ARTCI
AUTORITE DE REGULATION DES TELECOMMUNICATIONS/TIC DE COTE D'IVOIRE
CONSEIL DE REGULATION

REPUBLIQUE DE CÔTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2025-1215

DE L'AUTORITE DE PROTECTION DE LA REPUBLIQUE DE COTE D'IVOIRE

EN DATE DU 18 FEVRIER 2025

PORTANT AUTORISATION DE TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL

PAR FALCON SECURITY HUB

Conseil de Régulation : 31 Av Nogués, Imble Broadway 2ème étage 17 BP 110 Abj 17 Tél: +225 27 20 34 43 04 - Fax: +225 27 20 34 43 02
Siège Direction Générale : Marcory Anoumabo, 18 BP 2203 Abj 18 Tél: +225 27 20 34 43 73 / 74 - Fax: + 225 27 20 34 43 75
www.artci.ci

L'AUTORITE DE PROTECTION,

Vu la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;

Vu la Loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité ;

Vu la Loi n°2013-546 du 30 juillet 2013 relative aux Transactions électroniques ;

Vu la Loi n°2014-136 du 24 mars 2014 portant règlementation des bureaux d'information sur le crédit ;

Vu la Loi n°2015-532 du 20 juillet 2015 portant Code du travail ;

Vu la Loi n°2024-352 du 06 juin 2024 relative aux communications électroniques ;

Vu le Décret n°2012-934 du 19 septembre 2012 portant organisation et fonctionnement de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) ;

Vu le Décret n°2014-105 du 12 mars 2014 portant définition des conditions de fourniture des prestations de cryptologie ;

Vu le Décret n°2014-106 du 12 mars 2014 fixant les conditions d'établissement et de conservation de l'écrit et de la signature sous forme électronique ;

Vu le Décret n°2015-79 du 04 février 2015 fixant les modalités de dépôt des déclarations, de présentation des demandes, d'octroi et de retrait des autorisations pour le traitement des données à caractère personnel ;

Vu le Décret n°2019-947 du 13 novembre 2019 portant nomination du Président de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

Vu le Décret n°2019-985 du 27 Novembre 2019 portant nomination des Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) ;

Vu le Décret n°2021-916 du 22 décembre 2021 portant adoption du référentiel général de sécurité des systèmes d'information et du plan de protection des infrastructures critiques ;

Vu le Décret n°2021-917 du 22 décembre 2021 définissant les procédures d'audit, de contrôle et de certification des systèmes d'information ;

Vu le Décret n° 2022-783 du 12 octobre 2022 portant renouvellement partiel du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

Vu le Décret n° 2023-440 du 24 mai 2023 relatif au contrôle de la qualité des engrais ;

Vu le Décret n°2025-55 du 17 janvier 2025 portant nomination du Directeur Général de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI)

Vu l'Arrêté 0099 MTND du 16 août 2024 modifiant l'Arrêté n°511/MPTIC/CAB du 11 novembre 2014 portant définition du profil et fixant les conditions d'emploi du correspondant à la protection des données à caractère personnel ;

Vu la Décision n°2013-0003 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 20 septembre 2013 portant règlement intérieur ;

Vu la Décision n°2014-0021 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 03 septembre 2014 portant conditions et critères applicables à la limitation du traitement des données à caractère personnel ;

Vu la Décision n°2014-0022 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 03 septembre 2014 portant conditions de la suppression des liens vers les données à caractère personnel, des copies ou des reproductions de celles-ci existant dans les services de communication électronique accessibles au public ;

Vu la Décision n°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel ;

Vu la Décision n°2017-0354 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 26 octobre 2017 portant procédure de mise en conformité des responsables du traitement avec la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;

Vu la Décision n°2021-0676 du Conseil de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 04 Août 2021 portant procédure de contrôle en matière de Protection des Données à Caractère Personnel ;

Vu le rapport d'audit de protection des données personnelles de FALCON SECURITY HUB ;

Par les motifs suivants :

Considérant que conformément à l'article 53 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, les responsables du traitement sont tenus de procéder à la mise en conformité des traitements qu'ils opèrent avec ladite loi ;

Considérant que pour faciliter cette mise en conformité, l'Autorité de Protection a par décision n°2017-0354 du 26 octobre 2017, défini la procédure de mise en conformité des responsables du traitement avec la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;

Considérant que FALCON SECURITY HUB est une SARL de droit ivoirien, avec un capital social de 1.000.000 FCFA, immatriculée au RCCM d'Abidjan sous le numéro CI-ABJ-2010-B- 4853 et dont le siège social est situé à Marcory zone 4 C, rue Thomas Edison ;

Considérant que FALCON SECURITY HUB a pour objet social les activités liées à la gestion de flottes, la géolocalisation, la vidéoprotection, le contrôle et la sécurité incendie.

Considérant que FALCON SECURITY HUB a saisi l'Autorité de Protection d'une demande de mise en conformité ;

Considérant que FALCON SECURITY HUB a effectué son audit de protection des données personnelles ;

Considérant par ailleurs que le personnel de FALCON SECURITY HUB a effectué une formation sur la protection des données personnelles ;

Considérant les prescriptions contenues dans le rapport d'audit de protection des données personnelles.

Après en avoir délibéré,

DECIDE :

Article 1 :

FALCON SECURITY HUB est autorisée à effectuer les traitements des données mentionnées dans l'annexe 1 de la présente décision.

Les données non mentionnées dans l'annexe 1 ne devront aucunement faire l'objet d'un quelconque traitement de la part de FALCON SECURITY HUB.

Article 2 :

FALCON SECURITY HUB est autorisée à communiquer les données traitées uniquement aux destinataires habilités notamment :

1. les Services internes de FALCON SECURITY HUB, suivant leur niveau d'habilitation ;
2. la Caisse Nationale de Prévoyance Sociale (CNPS) ;
3. les Avocats et intermédiaires de justice ;
4. les Officiers de police judiciaire munis d'une réquisition ;
5. les Autorités publiques agissant dans le cadre de leurs missions ;
6. les Partenaires techniques et commerciaux ;
7. les Compagnies d'assurance ;
8. le Procureur de la République et les officiers de police judiciaire munis d'une réquisition ;
9. les Agents assermentés de l'Autorité de Protection, dans le cadre de leurs missions de contrôle.

Article 3 :

Avant tout transfert de données hors de la Côte d'Ivoire, FALCON SECURITY HUB est tenue de requérir l'autorisation préalable de l'Autorité de Protection et de stocker les données sur le territoire de la République de Côte d'Ivoire.

Article 4 :

Conformément à l'article 40 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, FALCON SECURITY HUB doit s'assurer que ses sous-traitants apportent des garanties suffisantes au regard des mesures de sécurité technique et organisationnelle relatives aux traitements de données qu'ils opèrent.

Il incombe à FALCON SECURITY HUB, ainsi qu'à ses sous-traitants, de veiller au respect de ces mesures.

Article 5 :

Les traitements de données autorisés dans la présente décision correspondent aux quatorze (14) finalités énumérées à l'annexe 2 de la présente décision.

Article 6 :

FALCON SECURITY HUB est tenue de mettre en œuvre les prescriptions énoncées dans l'annexe 4 de la présente décision. Elle le fait dans les délais prévus dans ladite annexe. La mise en œuvre desdites prescriptions fera l'objet d'un contrôle par l'Autorité de Protection.

L'Autorité de Protection délivrera une attestation de conformité à FALCON SECURITY HUB, lorsque toutes les prescriptions auront été mises en œuvre.

Article 7 :

FALCON SECURITY HUB est tenue de ne pas procéder au traitement de l'empreinte digitale pour le contrôle de présence des employés au sein des locaux de la société.

Article 8 :

En application de l'article 42 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, FALCON SECURITY HUB est tenue d'établir pour le compte de l'Autorité de Protection, un rapport annuel sur le respect des dispositions de l'article 41 de ladite loi.

FALCON SECURITY HUB communique ce rapport à l'Autorité de Protection, au plus tard le 31 janvier de l'année suivant l'exercice écoulé.

Article 9 :

L'Autorité de Protection procède à des contrôles auprès de FALCON SECURITY HUB, afin de vérifier le respect de la présente décision, dont la violation donnera lieu à des sanctions, conformément à la règlementation en vigueur.

Article 10 :

FALCON SECURITY HUB est tenue de procéder au paiement des frais de dépôts de demande d'autorisation auprès du Greffe de l'ARTCI, conformément à la décision n°2016-

0201 de l'Autorité de Protection de la République de Côte d'Ivoire fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel.

L'Autorité de Protection lui délivrera une facture à cet effet.

Article 11 :

La présente Décision entre en vigueur à compter de la date de sa notification à FALCON SECURITY HUB.

Article 12 :

Le Directeur Général est chargé de l'exécution de la présente décision, qui sera publiée au Journal Officiel de la République de Côte d'Ivoire et sur le site internet de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire.

Fait à Abidjan, le 18 Février 2025
En deux (2) exemplaires originaux

Le Président

Le Président

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

ANNEXE 1

DONNEES AUTORISEES AUX TRAITEMENTS (FALCON SECURITY HUB)

❖ **Données ordinaires**

- **Données d'identification :** Noms et prénoms, âge, nationalité, date et lieu de naissance,
- **Données de vie personnelle :** Situation matrimoniale, nombre d'enfants
- **Données de vie professionnelle :** Fonction, matricule, heure d'entrée et de sortie des véhicules, nom de l'entreprise, RCCM, raison sociale de l'entreprise, lieu de l'incident, expérience scolaire et professionnelle, expérience éducative et professionnelle, ancien CNPS, statut contractuel, date d'embauche et date de sortie (cdi ou cdd), heure de départ et d'arrivée, numéro CNPS
- **Données d'informations d'ordre économique et financier :** Montant, Relevé d'identité Bancaire (RIB), numéro de compte, salaire, montant des devis, DFE
- **Données de localisation :** Données GPS, domicile
- **Numéro d'identification national :** Numéro de téléphone, numéro du permis de conduire, numéro d'immatriculation
- **Données de connexion :** Adresse mail
- **Données biométriques :** Images, vidéos, empreintes digitales

❖ **Données sensibles**

- **Données médicales :** Etat général de santé
- **Autre donnée sensible :** Filiation

Fait à Abidjan, le 18 Février 2025

Le Président

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

Autorité de Régulation des Télécommunications / TIC de Côte d'Ivoire * ARTCI * Le Président

ANNEXE 2 : LISTE DES TRAITEMENTS PAR FINALITE (FALCON SECURITY HUB)

FINALITES	TRAITEMENTS
1. Gestion de la géolocalisation pour le compte des clients	- Réception - Consultation - Vérification - Suivi
2. Gestion de la géolocalisation interne	- Réception - Consultation - Vérification - Suivi
3. Gestion des activités financières des clients	- Réception - Consultation - Utilisation - Validation
4. Gestion de la formation des agents	- Collecte - Enregistrement
5. Gestion commerciale	- Collecte - Enregistrement - Suivi
6. Sécurité des biens et des personnes au sein des locaux (Vidéosurveillance en interne)	- Consultation - Visionnage - Reporting
7. Gestion de la vidéosurveillance pour le compte des clients	- Consultation - Visionnage - Reporting
8. Gestion du système d'information	- Consultation - Vérification
9. Gestion de la biométrie interne	- Contrôle

10. Gestion de l'installation de la biométrie pour le compte des clients	- Contrôle - Consultation
11. Gestion des ressources humaines	- Vérification - Validation - Suivi
12. Gestion de la paie	- Vérification - Validation - Suivi
13. Gestion de la relation client	- Réception - Consultation - Vérification - Envoi - Communication
14. Gestion du site internet	- Collecte - Consultation

Fait à Abidjan, le 18 Février 2025

Le Président

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

ANNEXE 3 :

PRESCRIPTIONS ET DELAIS D'EXECUTION (FALCON SECURITY HUB)

POINTS D'ANALYSE	PRESCRIPTIONS	DELAIS D'EXECUTIO
La légitimité et la licéité des traitements	Il est prescrit à FALCON SECURITY HUB de procéder au recueil du consentement préalable des personnes concernées. Elle le recueillera comme ci-dessous : ➢ **Dans le cadre de la gestion des relations avec les clients, les fournisseurs et les autres partenaires :** ○ insérer des clauses de consentement préalable, conformes aux exigences légales, dans les contrats proposés aux clients, fournisseurs et partenaires commerciaux ; ○ mettre à la disposition des personnes concernées un formulaire de recueil du consentement préalable. Les formulaires devront être mis à disposition lors de l'entrée en relation clientèle ; ○ mettre à la disposition des personnes concernées un formulaire de recueil du consentement préalable spécifique pour les traitements de données sensibles et les transferts de données. ➢ **Dans le cadre du recrutement et de la gestion du personnel :** ○ mettre à disposition, lors de l'entretien d'embauche, un formulaire de recueil de consentement préalable ; ○ mettre à disposition, lors de l'entretien d'embauche, un formulaire de recueil de consentement spécifique aux données sensibles ; ○ insérer des clauses de consentement préalable dans les contrats de travail proposés à la signature des salariés.	**60 jours**

	○ annexer au contrat des formulaires de consentement spécifiques à la géolocalisation et la biométrie. ➢ **Sur les sites internet :** ○ Intégrer au site internet un système de gestion des cookies personnalisable, offrant à l'utilisateur la liberté d'accepter ou de refuser la collecte et le transfert de ses données personnelles (falconcontrolsystems.com/) ○ Élaborer et mettre en ligne des Conditions Générales d'Utilisation (CGU), une politique de gestion des cookies, les mentions légales et la politique de confidentialité sur le site (falconcontrolsystems.com/) ; ○ Insérer des mentions d'information et de recueil du consentement dans chaque formulaire de collecte de données (contact…).	
Les délais de conservation	➢ **Concernant la conservation des données relatives à :** - **la gestion du personnel** : Il est prescrit à FALCON SECURITY HUB de conserver les données traitées pendant toute la durée du contrat de travail. En cas de rupture du contrat de travail, les données traitées devront être conservées pendant une période supplémentaire de : ○ trente (30) ans pour les données liées à la gestion du personnel et la paie ; ○ trois (03) mois pour les mots de passe ; ○ un (01) an pour les données de connexion ; ○ trois (03) ans pour toutes les autres données. - **la gestion des ressources humaines :** Il est prescrit à FALCON SECURITY HUB de conserver les données de recrutement traitées pendant une période de deux (02) ans, à compter du dernier contact avec la personne concernée. Par ailleurs, les dossiers médicaux doivent être conservés et archivés exclusivement par le personnel soignant (médecin du travail ou infirmier).	**12 mois**

- **la gestion des données relatives aux clients, fournisseurs et autres partenaires :**

Il est prescrit à FALCON SECURITY HUB de conserver les données traitées pendant une période de dix (10) ans, à compter de la fin de l'exercice au cours duquel les traitements ont été réalisés, conformément à l'article 24 de l'Acte Uniforme portant organisation et harmonisation des comptabilités des entreprises.

FALCON SECURITY HUB devra conserver également les pièces et documents relatifs aux opérations effectuées, y compris les livres de comptes et les correspondances commerciales, pendant dix (10) ans, après l'exécution de l'opération.

➢ **Concernant l'archivage électronique :**

Au regard du grand nombre de documents quotidiennement traités par les services, et afin d'optimiser le traitement de ces informations, il est prescrit à FALCON SECURITY HUB, de mettre en œuvre une politique globale de gestion électronique des documents (GED).

La gestion électronique des documents devra :

- obéir aux dispositions du décret n°2016-851 du 19 Octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique ;

- permettre de rendre plus efficace les processus et circuits d'information, notamment par des actions de collecte, de numérisation, de validation, de diffusion, de classement, d'indexation et d'archivage des documents.

Par ailleurs, il est prescrit à FALCON SECURITY HUB de sélectionner un prestataire de service d'archivage électronique afin de débuter le projet d'archivage électronique.

	➢ **Concernant l'archivage physique :** Il est prescrit à FALCON SECURITY HUB de procéder à un archivage physique des documents, conformément aux réglementations applicables et aux standards en matière de protection des données personnelles.	
La proportionnalité des données	➢ **Dans le cadre de la gestion du recrutement :** En application de l'article 21 de la loi relative à la protection des données à caractère personnel, il est prescrit à FALCON SECURITY HUB de ne pas collecter et traiter le casier judiciaire des agents collectés au moment du recrutement. ➢ **Dans le cadre de la gestion des données sensibles :** Il est prescrit à FALCON SECURITY HUB de limiter l'accès aux données de santé à une seule personne au sein de la société, qui assurera la transmission de ces données à l'assurance et lui fera signer, au besoin, un accord de confidentialité. Pour la gestion des données sensibles, il est prescrit à FALCON SECURITY HUB d'élaborer et de mettre en œuvre une politique de gestion des données sensibles. Dans ce cadre, elle devra : ○ faire l'inventaire des données sensibles traitées ; ○ analyser la proportionnalité des données sensibles traitées ; ○ épurer sa base de données des informations sensibles disproportionnées et conserver les données pertinentes ; ○ sécuriser les données sensibles traitées ; ○ définir les accès aux données sensibles ; ○ collecter strictement les données nécessaires aux finalités définies ; ○ procéder au recueil du consentement sur un formulaire distinct ; ○ réaliser une analyse d'impact relative à la protection des données (AIPD) pour le traitement des données biométriques, de géolocalisation et des données sensibles.	**30 jours**

La transparence du traitement	Il est prescrit à FALCON SECURITY HUB de faire preuve de transparence. La transparence requiert que les personnes concernées soient informées : - de l'identité du responsable du traitement et, le cas échéant, celle de son représentant dûment mandaté ; - de la finalité du traitement ; - des catégories de données concernées ; - des destinataires auxquels les données sont susceptibles d'être communiquées ; - de l'existence et des modalités d'exercice de leurs droits d'accès et de rectification ; - de la durée de conservation des données ; - de l'éventualité de tout transfert de données à destination de pays tiers. FALCON SECURITY HUB le fera par le biais : - de mentions légales, de politique de confidentialité, de politique de gestion des cookies élaborées et rendues disponibles sur son site internet ; - de mentions légales et de politique de confidentialité sur ses formulaires, les contrats, les listes de présences et les appels à candidature ; - de mentions légales, de politique de confidentialité d'affiches dans tous les lieux où elle opère des traitements de données à caractère personnel ; - de messages véhiculés par voie de presse, et en langues locales, par le canal de la Radio nationale et des radios de proximité.	**90 jours**
Le système informatique	Il est prescrit à FALCON SECURITY HUB la mise en œuvre des mesures suivantes : - Mise en place d'un système de gestion des journaux centralisé (SIEM) des accès au système d'information pour surveiller et analyser les événements en temps réel ; - Établir une politique de gestion des habilitations avec des profils d'accès adaptés aux besoins actuels de l'entreprise, et mettre à jour régulièrement ces habilitations pour éviter les autorisations obsolètes ;	**90 jours**

	- Mettre en place un audit périodique des habilitations pour détecter les anomalies ou permissions inutiles ; - Élaborer une procédure de notification des personnes concernées en cas de violation de données ou d'accès frauduleux, afin de garantir une réponse rapide et conforme aux obligations légales ; - Mettre en place un chiffrement des données sensibles, à la fois pour les données au repos et les données en transit, afin de protéger les informations confidentielles contre toute interception ou accès non autorisé ; - Implémenter des mesures de verrouillage des ports USB sur les postes de travail pour limiter l'utilisation de supports externes non autorisés ; - Sensibiliser les utilisateurs à la création de mots de passe robustes et à l'usage d'un gestionnaire de mots de passe ; - Utiliser un proxy filtrant pour surveiller les connexions Internet et permettre un déblocage uniquement sur demande justifiée ; - Mettre en place une analyse de risques dédiée à la sécurité des données personnelles ; - Rédiger et diffuser une charte informatique à l'ensemble du personnel, détaillant les pratiques de sécurité, les responsabilités, et les comportements à adopter ; - Rédiger une charte informatique claire et exhaustive, qui sera diffusée à l'ensemble du personnel. Cette charte devra inclure : o Les bonnes pratiques de sécurité informatique à adopter ; o Les responsabilités individuelles en matière de protection des données et des systèmes ; o Les comportements à éviter (e.g., partage de mots de passe, accès non autorisé) ; o Etc ; - Remplacer l'utilisation des données biométriques pour l'accès aux zones sensibles par des alternatives conformes aux principes de respect de la vie privée, telles que des contrôles d'accès basés sur des	

	identifiants et des mots de passe sécurisés ou des badges électroniques personnalisés. Ces dispositifs pourront être renforcés par l'installation d'un système de vidéosurveillance, tout en veillant à respecter les réglementations en matière de protection des données personnelles ; - Réduire le délai de verrouillage automatique à 5 minutes pour améliorer la sécurité des sessions utilisateur ; - Mettre à jour régulièrement le logiciel VPN utilisé pour pallier d'éventuelles vulnérabilités ; - Élaborer un plan de continuité d'activité et une politique de sauvegarde pour assurer la disponibilité des données et des systèmes en cas de sinistre ou d'incident majeur ; - Mettre en place un Plan de Reprise et de Continuité d'Activité (PCA/PRC) pour assurer la résilience de ses opérations en cas d'incident majeur ; - Effectuer des audits de sécurité réguliers pour identifier les vulnérabilités et évaluer l'efficacité des mesures de protection mises en place.	
Les destinataires des données traitées	Il est prescrit à FALCON SECURITY HUB : - de communiquer les données traitées uniquement aux destinataires habilités ; - en cas de transferts, d'entamer auprès de l'Autorité de Protection, les démarches en vue d'obtenir les autorisations requises pour les autres transferts de données qu'elle opère ; - d'effectuer des transferts de données personnelles uniquement vers des pays qui assurent un niveau de protection au moins équivalent à celui de la Côte d'Ivoire. Le pays de destination doit au minimum, disposer d'une loi relative à la protection des données personnelles et d'une Autorité de Protection.	**30 jours**
Exactitude des données	Il est prescrit à FALCON SECURITY HUB de mettre en place une politique globale d'actualisation des données.	**12 mois**

Les sous-traitants	➢ **Dans le cadre de ses relations avec les sous-traitants** : FALCON SECURITY HUB est amenée à procéder à des échanges de fichiers contenant des données à caractère personnel avec des tiers. Elle est donc tenue : - d'inclure des clauses relatives à la protection des données à caractère personnel dans les contrats qui les lient ; - de contracter uniquement avec des sous-traitants capables d'apporter des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer. Il incombe à FALCON SECURITY HUB et à ses sous-traitants, de veiller au respect de ces mesures. ➢ **Dans le cadre de ses relations avec ses clients, en sa qualité de sous-traitants :** - d'inclure dans les contrats clients, des clauses spécifiques en matière de données personnelles ; - de recommander à ses clients de se mettre en conformité avec la loi ivoirienne sur la protection des données personnelles ; - de signer au besoin, un accord de confidentialité des données (NDA) afin d'assurer la sécurité et la confidentialité des données.	**12 mois**
Le correspondant à la protection	Il est prescrit à FALCON SECURITY HUB : - de désigner un correspondant à la protection des données personnelles et de faire valider cette désignation par l'autorité de protection ; - de mettre à la disposition du correspondant, les ressources et les moyens nécessaires afin de mener à bien sa mission ; - de préparer un plan pluriannuel de formation en matière de protection des données personnelles ;	**30 jours**

	- d'informer régulièrement l'ensemble de son personnel des missions et des actions du correspondant à la protection.	
Les droits d'accès, de rectification, d'effacement et d'opposition.	Il est prescrit à FALCON SECURITY HUB : - d'élaborer une politique spécifiquement liée à la gestion des droits des personnes concernées, et une procédure de réponse aux demandes d'exercice de droit ; - de communiquer aux personnes concernées, les contacts du correspondant à la protection, auprès duquel celles-ci pourront exercer leurs droits d'accès, de rectification, d'effacement et d'opposition.	**30 jours**
La formation du personnel	Il est prescrit à FALCON SECURITY HUB : - de mettre en place une politique de formation et de sensibilisation de l'ensemble de son personnel sur la protection des données à caractère personnel ; - de mettre à la disposition du personnel, des outils pédagogiques relatifs à la protection des données à caractère personnel comme : o des guides individuels pour les différentes catégories d'acteurs ; o des sessions de formation inscrites au catalogue de la DRH ; o la sensibilisation de l'ensemble du personnel ; o des modules d'apprentissage en ligne (« e-learning ») ; o la formation du correspondant à la protection et des chargés de protection des données personnelles, sanctionnée par un certificat. - d'inscrire la formation du personnel en matière de protection des données au calendrier annuel de formation.	**90 jours**

Les procédures	Il est prescrit à FALCON SECURITY HUB : - de développer une stratégie de protection des données personnelles conforme aux réalités locales et aux exigences réglementaires nationales ; - d'élaborer une charte PDCP et de la diffuser à l'ensemble du personnel ; - d'élaborer une procédure de gestion des droits des personnes concernées ; - d'insérer des clauses de recueil du consentement et de transparence dans ses procédures ; - d'élaborer une politique de conservation des données ; - d'élaborer une procédure d'archivage physique et électronique ; - d'adopter une procédure de notification des violations et incidents en matière de protection des données personnelles ; - d'élaborer une politique de gestion des données sensibles ; - d'élaborer une cartographie des risques et d'y intégrer les risques liés à la protection des données personnelles ; - d'élaborer une politique de gestion des cookies et une politique de confidentialité pour le site internet ; - d'élaborer une procédure d'actualisation des données ; - d'élaborer une procédure de contrôle d'accès des locaux ; - d'élaborer une procédure spécifique pour l'encadrement des relations avec les sous-traitants.	**120 jours**

La géolocalisation	Il est prescrit à FALCON SECURITY HUB : - **Dans le cadre de la gestion de la géolocalisation des véhicules utilisés par les agents :** - d'informer les personnes concernées de la présence de dispositifs de géolocalisation dans les véhicules ; - de désactiver les dispositifs de géolocalisation en dehors des heures de travail. Le dispositif de géolocalisation installé dans les véhicules mis à la disposition du personnel ne doit pas être utilisé : ○ pour contrôler l'employé en permanence ; ○ pour suivre les déplacements des représentants du personnel et des délégués syndicaux dans le cadre de leur mandat ; ○ pour collecter la localisation en dehors du temps de travail (trajet domicile-travail, temps de pause, etc.) ; ○ pour calculer le temps de travail des employés alors qu'un autre dispositif existe déjà. FALCON SECURITY HUB devra donc désactiver les dispositifs de géolocalisation en dehors des heures de travail. ➢ **Dans le cadre de la gestion des prestations auprès des clients :** ○ d'insérer dans les contrats, des clauses spécifiques relatives à la protection des données à caractère personnel ; ○ de signer au besoin, un accord de non-divulgation afin de garantir la confidentialité des données. Par ailleurs, il est prescrit à FALCON SECURITY HUB de réaliser une analyse d'impact relative à la protection des données (AIPD) pour tous traitements effectués impliquant la géolocalisation.	**90 jours**

La biométrie	Il est prescrit à FALCON SECURITY HUB de (d') : ➢ **Dans le cadre de la gestion de la biométrie utilisée par les agents :** - cesser l'utilisation de l'empreinte dans l'optique de contrôler la présence des employés au sein des locaux de la société ; - utiliser des matériels biométriques sans base de données ; - faire des formations sur l'usage de la biométrie ; - soumettre à l'ARTCI une analyse d'impact (AIPD) préalablement à tout traitement des données biométriques ; - inclure dans la cartographie des risques les éléments et risques liés à la protection des données à caractère personnel. ➢ **Dans le cadre de la gestion des prestations auprès des clients :** - d'insérer dans les contrats des clauses spécifiques relatives à la protection des données à caractère personnel ; - de signer au besoin, un accord de non-divulgation afin de garantir la confidentialité des données. ➢ **Concernant les durées de conservation des données biométriques** Il est prescrit à FALCON SECURITY HUB supprimer les données d'identification biométrique autres que les gabarits biométriques au plus tard dans les six (6) mois qui suivent : - la date de retrait des habilitations ; - ou la date de la cessation des fonctions de la personne concernée au sein de FALCON SECURITY HUB ; - ou la date de retrait des habilitations pour le compte de la personne physique ou morale ayant qualité d'employeur.	**30 jours**

La vidéosurveillance	➢ **Dans le cadre de la vidéosurveillance interne et de l'installation de la vidéosurveillance pour le compte de ses clients :** Il est prescrit à FALCON SECURITY HUB : ○ de requérir l'accord du personnel pour la mise en place du dispositif de vidéosurveillance ; ○ d'informer les personnes concernées de l'existence d'un dispositif de vidéosurveillance. Elle le fera au moyen d'affiches placées à hauteur de vue dans les zones filmées par les caméras, et des pictogrammes placés de façon visible, aux entrées et aux sorties des locaux sous surveillance. Les affiches et pictogrammes doivent indiquer, d'une façon claire et visible, les informations suivantes : - le nom du responsable du traitement ; - le fait que l'établissement est placé sous vidéosurveillance ; - la finalité du dispositif (sécurité des biens et personnes) ; - les coordonnées du contact pour l'exercice, par les personnes concernées, des droits d'accès, de rectification et d'opposition ; - le numéro d'autorisation octroyé par l'Autorité de Protection. ○ veiller à ce que les caméras qui filment les zones de circulation ne portent pas atteinte à la vie privée des personnes concernées ; ○ éviter de diriger les caméras de vidéosurveillance dans les toilettes, les lieux de pause, ou de repas, de repos des employés ; ○ réaliser une analyse d'impact relative à la protection des données (AIPD). ➢ **Concernant les durées de conservation des images de vidéosurveillance :**	**30 jours**

	Il est prescrit à FALCON SECURITY HUB, de conserver les données collectées pendant une période de trente (30) jours. En cas d'incidents, les données collectées doivent être conservées pendant une période d'un (1) an, à compter de la dernière sauvegarde mensuelle. En cas de litige, les données pourront être conservées jusqu'au règlement définitif du litige.	

Fait à Abidjan, le 18 Février 2025

Le Président

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

PROJET DE FACTURE (FALCON SECURITY HUB)

FALCON SECURITY HUB
Marcory zone 4C
Rue Thomas Edison
Tél. : 27 21 35 13 88

DESIGNATION	NOMBRE	COUT UNITAIRE	MONTANT
Frais de dépôt de dossiers de demande d'autorisation de traitements de données à caractère personnel pour les finalités suivantes : 1. Gestion de la géolocalisation pour le compte des clients 2. Gestion de la géolocalisation interne 3. Gestion des activités financières des clients 4. Gestion de la formation des agents 5. Gestion commerciale 6. Sécurité des biens et des personnes au sein des locaux (Vidéosurveillance en interne) 7. Gestion de la vidéosurveillance pour le compte des clients 8. Gestion du système d'information 9. Gestion de la biométrie interne 10. Gestion de l'installation de la biométrie pour le compte des clients 11. Gestion des ressources humaines 12. Gestion de la paie 13. Gestion de la relation client 14. Gestion du site internet	14	200 000	2.800.000
TOTAL			2.800.000

Arrêtée la présente facture à la somme de : **Deux Millions Huit Cent Mille Francs CFA HT**

NB : *Veuillez payer par chèque ou par virement bancaire à l'ordre de :*

ARTCI ou Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire
Ecobank : CI0590100113122488700182

Fait à Abidjan, le 18 Février 2025
Le Président

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

Autorité de Régulation des Télécommunications / TIC de Côte d'Ivoire * ARTCI * Le Président