République du Sénégal
Un Peuple- Un But- Une Foi

Présidence de la République

COMMISSION DE PROTECTION DES DONNEES PERSONNELLES (CDP)

COMMISSION DE PROTECTION DES DONNÉES PERSONNELLES

REFERENTIEL DE CONTROLE

Guide pour les entreprises du secteur privé et public relatif aux traitements de données à caractère personnel dans le cadre de l'exécution des missions de contrôle

Edition 2022

Table des matières

Liste des sigles et abréviations

CDP : Commission de protection des Données Personnelles

DAJC : Direction des Affaires Juridiques et de la Coopération

DTIC : Direction de la Technologie, de l'Innovation et du Contrôle

DAF : Direction Administrative et Financière

DP : Données Personnelles

PDP : Protection des Données Personnelles

PV : Procès-Verbal

SI : Système d'Information

SP : Session Plénière

Introduction

La Commission de protection des Données Personnelles (CDP) est une autorité administrative indépendante créée par la loi n°2008-12 du 25 janvier 2008. Elle est chargée de vérifier la légalité de la collecte et du traitement des données personnelles des citoyens sénégalais et de s'assurer que toutes les précautions sont prises pour qu'elles soient sécurisées.

Relativement à ses missions, la CDP supervise l'application de la loi par les responsables de traitement, notamment par la vérification a priori, et a posteriori, des traitements de données à caractère personnel mis en œuvre.

A ce titre, la CDP est dotée d'un pouvoir de contrôle lui permettant de vérifier l'application concrète de la loi n°2008-12 et de ses textes d'application sur la protection des données personnelles. A cet effet, ses agents peuvent accéder directement à tous les éléments intervenant dans les processus de collecte et de traitement des données personnelles (les systèmes, les applications, les équipements, les locaux, les supports d'information...) afin d'en vérifier la conformité.

Ces contrôles peuvent donner lieu à des sanctions administratives, pécuniaires ou pénales.

Dès lors, le présent référentiel a été développé par la commission à l'intention des organismes privés et publics. Il explique en détail le processus d'exécution des missions de contrôle de la CDP. En outre, le présent guide met l'accent sur la manière de réguler certains types de traitements (vidéosurveillance, géolocalisation, etc…). L'objectif étant de fournir aux organismes privés et publics, un outil d'aide à la mise en conformité pour les traitements de données à caractère personnel afin d'assurer le bon déroulement des missions de contrôle.

Quelques rappels utiles

Une donnée personnelle (DP)

Il s'agit, au sens de la loi, de toute donnée permettant d'identifier une personne physique de manière directe (nom, prénom, photo), ou indirecte (adresse postale, adresse e-mail, numéro de téléphone, adresse IP, enregistrement vocal, etc…).

Un traitement de données personnelles

Il s'agit de toute opération ou ensemble d'opérations (collecte, enregistrement, exploitation, consultation, conservation, sauvegarde, extraction, transfert, partage, suppression, archivage…) portant sur des données à caractère personnel, que le procédé utilisé soit automatisé ou non, et indépendamment du volume de données traitées.

Le responsable de traitement

C'est la personne, l'autorité publique, le service ou encore l'organisme qui, seul ou avec d'autres, prend la décision de collecter des données personnelles et en détermine les finalités et les moyens.

Le responsable de traitement N'EST PAS le propriétaire des données collectées.

Le sous-traitant

C'est la personne physique ou morale, publique ou privée, tout service ou toute association qui traite des données personnelles pour le compte d'un responsable de traitement.

1. Le pouvoir de contrôle de la CDP

La CDP dispose, aux termes de l'article 25 de la loi n° 2008-12 du 25 janvier 2008, d'un pouvoir de contrôle sur tout traitement de données à caractère personnel.

Les missions de contrôle permettent à la CDP de vérifier l'application des dispositions de la loi précitée et de s'assurer que le traitement mis en œuvre ne porte pas atteinte aux droits et libertés des personnes dont les données personnelles sont traitées. Elles ont également comme objectif de s'assurer que les déclarations et/ou demandes d'autorisation faites par les responsables de traitement auprès de la CDP, et pour lesquelles ils ont reçu des récépissés ou des autorisations, sont toujours conformes à leurs pratiques quotidiennes.

Lors d'un contrôle, la CDP s'intéresse notamment :

- A l'identité du responsable de traitement ;
- A la finalité de la collecte ;
- Aux personnes concernées par la collecte ;
- Aux catégories des données collectées ;
- A l'origine des données collectées ;
- A la durée de conservation des données collectées ;
- Au lieu de stockage des données collectées ;
- Aux mesures de sécurité mises en œuvre pour la préservation des données collectées ;
- Aux transferts de données personnelles (s'il y a lieu).

1.1. Le cadre légal

Les articles 25 à 28 de la loi n° 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel, les articles 12 à 19 du décret n° 2008-721 du 30 juin 2008 portant application de la loi précitée et les articles 17 à 22 du Règlement intérieur de la CDP encadrent les missions de contrôle de la CDP.

L'entrave à l'action de la CDP, et particulièrement à ses opérations de contrôle sur site ou sur convocation, est sanctionnée par l'article 431-28 de la loi n°2016-29 du 08 novembre 2016 modifiant le Code pénal (431-31 de la loi n° 2008-11 du 25 janvier 2008).

1.2. Les organismes contrôlables par la CDP

La CDP a le pouvoir d'effectuer des contrôles auprès de l'ensemble des organismes privés et publics qui traitent des données à caractère personnel.

Ce contrôle de la CDP concerne ainsi les entreprises privées, les associations ainsi que les organismes publics ayant un établissement au Sénégal ou traitant des informations personnelles d'individus résidant sur le territoire national.

1.3. Les différentes formes de contrôle

La CDP peut contrôler le respect de l'application de la loi n° 2008-12 du 25 janvier 2008 de quatre façons : en se déplaçant sur site, en effectuant un contrôle en ligne, en évaluant la conformité via un questionnaire, ou en convoquant une audition.

Le contrôle sur site

La CDP peut décider de se rendre directement sur les lieux du traitement des données d'un responsable de traitement afin de mener ses investigations.

Dans ce cas, les membres et agents assermentés de la commission ont accès, dans les conditions prévues par l'article 45 et suivants du Code de Procédure Pénale, pour l'exercice de leurs missions, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement des données à caractère personnel et qui sont à usage professionnel, à l'exclusion des parties de ceux-ci affectées au domicile privé.

Le contrôle en ligne

Depuis ses locaux, la CDP a la possibilité de faire des vérifications en consultant les données collectées par le responsable de traitement en ligne. La commission se limitera, dès lors, au contrôle de ce qui est accessible « librement ». Le contrôle peut porter, par exemple, sur la présence de cookies et de traceurs placés sur le site internet, s'assurer que le consentement de l'utilisateur est recueilli pour toute collecte de ses données ou encore, vérifier que la sécurité du site est robuste afin que les données des utilisateurs ne puissent pas être accessibles facilement par un tiers.

Ce type de contrôle consiste également pour les sites de commerce électronique, à vérifier les Conditions Générales de Ventes (CGV) ou d'Utilisation (CGU) ainsi que les mentions légales.

Le contrôle sur pièces

Ce contrôle consiste à envoyer un questionnaire d'évaluation de conformité au responsable de traitement visé. Ce dernier devra ensuite communiquer à la CDP ses réponses dans un délai déterminé en y joignant tout document utile permettant de les justifier.

L'audition

Le contrôle par audition s'effectue après convocation du responsable de traitement dans les locaux de la CDP. Lors de cette convocation, le responsable de traitement, et/ou ses représentants, sera tenu de répondre à des questions portant sur le(s) traitement(s) faisant l'objet des vérifications et, le cas échéant, rendre possible un accès aux ressources de l'organisme.

Dans la suite du document, nous aborderons en détail la procédure de contrôle sur site qui est, aujourd'hui, l'un des contrôles les plus utilisés par la CDP pour vérifier la conformité des responsables de traitement. A noter aussi, que ce document sera régulièrement modifié pour intégrer de nouvelles mises à jour.

2. Les missions de contrôle sur site

2.1. Définition et objectif d'une mission de contrôle sur site

Définition :

Le contrôle sur site consiste en des opérations d'enquête et d'investigations effectuées dans les locaux du responsable de traitement après la mise en œuvre d'un traitement de données à caractère personnel.

Objectif :

S'assurer que les pratiques quotidiennes du responsable de traitement sont conformes à la déclaration ou demande d'autorisation faite auprès de la CDP.

2.2. Décision de contrôle

Les missions de contrôles initiées par la CDP se font le plus souvent :

- Dans le cadre du programme annuel de contrôle : tous les ans, la CDP élabore un programme annuel de contrôle en fonction des sujets d'actualité (Vidéosurveillance, Géolocalisation, Intelligence artificielle, …) ou des projets à forte valeur ajoutée pouvant impacter considérablement la vie privée de nombreux concitoyens (État Civil, Identité Numérique…).

- A la suite d'une plainte ou d'un signalement : le service contentieux de la CDP reçoit régulièrement des plaintes et signalements concernant des abus sur le non-respect de la vie privée. Des contrôles peuvent ainsi être effectués pour vérifier la conformité des responsables de traitements et s'assurer du respect des droits des personnes.

- Sur demande de la Session plénière concernant un dossier en instruction : en raison de la complexité de certains dossiers instruits en session plénière, il peut être décidé d'effectuer un contrôle approfondi du traitement qui est fait des données afin d'en vérifier la conformité.

- Sur demande d'une autorité de protection (coopération internationale) : des opérations de contrôle peuvent être initiées au regard de la coopération entre certaines autorités de protection. Cette coopération contribue à une meilleure protection des personnes qui sont de plus en plus concernées par des traitements de données effectuées dans plusieurs pays, au vu du caractère transnational des nouvelles technologies.

- À la suite de la clôture d'un contrôle, d'une mise en demeure ou d'une sanction : des investigations peuvent être menées à la suite d'une procédure de contrôle clôturée, d'une mise en demeure ou d'une sanction, notamment pour vérifier que les mesures de mise en conformité ont bien été adoptées par l'organisme contrôlé.

2.3. Les acteurs du contrôle

Les personnes qui interviennent dans les missions de contrôle sont assermentées et sont tenues par un engagement de confidentialité.

Il s'agit principalement :

- des commissaires contrôleurs, au nombre de trois (03), désignés parmi les membres de la Session plénière ;
- des agents de la CDP habilités ;
- des experts choisis par la Présidente de la Commission pour certaines missions nécessitant une expertise particulière (exemple : contrôle sur les données de santé).

2.4. Le déroulement d'une mission de contrôle sur site

2.4.1. Avant la mission

<u>Étape 1 : Préparation des documents officiels</u>

- Décision de la mission de contrôle validée par la Session Plénière et signée par la Présidente de la CDP

Dans la décision, il est fait mention du nom et de l'adresse du responsable de traitement, du nom des commissaires et des agents contrôleurs chargés de l'opération, de l'objet ainsi que de la durée de l'opération.

- Ordres de missions des commissaires et agents contrôleurs

Les ordres de mission sont préparés par la DAF et signés par la Présidente en précisant le nom, la fonction des commissaires et agents contrôleurs chargés de l'opération, le nom et l'adresse du responsable de traitement, l'objet de la mission, la durée de l'opération et, s'il y a lieu, le moyen de transport utilisé.

- Lettre d'information au Procureur de la République signée par la Présidente de la CDP

Le Procureur de la République territorialement compétent est informé vingt-quatre (24) heures avant toute mission de contrôle. Il est précisé dans le courrier rédigé par la DTIC la date, le lieu, le nom du responsable de traitement, l'heure et l'objet du contrôle.

- Lettre d'information au responsable du traitement s'il ne s'agit pas d'une mission inopinée

Le responsable de traitement est informé de la date, de l'heure et de l'objet du contrôle afin qu'il prenne toutes les dispositions nécessaires pour le bon déroulement de la mission (contrairement aux contrôles inopinés où le responsable de traitement n'est pas informé). Ce courrier est également préparé par la DTIC.

- Lettre de notification du droit d'opposition

La notification du droit d'opposition est préparée par la DTIC. Cette notification permet au responsable de traitement de s'opposer au contrôle s'il le souhaite, conformément à la loi.

- Canevas du procès-verbal

Pour une meilleure organisation de la mission de contrôle, les agents contrôleurs préparent en amont le canevas du procès-verbal à renseigner à la fin de la mission.

<u>Étape 2 : Préparation de la mission de contrôle</u>

- Exploitation du dossier de l'organisme si le traitement a déjà été déclaré à la CDP
- Recueil d'informations sur l'organisme à contrôler

La collecte d'informations peut se faire via le site internet de l'organisme, la presse, les déclarations effectuées auprès de la CDP…

- Collecte des « outils » de travail du contrôleur

Un papier et un stylo pour les prises de note

Un ordinateur portable (il ne doit pas être connecté au réseau de l'organisme contrôlé)

Une clé USB pour le recueil des copies de documents numériques

Un appareil photo (ou téléphone portable)

- Identification des rôles de chaque agent contrôleur

Pour une meilleure organisation de la mission de contrôle, il est préférable d'identifier, en amont, le rôle de chaque agent contrôleur : le chef de la délégation (commissaire), l'agent en charge des entretiens juridiques (DAJC), l'agent en charge des entretiens techniques (DTIC), l'agent en charge de la collecte des informations (photos, prises de note, copie des documents…).

2.4.2. Pendant la mission

Étape 1 : Présentation des agents à l'accueil de l'organisme contrôlé

- Déclinaison des identités des contrôleurs en présentant leurs cartes professionnelles
- Demande de rencontre du responsable de traitement (ou de la personne désignée par le responsable de traitement)

NB : A cette étape, il n'est pas nécessaire de divulguer l'objet du contrôle.

Étape 2 : Entretien avec le responsable de traitement et / ou ses représentants

- Identification du responsable de traitement
- Bref rappel des attributions de la CDP (rôle, statut, missions)
- Présentation du Comité de contrôle (identité et qualité des contrôleurs)
- Présentation de l'objet de la mission
- Remise des documents officiels (décision signée, ordre de mission)
- Notification au responsable du traitement de son droit d'opposition à la tenue de la mission

1er cas : Refus du contrôle par le responsable de traitement

Le responsable de traitement peut s'opposer à la mission de contrôle pour les motifs qui lui appartiennent. Dans ce cas, un procès-verbal de carence est établi (à faire signer au responsable de traitement dans la mesure du possible) et la mission de contrôle n'aura pas lieu.

En application de l'article 26 de la loi 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel, *le Président de la CDP saisit, en cas d'opposition du responsable des lieux, le Président du Tribunal Régional dans la juridiction de laquelle sont situés les locaux à visiter, ou du juge délégué par lui, afin d'obtenir une autorisation ».*

Le président du Tribunal Régional qui est saisi statue par ordonnance motivée.

Le courrier de saisine du Président du Tribunal Régional est préparé par la DAJC et signé par le Président. Si l'ordonnance du juge est favorable à la poursuite de la mission de contrôle, la mission se poursuivra un autre jour.

2e cas : Acceptation du contrôle par le responsable de traitement

Au cas où le responsable des lieux ne s'y oppose pas, la mission de contrôle peut débuter.

Étape 3 : Le contrôle proprement dit

- Entretiens avec le responsable de traitement, les salariés ainsi que toute personne susceptible de nous apporter des éclaircissements par rapport à la mission de contrôle.

Ces entretiens permettent de recueillir des éléments d'information relatifs à l'organisme contrôlé et aux traitements mis en œuvre (activités, forme et structure juridique de l'organisme, nombre de salariés, nombre de clients, nombre de partenaires, nombre de sous-traitants, fonctionnement du service, traitements, architecture des systèmes d'informations, implantation géographique pour vérifier les flux transfrontaliers, caméras de surveillance, etc.)

- Vérifications et recueil des éléments de preuve

La priorité d'une mission de contrôle reste la collecte d'un maximum d'informations techniques et juridiques permettant d'apprécier la conformité des traitements mis en œuvre avec la loi sur la protection des données personnelles :

- ***Investigations sur les postes de travail*** *(modalités d'accès aux fichiers, recherche de fichiers par mot clé, les zones de commentaires dans les applications, etc.) ;*

- ***Vérification de la sécurité des systèmes d'information*** *(Documents et procédures, Partage réseau, paramétrage des droits d'accès sur les répertoires, logiciels de prise de main à distance, tâches d'administration, sécurité des postes nomades, etc.) ;*
- ***Vérification de la durée de conservations des données*** *(procédure de purge automatique, vérification dans le système / l'application directement, etc.) ;*
- ***Investigation d'un système de vidéosurveillance*** *(plan d'installation, affiches, durée de conservation des images, modalités d'exercice des droits des personnes, mesures de sécurité) ;*
- ***Audition du personnel*** *(toujours présenter son identité et indiquer l'objet de sa présence).*

Les membres de la Commission des Données Personnelles et les agents mentionnés à l'article 25 de la loi 2008-12 portant sur la protection des données à caractère personnel peuvent demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie. Ils peuvent recueillir, sur place ou sur convocation, tout renseignement et toute justification utiles dans le cadre de la mission. Ils peuvent accéder aux programmes informatiques et aux données, demander la transcription de tout traitement dans des documents appropriés directement utilisables pour les besoins du contrôle. Ils peuvent être assistés par des experts choisis par la Commission des Données Personnelles.

Cette phase permet de confirmer les informations recueillies lors des entretiens avec le responsable de traitement et d'effectuer des constatations.

- Rédaction du procès-verbal (PV)

A l'issue de la phase de vérification, un procès-verbal est dressé. Celui-ci rend compte, de manière factuelle, de l'ensemble des informations qui ont été communiquées aux agents contrôleurs et des constatations qu'ils ont opérées.

Le procès-verbal est une pièce centrale dans la constitution d'un dossier de sanction : il contient, dans son corps ou ses annexes, les éléments de preuve permettant de rapporter le cas échéant les manquements à la loi n° 2008-12 constatés.

Le procès-verbal doit énoncer :

- *l'objet de la mission, la nature, le jour, l'heure et le lieu des vérifications ou des contrôles effectués, les agents présents et la qualité des personnes rencontrées ;*
- *les déclarations des personnes et les demandes formulées par les agents ;*
- *l'inventaire des documents dont une copie a été prise durant la mission de contrôle (en annexe du PV) ;*

- *toute invocation du secret professionnel et le cas échéant, les dispositions législatives ou règlementaires auxquelles la personne invoquant ce secret s'est référée ainsi que la nature des données que cette personne considère comme couvertes par ce secret ;*
- *les difficultés éventuelles rencontrées et les motifs qui ont empêché ou entravé le déroulement de la mission ;*
- *les compléments de documents demandés (contrats, extractions de bases de données, etc.) devant être adressés à la CDP dans un délai imparti de 48h.*

Le procès-verbal est signé (après relecture) de manière contradictoire par :

- *les agents chargées du contrôle et qui y ont procédé ;*
- *le responsable de traitement (ou toute personne désignée par celui-ci).*

En cas de refus ou d'absence de celles-ci, mention en est portée au procès-verbal.

Le procès-verbal est notifié au responsable des lieux et au responsable des traitements.

Si la visite a eu lieu avec l'autorisation et sous le contrôle du juge, la copie du procès-verbal est adressée au juge par la Présidente de la CDP.

2.4.3. Après la mission de contrôle

Étape 1 : Étude du procès-verbal et des documents issus de la mission de contrôle

- Exploitation du procès-verbal et des éléments de preuve recueillis lors de la mission de contrôle par la DAJC et la DTIC

Objectifs :

- ⇨ *Apprécier la conformité du traitement*
- ⇨ *Relever des manquements à la loi*

Au-delà des spécificités de chaque contrôle, les manquements constatés très souvent sont :

- ⇨ *Surveillance des salariés de manière permanente à l'aide de caméras installées sur les lieux de travail ;*
- ⇨ *Absence ou détournement de finalité de traitement, non pertinence ou caractère excessif des données ;*
- ⇨ *Absence de durée de conservation ou durée de conservation inadéquate avec la finalité ;*
- ⇨ *Défaut d'information des personnes sur la collecte de leurs données ;*

- ⇨ *Modalités d'exercice des droits des personnes concernées (droits d'accès, d'opposition, de rectification et de suppression) non formalisées*
- ⇨ *Défauts de sécurité et de confidentialité des données.*

Étape 2 : État des lieux sur les principales constatations, formulations de recommandations et conclusions

- L'exploitation du procès-verbal et des documents issus de la mission fait ensuite l'objet d'un compte-rendu juridique et technique décrivant la méthode utilisée pour relever chaque manquement.
- A l'issu de ce compte-rendu, la DAJC et la DTIC formulent des recommandations en fonction des manquements relevés.
- Ce compte rendu sera ensuite transmis aux commissaires contrôleurs et experts ayant participé à la mission pour relecture, amendements et suite à donner au contrôle.

Étape 3 : Transmission des conclusions de la mission de contrôle à la Présidente et la Session Plénière pour appréciation

- Présentation par le Comité de contrôle à la Session plénière des conclusions de la mission.

Étape 4 : Verdict

- Traitement conforme : une lettre de clôture du contrôle est envoyée au Responsable de traitement.
- Traitement non conforme : transmission du dossier au Comité de sanction pour décision (avertissement, mise en demeure, injonction de cesser le traitement, amende pécuniaire).

2.5. Les sanctions de la CDP en cas de manquement

En application des articles 29 et suivants de la loi n°2008-12 précitée et suite à un traitement non conforme, la CDP peut prononcer des mesures suivant le niveau de gravité des manquements relevés :

1) un avertissement à l'égard du responsable du traitement ne respectant pas les obligations découlant de la présente loi.

2) une mise en demeure de faire cesser les manquements concernés dans le délai qu'elle fixe.

Si le responsable du traitement ne se conforme pas à la mise en demeure qui lui a été adressée, la CDP peut prononcer à son encontre, après procédure contradictoire, les sanctions suivantes :

1) un retrait provisoire de l'autorisation accordée pour une durée de trois (3) mois à l'expiration de laquelle, le retrait devient définitif ;

2) une amende pécuniaire d'un (1) million à cent (100) millions de Francs CFA ;

Le recouvrement des pénalités se fait conformément à la législation relative au recouvrement des créances de l'État.

3. Référentiel relatif aux traitements de données à caractère personnel

3.1. Aux fins de traitement des données magnétiques et/ou biométriques (contrôle d'accès)

Définition	La biométrie permet d'identifier et d'authentifier une personne sur la base d'un ensemble de données reconnaissables et vérifiables, uniques et spécifiques à celles-ci. Les données biométriques relèvent soit de la physiologie de la personne (ADN, iris, empreinte digitale ou palmaire, rétine, reconnaissance faciale, géométrie du contour de la main ou du doigt, système et configuration des veines, etc.), soit de son comportement (voix, dynamique des frappes au clavier, dynamique de signature, l'écriture, etc.)
Catégories de personnes concernées	Les personnes concernées par le traitement sont : les salariés, les stagiaires, les intérimaires, les consultants, les prestataires, les conseillers, les visiteurs.
Catégories de données traitées	nom, prénom, photo, empreinte digitale, fonction, service, numéro du badge et date de validité, heures d'entrée et de sortie, en cas d'accès à un parking : numéro d'immatriculation du véhicule, numéro de place de stationnement.

Finalités du traitement	Les finalités visées sont notamment : - le contrôle des accès aux bâtiments, locaux et salles (informatique, archives) ; - la limitation des accès à certains endroits de l'entreprise ; - la gestion des horaires et du temps de présence des salariés ; - le contrôle d'accès des visiteurs.
Durée de conservation des données	- Les données personnelles relatives au système d'accès par badges magnétiques ou biométriques doivent être supprimées dès le départ du salarié. - Pour les badges visiteurs permettant de réidentifier la personne, les données peuvent être conservées 06 mois.
Droit des personnes	- **le droit à l'information préalable :** Les salariés sont informés du traitement de leurs données personnelles, notamment de l'identité du responsable du traitement, des finalités du traitement, des destinataires des données. Cette information doit être portée dans une clause du contrat de travail, dans le règlement intérieur de l'entreprise, ou dans un document écrit ou électronique remis au salarié lors de l'embauche. - **le droit d'accès :** L'employeur doit mettre en place toutes les mesures nécessaires pour permettre aux salariés d'accéder à leurs données personnelles. Les modalités d'exercice du droit d'accès doivent être précisées dans une note de service, dans le règlement intérieur de l'entreprise, ou dans un document écrit ou électronique remis au salarié lors de l'embauche. L'employeur communique les données demandées par les salariés dans un délai ne dépassant pas un (01) mois. - **le droit d'opposition :** Les salariés ont le droit de s'opposer aux traitements de leurs données personnelles ne répondant pas à une obligation légale de l'employeur, aux finalités visées et aux nécessités du service. Les modalités d'exercice du droit d'opposition doivent être précisées dans une note de service, dans le règlement intérieur de l'entreprise, ou dans un document écrit ou électronique remis au salarié lors de l'embauche. - **le droit de rectification et de suppression :** Les salariés ont le droit de demander que leurs données personnelles inexactes ou incomplètes soient rectifiées, complétées, mises à jour ou supprimées. Les modalités d'exercice du droit d'accès doivent être précisées dans une note de service, dans le règlement intérieur de l'entreprise, ou dans un document écrit ou électronique remis au salarié lors de l'embauche.
Sécurité des données	- Utiliser 2 doigts maximum pour relever les empreintes ;

	- Définir une politique de sécurité pour l'accès aux SI et une politique d'habilitation pour l'accès aux données biométriques ; - Prendre les mesures nécessaires pour éviter tout détournement de finalité ; - Éviter d'utiliser un élément biométrique comme un identifiant universel ou l'identification d'une personne à partir de plusieurs données biométriques ; - Chiffrer les données dès leur enrôlement ; - Sensibiliser les parties prenantes concernées.
Sous-traitant	Lorsque le responsable du traitement fait appel à un sous-traitant, notamment pour la confection des badges, l'installation et la maintenance du système, celui-ci doit assurer la sécurité et la confidentialité des données auxquelles il a accès. Le sous-traitant doit signer un engagement de confidentialité dans le cadre de sa mission. Le sous-traitant doit aussi accomplir ses formalités déclaratives auprès de la CDP pour être en conformité.

3.2. Aux fins de gestion du personnel

Définition	Les traitements visant à permettre la gestion du personnel, qu'ils soient mis en œuvre à partir d'outils internes ou externalisés auprès d'un prestataire de service, conduisent à collecter des données relatives à des personnes physiques (employés, salariés, stagiaires, etc.).
Catégories de personnes concernées	Les employés, les salariés, les stagiaires, les intérimaires, les consultants, les conseillers.
Catégories de données traitées	Les catégories de données pertinentes pour la gestion du personnel sont les suivantes : - noms, prénoms, sexe, date et lieu de naissance, adresse, numéro de téléphone personnel et professionnel, adresse électronique, situation matrimoniale, nombre d'enfants, nationalité, coordonnées personnelles, matricule interne, extrait casier judiciaire volet n°3 ; - noms, prénoms des enfants et époux ou épouse (s), nom et prénoms et numéro de téléphone de la personne à contacter en cas de besoin ; - statut de l'employé (salarié, intérimaire, stagiaire, consultant interne, conseiller) ;

	- les données relatives aux actes d'avancement ; - date et conditions d'embauche ou de recrutement, poste occupé, missions confiées, horaires de travail fixées ; - données de connexion enregistrées pour assurer le bon fonctionnement des applications et réseaux de l'organisme.
Destinataire des données	Les personnes et structures habilitées à recevoir les données collectées auprès du personnel sont : • les services de gestion des ressources humaines ; • les supérieurs hiérarchiques des employés concernés ; • les institutions sociales (l'IPRES, la CSS, IPM) ; • l'administration fiscale (la DGID) ; • la Direction générale de la Solde ; • l'Inspection du travail ; • les compagnies d'assurances contractantes. Les données peuvent être communiquées à tout autre organisme public légalement habilité.
Finalités du traitement	Les finalités visées sont : **II .1. La gestion administrative et financière et la gestion organisationnelle du travail :** La gestion administrative et financière et la gestion organisationnelles du travail peut comprendre : - la gestion des dossiers du personnel ; - la gestion des fiches de postes du personnel ; - la gestion administrative et financière du personnel(élaboration de contrat, congés, les salaires ou autres rémunérations, déclarations fiscales et sociales) ; - la gestion des agendas professionnels et des tâches à effectuer par le personnel autorisé ; - la gestion des réunions périodiques des départements ou services ; - la gestion des annuaires internes et organigrammes ; - la gestion des dotations individuelles en fourniture, d'équipements, de véhicules, de bons de carburants, d'achats et de restauration, de cartes de paiement, de crédit téléphonique. **II.2. La mise à la disposition des employés d'outils informatiques :** Le traitement de données personnelles des salariés à des fins de mise à disposition d'outils informatiques prend en compte :

	- l'installation, le suivi et la maintenance du parc informatique ; - la gestion de la messagerie électronique professionnelle ; - la gestion du dispositif intranet de l'organisme. **II.3. La formation et le suivi des carrières :** Le traitement de données personnelles à des fins de formation et de suivi des carrières des employés comprend notamment : - le traitement des demandes de formation ; - l'organisation des sessions de formation ; - le suivi des formations internes et externes du personnel ; - l'évaluation des formations et des connaissances ; - l'évaluation du personnel ; - la gestion de la mobilité professionnelle des employés ; - le suivi des affectations de postes ; - la mise à disposition et le détachement des agents ; - le changement de corps professionnel.
Durée de conservation des données	- Les données à caractère personnel ne peuvent être conservées au-delà de dix (10) ans après le départ de l'employé, sous réserve de dispositions particulières fixant une durée de conservation. - Pour les données de téléphonie, elles peuvent être conservées 06 mois, sous réserve du respect des dispositions relatives à la durée de conservation des pièces comptables (factures), qui est de 10 ans.
Droit des personnes	Les personnes employées dans les organismes publics et privés exercent leurs droits à l'égard du traitement de leurs données dans les conditions fixées par la loi n°2008-12 du 25 janvier 2008 portant protection des données en ses articles 58 et suivants. Ces droits sont : - **le droit à l'information préalable :** Les salariés sont informés du traitement de leurs données personnelles, notamment de l'identité du responsable du traitement, des finalités et des destinataires des données. Cette information doit être portée dans une clause du contrat de travail ou dans un document écrit ou électronique remis au salarié lors de l'embauche. - **le droit d'accès :**

	L'employeur doit mettre en place toutes les mesures nécessaires pour permettre aux salariés d'accéder à leurs données personnelles. Les modalités d'exercice du droit d'accès doivent être précisées dans une note de service ou dans un document écrit ou électronique remis au salarié lors de l'embauche. L'employeur communique les données demandées par les salariés dans un délai ne dépassant pas un (01) mois. - **le droit d'opposition :** Les salariés ont le droit de s'opposer aux traitements de leurs données personnelles ne répondant pas à une obligation légale de l'employeur ou à une nécessité de service. Les modalités d'exercice du droit d'opposition doivent être précisées dans une note de service ou dans un document écrit ou électronique remis au salarié lors de l'embauche. - **le droit de rectification et de suppression :** Les salariés ont le droit de demander que leurs données personnelles inexactes ou incomplètes soient rectifiées, complétées, mises à jour ou supprimées. Les modalités d'exercice du droit d'accès doivent être précisées dans une note de service ou dans un document écrit ou électronique remis au salarié lors de l'embauche.
Sécurité des données	- Définir une politique de sécurité pour l'accès aux SI et une politique d'habilitation pour l'accès aux données du personnel ; - Utiliser des coffres forts, armoires et tiroirs à clés dans les bureaux où sont stockées les dossiers du personnel ; - Prendre les mesures de sécurité nécessaires pour éviter tout détournement de finalité ; - Sensibiliser les parties prenantes concernées.
Sous-traitant	Lorsque l'employeur fait appel à un sous-traitant (cabinet comptable, fiscal et Ressources Humaines) pour l'externalisation de la gestion administrative et financière de son personnel, celui-ci doit présenter des garanties appropriées pour la sécurité et la confidentialité des données personnelles qu'il traite. Par ailleurs, le sous-traitant s'engage à traiter les données personnelles des salariés de façon confidentielle. Un engagement de confidentialité signé par le sous-traitant est consigné au contrat qui le lie à l'employeur.

3.3. Aux fins de vidéosurveillance

Définition	La vidéosurveillance est un système composé d'une ou plusieurs caméras installées à l'intérieur et/ou à l'extérieur d'un local, dans un espace public ou privé, pour surveiller en vue de capter des images et/ou des sons.
Lieux de travail	Locaux, bâtiments, salles, bureaux fermés, open space servant à l'exercice d'une activité professionnelle.
Fonctionnalités du système de vidéosurveillance	Les caractéristiques et fonctionnalités des systèmes de vidéosurveillance autorisés dans les lieux de travail sont : - visualisation en temps réel des images ; - enregistrement en continu, sur plage horaire ou sur détection de mouvement ; - accès aux images à distance ; - utilisation d'un enregistreur analogique ou numérique ; - utilisation de caméras fixes ou mobiles ; - suppression automatique ou manuelle des images.
Emplacement des caméras de surveillance	**Emplacements autorisés :** Les caméras peuvent être installés dans les zones suivantes : - les entrées et sorties du bâtiment à condition qu'elles ne filment pas la voie publique ; - les entrées et sorties des locaux et salles informatiques ; - les voies de circulation ou couloirs ; - les escaliers ; - les issues de secours ; - les entrepôts de marchandises ou de biens ; - les caisses, à condition que la caméra ne soit pas davantage fixée sur le caissier ; - les salles d'attente ; - les parkings. **Emplacements interdits :** Il est interdit d'installer des caméras de vidéosurveillance dans les endroits suivants : - les vestiaires ; - les toilettes ; - les cabines d'essayage dans les boutiques ou magasins ; - l'intérieur des bureaux ou espaces mis à la disposition des employés à des fins de détente et de pause ; - les locaux réservés aux délégués du personnel et les issues à ces locaux.

Catégories de personnes concernées	Les employés et les visiteurs.
Catégories de données traitées	Les catégories de données autorisées sont les images. Toutefois, il n'est pas autorisé l'enregistrement de données sonores.
Destinataire des données	Les images peuvent être communiquées aux autorités judiciaires dans le cadre d'une enquête judiciaire.
Finalités du traitement	Les finalités visées sont : - la sécurité des biens ; - la sécurité des personnes. Il est strictement interdit de surveiller délibérément et de manière permanente les employés sur leurs lieux de travail sauf si ceux-ci manipulent des biens précieux ou dangereux.
Durée de conservation des données	Les images collectées sont conservées pour une durée maximum de trois (3) mois.
Droit des personnes	L'installation de caméras de surveillance sur un lieu de travail requiert l'information préalable des employés et des visiteurs. Cette information doit être portée sur un panneau visible, affichée dans les espaces sous surveillance. Le panneau doit indiquer : - L'existence du système ; - le nom du responsable du système ; - le numéro de récépissé délivré par la CDP ; - le numéro de personne à contacter pour l'exercice du droit d'accès. Par ailleurs, les instances représentatives du personnel doivent être informés et consultées avant toute installation de caméras de surveillance.
Sécurité des données	- Établir une politique d'habilitation pour les personnes qui peuvent visionner les images ou vidéos dans l'exercice de leurs fonctions ; - Sauvegarder et préserver l'intégrité des données ; - Sensibiliser les parties prenantes concernées aux règles de sécurité ;
Sous-traitant	Lorsque le responsable du système de vidéosurveillance fait appel à un sous-traitant ou un prestataire, pour l'installation et la maintenance, celui-ci doit être conforme avec la réglementation et signer un engagement de confidentialité dans le cadre de sa mission.

3.4. Aux fins de géolocalisation

Définition	La géolocalisation est un système permettant de collecter des informations sur une personne ou sur un objet à l'aide de leurs coordonnées géographiques.
Catégories de personnes concernées	Les employés, les clients, les particuliers.
Catégories de données traitées	**Pour les véhicules de fonction et de service des entreprises publiques et privées :** - les données d'identification des employés : nom, prénom, fonction, numéro de matricule ; - les données d'identification du véhicule : marque du véhicule, numéro d'immatriculation du véhicule ; - les données de localisation du véhicule : les coordonnées géographiques, les itinéraires, les positions en temps réel, les arrêts, le nombre de kilomètres parcourus ; - les informations relatives à la vitesse du véhicule ; - les informations relatives aux dates et heures d'activation et de désactivation des systèmes de géolocalisation, pendant et en dehors des heures de travail ; **Pour les sociétés de location de véhicules :** - les données d'identification du client : nom, prénom, numéro de téléphone, numéro du permis de conduire ou numéro de la carte nationale d'identité ; - la durée de la location ; - les données de localisation du véhicule : la localisation en temps réel du véhicule, le nombre de kilomètres parcourus. **Pour les particuliers :** Lorsqu'un particulier emploie un personnel affecté à la conduite de ses véhicules, les données de localisation suivantes peuvent être collectées et traitées : - les itinéraires et coordonnées géographiques du véhicule ; - la localisation en temps réel du véhicule ; - le nombre de kilomètres parcourus ; - les informations relatives à la vitesse du véhicule.

Finalités du traitement	Le recours à des systèmes de géolocalisation doit permettre de poursuivre les finalités suivantes : **Pour les véhicules de fonction et de service des entreprises publiques et privées :** - Gestion de la flotte de véhicules (maintenance et révisions techniques) ; - Sécurité des personnes (prévention et assistance en cas d'accident), des véhicules (détection et traçabilité en cas de vol) ; - Contrôle à temps réel des trajets et itinéraires et production de rapports ; - Contrôle du respect d'une obligation légale ou réglementaire imposant la mise en œuvre d'un dispositif de géolocalisation, en raison du type de transport ou de la nature des biens transportés (hydrocarbures ou autres) ; - Contrôle du respect des règles d'utilisation du véhicule, définies par l'entreprise propriétaire. Le recours à un système de géolocalisation de véhicules peut avoir pour finalité accessoire le suivi du temps de travail, lorsque ce suivi ne peut être réalisé par un autre moyen, sous réserve notamment de ne pas collecter ou traiter de données de localisation en dehors du temps de travail des employés concernés. **Pour les sociétés de location de véhicules :** - Gestion de la flotte de véhicules (facturation de la prestation) ; - Sécurité des personnes (prévention et assistance en cas d'accident), des véhicules loués (détection et traçabilité en cas de vol) ; - Contrôle du respect des règles d'utilisation des véhicules loués définies par le propriétaire. **Pour les particuliers :** - Sécurité des personnes (prévention et assistance en cas d'accident), du véhicule (prévention, détection et traçabilité en cas de vol).
Durée de conservation des données	Au regard des finalités précitées, pour les trois catégories de systèmes de géolocalisation, la durée nécessaire de conservation des données d'identification des personnes physiques et de localisation est fixée à deux (2) ans à compter de leur collecte.

	Au-delà de cette durée de conservation, les données doivent être archivées de manière sécurisées ou supprimées.
Droit des personnes	L'installation de systèmes de géolocalisation sur des véhicules d'entreprises, des véhicules de location et des véhicules de particuliers, affectés à personnel dédié requiert l'information préalable des personnes utilisatrices. Pour les entreprises publiques et privées, les employés concernés doivent être formellement informés par note de service, par note d'information ou par tout document d'information dûment notifié à la personne concernée. Ce document indique : - l'identité de l'exploitant du système de géolocalisation et du sous-traitant, le cas échéant ; - les finalités du système de géolocalisation ; - les catégories de données collectées et traitées ; - les règles d'activation et de désactivation du système de géolocalisation ; - les mesures prises pour assurer la sécurité des données ; - les mesures prises pour assurer la protection de la vie privée des employés ; - les modalités d'exercice des droits d'accès, de rectification et d'opposition. Les sociétés de location de véhicules doivent préalablement informer de manière formelle leurs clients de l'existence de balises de géolocalisation sur les véhicules loués et des finalités de tels systèmes. Les clients doivent également être informés des catégories de données collectées et traitées.
Sécurité des données	- L'accès aux données collectées ne doit être possible que par les personnes habilitées à recevoir et consulter les informations issues du système de géolocalisation. Les personnes habilitées doivent être déterminées en fonction de la finalité du dispositif. - Le responsable de traitement pourra effectuer une analyse de risques afin d'évaluer au mieux les mesures de sécurité à prendre en compte pour la mise en place d'un système de géolocalisation.

	- Lorsqu'un exploitant de système de géolocalisation utilise des outils ou logiciels et plateformes développés et proposés par des tiers pour le traitement des données, il doit s'assurer que ces outils, logiciels et plateformes respectent les obligations de sécurité.
Protection de la vie privée	Les exploitants de système de géolocalisation de véhicules doivent prendre toutes les précautions utiles afin de protéger la vie privée des employés et des clients concernés. A ce titre, les mesures suivantes doivent être mises en œuvre : - désactiver le système de géolocalisation à l'issue des horaires de travail ou durant les heures de pause. A défaut de la possibilité de désactiver le système de géolocalisation en dehors des horaires de travail, les données collectées durant ces heures ne peuvent pas utilisées pour prendre des décisions à l'encontre des employés ; - s'engager formellement à l'endroit des employés et des clients à ne pas porter atteinte à leur vie privée ; - faire signer un engagement aux employés à utiliser les véhicules conformément aux règles prédéfinies par l'employeur ; - limiter les données de localisation collectées auprès des clients qui louent des véhicules.
Sous-traitant	Le sous-traitant doit veiller au respect des mesures de sécurité. A cet effet, lorsqu'un exploitant de système de géolocalisation fait appel aux services d'un sous-traitant, pour la mise à disposition du système de géolocalisation, le sous-traitant doit présenter des garanties suffisantes pour assurer la sécurité et la confidentialité des données. Un engagement de confidentialité doit être signé par le sous-traitant.

3.5. Aux fins de prospection commerciale

Définition	La prospection est une pratique consistant à faire des sollicitations par envoi de messages, quel qu'en soit le support ou la nature, notamment commerciale, politique ou caritative, en vue de promouvoir directement ou indirectement des biens, des services ou l'image d'une personne vendant des biens ou offrant des biens ou services. La prospection est faite au moyen d'un automate d'appel, d'un télécopieur, d'un courrier électronique ou par les nouveaux outils de communication (téléviseurs, consoles de jeux, objets connectés, SMS, blogs, réseaux sociaux, Twitter, etc).
Catégories de personnes concernées	Les prospects
Catégories de données traitées	- Fichiers clients (opérateurs de télécommunication, prestataires de services, banques, universités, cliniques, commerçants, hotels, etc.) - Fichiers des associations (Partis politiques, artistes, etc.) - Fichiers administratifs (Ministères, Démembrements de l'Etat, Ambassades, Consulats, etc.) - Fichiers électoraux.
Finalités du traitement	Les données collectées doivent permettre de poursuivre des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement de gestion des activités commerciales peut être mis en œuvre pour les finalités suivantes : - gestion des contrats (p. ex. : gestion des commandes, de la livraison, de l'exécution du service ou fourniture du bien, des factures et paiements) ; - gestion de programmes de fidélité ; - établissement de statistiques financières ; - réalisation d'enquêtes de satisfaction et d'études clients comprenant les sondages, les tests produits, les statistiques de vente réalisées par l'organisme concerné ; - réalisation d'actions de prospection commerciale et de marketing (envoi de messages publicitaires, jeux concours, parrainage, promotion, sondage); - sélection de fournisseurs.

Durée de conservation des données	La durée de conservation des données personnelles traitées est dictée par la finalité du fichier objet de la prospection directe. Sauf consentement des personnes concernées, il est interdit de conserver des données pour une durée illimitée en vue de procéder, à tout moment, à des opérations de prospection directe. Au-delà de la campagne de prospection commerciale et d'offres commerciales, les données doivent être supprimées ou archivées.
Consentement de la personne concernée	Toute opération de prospection directe, quel qu'en soit l'objet et sous quelque forme que ce soit, notamment par SMS, par courrier électronique ou par téléphone, sans le consentement préalable, libre et éclairé de la personne concernée, est interdite. La prospection directe ainsi prohibée se traduit par les cas de figures suivants : - en cas de collecte directe des données personnelles, les personnes concernées doivent consentir expressément à recevoir des messages à des fins de prospection ; - en cas de collecte indirecte des données personnelles, le responsable de traitement doit déclarer la base ou le fichier à la CDP avant d'adresser un message aux personnes concernées afin de requérir leur consentement. La réponse à ce message est gratuite et en l'absence de réponse, les données devront être supprimées automatiquement ; - en cas d'utilisation de base de données détenue par d'autres prestataires, le responsable de traitement ne peut utiliser que les données des personnes ayant expressément exprimé leur consentement. A cet effet, il doit informer ses partenaires, notamment les fournisseurs de services à valeur ajoutée, de l'obligation de respecter la législation avant toute prospection directe ; - en cas d'utilisation de bases de données déjà constituées et pour lesquelles le consentement des personnes concernées n'était pas préalablement requis, le responsable de traitement doit déclarer la base ou le fichier à la CDP avant d'informer les intéressés par l'envoi d'un message sur les nouvelles possibilités d'utilisation de leurs données personnelles et de la faculté de s'y opposer.
Droit des personnes	- **Droit à l'information** Lorsque les données traitées notamment à des fins de prospection directe sont collectées, soit directement auprès de la personne

	concernée, soit par l'intermédiaire d'un tiers, celle-ci doit être informée de la finalité, des catégories de données concernées, des destinataires en vue de pouvoir demander à ne plus figurer sur le fichier. - **Droit d'opposition** La personne faisant l'objet de prospection a le droit de se faire offrir expressément, sur le même support, la possibilité de s'opposer gratuitement et sans aucune justification, d'une part, à la réception de sollicitations et, d'autre part, à la communication de ses données à des tiers à des fins de prospection directe. Cette opposition, dont la procédure doit être indiquée de manière claire dans le message objet de la prospection, a un effet immédiat dès que la demande est formulée. Le droit d'opposition s'applique également aux informations mises à la disposition du public par les opérateurs de télécommunications. - **Droit d'accès** Les personnes concernées ont accès à leurs données traitées à des fins de prospection directe.
Sécurité des données	- Le responsable de traitement doit mettre en œuvre toutes les mesures de sécurité permettant de garantir la disponibilité, l'intégrité, la confidentialité et la traçabilité des données collectées. - Il est strictement interdit de procéder à la collecte et à tout traitement qui révèlent l'origine raciale, ethnique ou régionale, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle, les données génétiques ou plus généralement celles relatives à l'état de santé de la personne concernée. - En cas de prospection directe, le responsable du traitement doit veiller à ne pas cibler la consonance des noms des personnes, les lieux de naissance, les origines raciales ou ethniques, l'appartenance à une communauté religieuse ou les opinions politiques des personnes concernées.