cadre de ces fonctions exige non seulement une vigilance constante mais aussi une coopération étroite pour prévenir toute forme de risque lié à la sécurité des données. En conséquence, il est crucial que toutes les opérations de traitements soient effectuées dans un cadre strictement contrôlé et sécurisé, garantissant ainsi que toutes les mesures nécessaires sont prises pour protéger les informations contre tout accès non autorisé, utilisation abusive, perte, altération ou destruction.

Cette charte est donc conçue pour formaliser les obligations, les responsabilités et les procédures qui encadrent la collaboration du Client avec le Prestataire.
Par la présente charte, le Prestataire s'engage à respecter et à faire respecter toutes les stipulations contenues ici, pour maintenir et renforcer la protection des données personnelles et la sécurité systèmes informatiques du Client.

Article 1: Objectifs de la Charte

La présente charte vise à établir un cadre de coopération sécurisé entre le Client et le Prestataire, tout en respectant les principes suivants :

Protection des données personnelles

Assurer la protection intégrale des données personnelles traitées contre tout accès, utilisation ou divulgation non autorisés. Cela inclut la prévention de toute perte, altération ou destruction des données par des mesures de sécurité appropriées. L'intégrité, la confidentialité et la disponibilité des données personnelles des personnes concernées doivent être préservées à tout moment pour maintenir la confiance des parties prenantes et répondre aux attentes des personnes concernées.

Contrôle d'accès rigoureux

Établir et maintenir des contrôles d'accès robustes et personnalisés pour garantir que seul le Prestataire puisse accéder aux données personnelles, et uniquement pour les tâches spécifiquement définies par le contrat de service. Les droits d'accès doivent être attribués sur la base du principe du moindre privilège, et tous les accès doivent être régulièrement revus et ajustés en fonction des changements de rôle ou des besoins opérationnels.

1. Conformité réglementaire : Se conformer à toutes les lois et réglementations applicables en matière de protection des données, y compris, mais sans s'y limiter, le RGPD. Cela comprend la mise en œuvre de toutes les mesures nécessaires pour assurer la conformité réglementaire lors du traitement, de l'accès et de la gestion des données personnelles. Le Prestataire doit également aider le Client à répondre à toute demande de droits des sujets de données (comme les demandes d'accès, de rectification ou de suppression) de manière efficace et conforme.

2. Formation et sensibilisation : le Prestataire doit fournir une formation régulière et complète à son personnel concernant les exigences du RGPD, les bonnes pratiques en matière de sécurité des données et les spécificités de la manipulation des données. Cette formation doit viser à renforcer la sensibilisation à l'importance de la protection des données personnelles et à assurer que toutes les interactions avec le Client se conforment à cette charte et aux lois pertinentes.

3. Audits et rapports : Permettre des audits réguliers, à la fois internes et externes, pour vérifier le respect de cette charte. Le Prestataire doit fournir tous les rapports nécessaires et collaborer lors des audits pour démontrer leur conformité avec les normes de sécurité et réglementaires établies.

En adhérant à ces objectifs, le Client et le Prestataire s'engagent à maintenir un environnement de travail sécurisé qui protège les données personnelles contre toute menace ou vulnérabilité potentielles, tout en renforçant la conformité et la gouvernance des données au sein de leurs opérations respectives.

Article 2: Accès aux Données personnelles

L'accès aux données personnelles est strictement réglementé pour garantir que seul le Prestataire puisse accéder aux données dans le cadre de ses fonctions contractuelles. Les stipulations suivantes doivent être mises en place pour assurer la sécurité et la conformité de cet accès :

1. Autorisation formelle d'accès : Tout accès aux données personnelles par le Prestataire doit être formellement autorisé par le Client. Cette autorisation est conditionnée par la pertinence et la nécessité de l'accès dans le cadre des tâches assignées. L'accès ne peut être accordé que pour les fonctions spécifiques pour lesquelles il existe un besoin clairement défini de traitement des données.

2. Création, gestion et révocation des identifiants : L'accès aux données personnelles par le Prestataire est soumis à des protocoles stricts pour garantir la sécurité et la confidentialité des données. Les modalités suivantes doivent définir la gestion des identifiants et le processus d'autorisation :

Création des identifiants :

Les identifiants d'utilisateur pour accéder aux données personnelles sont créés uniquement par le département des systèmes d'information du client.

Chaque identifiant est unique et lié à une personne spécifique, le Prestataire, avec des permissions strictement définies basées sur le rôle et les besoins d'accès du Prestataire.

Les mots de passe associés aux identifiants doivent respecter les politiques de sécurité, incluant des critères de complexité et de renouvellement régulier.

Révocation et gestion des identifiants :

Les identifiants sont immédiatement révoqués lorsque le salarié du Prestataire cesse d'être impliqué dans le projet, change de fonction ou quitte l'entreprise.

Un audit des accès est réalisé trimestriellement par le client pour s'assurer que tous les identifiants actifs sont valides et appropriés.

3. Accès restreint aux informations des personnes concernées : L'accès aux informations personnelles des personnes concernées peut se faire qu'après une autorisation explicite du Client. Cette autorisation doit être documentée et limitée aux données strictement nécessaires pour accomplir les services spécifiés dans le contrat.

4. Mécanismes d'authentification sécurisée : Des méthodes d'authentification robustes, telles que l'authentification multifactorielle et les protocoles sécurisés de chiffrement des sessions, sont exigées pour tout accès aux données personnelles. Ces mesures garantissent que l'accès est sécurisé et protégé contre toute interception ou utilisation frauduleuse.

5. Revues périodiques des accès : Les droits d'accès accordés au Prestataire sont régulièrement revus par le Client pour s'assurer qu'ils restent appropriés et sécurisés. Cette revue a lieu au moins une fois par an ou chaque fois qu'un changement significatif dans les besoins opérationnels ou le personnel se produit.

6. Enregistrement et surveillance des connexions : Des registres des connexions seront établis sous les responsabilités respectives du Prestataire et du Client, mentionnant les date et nature détaillée des interventions ainsi que les noms de leurs auteurs. Ce registre aide à suivre l'accès au système et constitue un élément essentiel pour les audits de sécurité.

7. Procédures de déconnexion sécurisée : Des procédures de déconnexion automatique après une période d'inactivité ou à la fin de chaque session sont mises en place pour réduire le risque d'accès non autorisé. Le Prestataire est également tenu de suivre des pratiques strictes de fin de session pour assurer que l'accès aux données personnelles est sécurisé à la conclusion de chaque intervention.

En respectant ces directives, le Client et le Prestataire s'engagent à maintenir un haut niveau de sécurité et de confidentialité pour les données personnelles des personnes concernées. Cela renforce la confiance des personnes concernées et la conformité aux réglementations sur la protection des données.

Article 3: Utilisation des Données

L'utilisation des données personnelles est réglementée afin de garantir que le Prestataire manipule ces informations uniquement dans le cadre des tâches spécifiées par le contrat et respecte les principes de minimisation et de limitation des données. Les règles suivantes définissent l'usage approprié des données :

1. Finalité spécifique de l'utilisation : Les données personnelles ne doivent être utilisées que pour réaliser les tâches spécifiquement définies dans le contrat de services entre le Client et le Prestataire. Tout autre usage des données, non explicitement autorisé par le Client, est strictement interdit.

2. Minimisation des données : le Prestataire s'engage à n'accéder et à utiliser que les données strictement nécessaires pour accomplir les fonctions contractuellement agréées. Cette approche de minimisation vise à limiter l'exposition des données personnelles et à réduire le risque de leur traitement non autorisé.

3. Restrictions sur la copie et le transfert : Il est interdit de copier ou de transférer des données en dehors des systèmes autorisés sans l'approbation écrite préalable du Client. Toute copie des données pour des raisons de sauvegarde ou de traitement doit être effectuée conformément aux politiques de sécurité du Client et les supports de données doivent être chiffrés et sécurisés.

4. Utilisation d'Outils et de Matériel Autorisés :

Le Prestataire s'engage à n'utiliser que des outils, logiciels, plateformes, infrastructures et matériels expressément autorisés par le Client pour le traitement des données personnelles. Toute utilisation d'outils ou de matériel non autorisé est strictement interdite et considérée comme une violation grave des obligations du Prestataire.

5. Anonymisation et pseudonymisation : Lorsque cela est possible et applicable, les données doivent être anonymisées ou pseudonymisées pour protéger l'identité des individus lors de l'analyse de données ou du développement de systèmes qui n'ont pas besoin d'accéder à des données personnelles complètes.

6. Durée de conservation des données : Les données personnelles ne doivent pas être conservées plus longtemps que nécessaire pour les objectifs spécifiés dans le contrat. Le Prestataire doit se conformer aux politiques de conservation des données du Client.

7. Sécurité lors de l'utilisation des données : Lors de l'utilisation des données, le Client doit s'assurer que toutes les mesures de sécurité nécessaires sont en place, y compris les contrôles d'accès, le chiffrement et la surveillance pour prévenir et détecter toute utilisation inappropriée.

Article 4: Sécurité des Données

La sécurité des données personnelles est une priorité absolue pour le Client et le Prestataire. Les mesures suivantes sont établies pour garantir une protection efficace des données contre toute perte, altération, accès ou divulgation non autorisés :

1. Infrastructure de sécurité : le Prestataire doit maintenir une infrastructure de sécurité robuste et conforme aux normes industrielles. Cela inclut, sans s'y limiter, des pares-feux avancés, des systèmes de détection d'intrusion, et le chiffrement des données en transit et au repos.

2. Contrôles d'accès : Les contrôles d'accès doivent être configurés pour garantir que seul le Prestataire puisse accéder aux données sensibles. Les droits d'accès sont attribués sur la base du besoin de connaître et sont régulièrement revus pour assurer leur pertinence.

3. Gestion des identités et des accès : Un système de gestion des identités doit être en place pour créer, gérer et supprimer les identifiants et les accès de manière sécurisée. Les mots de passe doivent respecter des politiques de complexité élevée et être changés régulièrement.

4. Protection contre les malwares : le Prestataire est tenu d'utiliser des solutions antivirus et anti-malware à jour sur tous les systèmes qui accèdent aux données personnelles ou traitent des données personnelles.

5. Sécurité physique : Les installations où les données sont traitées ou stockées doivent être sécurisées par des mesures de sécurité physique, y compris, mais sans s'y limiter, des systèmes de contrôle d'accès et de surveillance vidéo.

6. Sauvegardes sécurisées : Des copies de sauvegarde des données doivent être réalisées régulièrement et stockées en sécurité dans des emplacements géographiquement distincts pour garantir la récupérabilité en cas de sinistre. Les sauvegardes doivent également être chiffrées et protégées par des contrôles d'accès stricts.

7. Plan de réponse aux incidents de sécurité : Un plan de réponse aux incidents doit être établi pour traiter rapidement et efficacement toute violation de la sécurité des données. Ce plan doit inclure des procédures pour isoler et éradiquer la source de l'incident, ainsi que des mesures pour communiquer avec le Client et, si nécessaire, avec les autorités réglementaires et les individus affectés.

8. Formation en sécurité des données : le personnel du Prestataire, ayant accès aux données personnelles, doit recevoir une formation régulière sur les meilleures pratiques en matière de sécurité des données, y compris la sensibilisation aux menaces courantes et aux techniques de prévention.

Article 5: Confidentialité et protection de données

Dans le cadre de son engagement à assurer la confidentialité et la sécurité des données personnelles, le Prestataire doit se conformer aux directives suivantes :

1. **Protection des données** :
    - **Stockage des données** : Toutes les données personnelles doivent être stockées dans des environnements sécurisés et conformes aux normes de sécurité de l'industrie. Les données sensibles stockées localement doivent être conservées dans des serveurs sécurisés avec un accès contrôlé.
    - **Cryptage** : Les données personnelles doivent être cryptées lors du stockage et du transfert. L'utilisation de protocoles de cryptage reconnus et approuvés par l'industrie est obligatoire pour assurer que les données restent inaccessibles et indéchiffrables en cas d'accès non autorisé.
    - **Sauvegarde** : Des sauvegardes régulières des données doivent être effectuées pour prévenir la perte de données due à des défaillances matérielles, des cyberattaques ou d'autres catastrophes. Les sauvegardes doivent également être stockées de manière sécurisée et cryptée.
2. **Partage d'informations** :
    - Les données personnelles ne doivent en aucun cas être partagées avec des tiers non autorisés. Tout partage d'informations doit être strictement conforme aux accords préétablis avec le Client et doit être documenté par des accords écrits stipulant les obligations de confidentialité et de sécurité des tiers.
    - Des contrôles doivent être mis en place pour s'assurer que les tiers respectent les mêmes standards de protection des données que ceux exigés par cette charte.

3. **Non divulgation** :
    - Le Prestataire doit signer un accord de non-divulgation. Cet accord doit stipuler clairement que les informations confidentielles obtenues ne peuvent être ni divulguées ni utilisées en dehors des limites de leur mission et de leurs responsabilités contractuelles.
    - Les obligations de confidentialité doivent continuer à s'appliquer même après la fin de l'engagement du Prestataire ou la conclusion du contrat de service avec le Client.

Article 6: Formation et Sensibilisation

Afin de renforcer la sécurité des données et de promouvoir une culture de la protection des données chez le Prestataire, les mesures suivantes doivent être mises en œuvre pour assurer que le personnel du Prestataire soit correctement formé et conscient des responsabilités liées à l'accès et à l'utilisation des données personnelles :

1. Programme de formation obligatoire : le personnel du Prestataire doit suivre un programme de formation obligatoire. Ce programme doit couvrir les principes fondamentaux de la protection des données, les exigences spécifiques du RGPD, ainsi que les politiques internes du Client en matière de sécurité des données.

2. Sensibilisation continue : En plus de la formation formelle, le personnel du Prestataire doit suivre des campagnes régulières de sensibilisation pour maintenir la sécurité des données et la protection de la vie privée comme priorités constantes. Cela peut inclure des bulletins d'information, des quiz de sécurité, et des affichages informatifs sur les lieux de travail.

3. Évaluation de la formation : L'efficacité des programmes de formation et de sensibilisation doit être évaluée régulièrement à travers des tests, des évaluations de la conformité et des audits internes pour s'assurer que le personnel du Prestataire comprend et applique les pratiques de sécurité des données.

Ces mesures visent à garantir que le Prestataire possède les connaissances et les compétences nécessaires pour gérer les données personnelles de manière sécurisée et conforme, réduisant ainsi les risques de violations de données et renforçant la sécurité globale du système d'information.

Article 7: Surveillance et Audit

Pour garantir la conformité continue du Prestataire avec les normes de sécurité et les obligations légales définies dans cette charte, les mesures de surveillance et d'audit suivantes doivent être mises en œuvre :

1. Audits réguliers : le Client a le droit de conduire des audits de sécurité internes et externes sur les systèmes, les processus et les données gérés par le Prestataire.

2. Fréquence des audits : Les audits peuvent être réalisés au maximum une fois par an, ou plus fréquemment, à la suite d'une violation de données.

3. Coopération lors des audits : le Prestataire est tenu de coopérer pleinement lors des audits et doit fournir l'accès à toutes les informations, systèmes et installations nécessaires pour faciliter ces audits, dans le strict respect de la confidentialité des données appartenant à ses autres clients. Cela inclut l'accès aux registres des activités, aux politiques de sécurité, aux protocoles de gestion des données et à tout autre document pertinent.

4. Audit par des tiers : le Client peut engager des auditeurs externes indépendants pour effectuer des audits de sécurité. Le Prestataire doit accepter et faciliter l'intervention de ces auditeurs tiers, qui doivent avoir accès aux mêmes informations que les auditeurs internes.

5. Rapports d'audit : À la suite de chaque audit, un rapport d'audit doit être généré, détaillant les constatations, les recommandations et les mesures correctives nécessaires. Le Prestataire est responsable de l'implémentation de ces mesures correctives pour remédier à tout écart identifié.