Centre de Gestion
de la Fonction Publique Territoriale
de la Haute-Garonne
590 rue Buissonnière - CS 37666 - 31676 LABEGE CEDEX - Tél 05 81 91 93 00 - Fax 05 62 26 09 39 - contact@cdg31.fr - www.cdg31.fr

CHARTE D'UTILISATION DU SYSTEME D'INFORMATION ET DE COMMUNICATION DU CDG31

Document soumis à avis du Comité Technique le 15/12/2015
Approuvé par délibération du Conseil d'Administration le 28/01/2016

SOMMAIRE

PREAMBULE

1 - Le contexte et les enjeux

Différents outils technologiques peuvent être mis à la disposition des représentants de l'établissement ou des agents du CDG31 dans le cadre de l'exercice de leur mission.

Ils constituent un corpus de moyens indispensables à la qualité du service public déployé par l'établissement et participent également à la qualité de l'environnement de travail des agents.

Il appartient au CDG31, en qualité d'institution publique et d'employeur, de garantir la bonne utilisation de ces outils, dans le respect des personnes, de la loi, de la déontologie et de la bonne économie des emplois et des moyens.

2 - L'objectif

La présente charte informatique est un code de déontologie interne rappelant les grands axes du cadre légal de la mise à disposition des équipements ci-dessous indiqués et précisant un cadre opérationnel propre à l'administration du système d'information et de communication au sein de l'établissement.

Elle concerne donc :

- les matériels, notamment les micro-ordinateurs (fixes ou portables), les périphériques, les téléphones (fixes ou portables) et tout équipement de même nature mis à disposition ;
- tous les accès et applications, à savoir les applicatifs métiers, toute licence en bureautique ou spécifique, la messagerie électronique, les accès Internet, Extranet, Intranet (liste non exhaustive).

3 - Le champ d'application

La présente charte s'applique à l'ensemble des utilisateurs auxquels le CDG31 donne accès à ses équipements et bases informatiques pour la réalisation de ses missions, quelle que soit leur qualité (élus du Conseil d'Administration, agents tous statuts confondus, représentants syndicaux, vacataires, stagiaires).

Ceux-ci ont par ailleurs la charge de veiller à son respect dans le cadre de l'intervention, sous leur contrôle ou responsabilité, d'intervenants extérieurs.

4 – Définition

Le Système d'information et de communication du CDG31 peut être défini comme l'ensemble des ressources informatiques et téléphoniques, matérielles ou immatérielles, mises en place par le CDG31 dans le cadre de la réalisation de ses missions institutionnelles, ainsi que celles auxquelles il est possible d'accéder à distance, directement ou en cascade, à partir du réseau administré ou utilisé par le CDG31.

I – LE SYSTEME D'INFORMATION ET DE COMMUNICATION DU CDG31

A – LE CADRE LEGAL

Le présent document a été établi par référence aux textes qui suivent. Ces textes, ou tout autre promulgué ultérieurement à l'approbation du présent document, seront le cadre de référence pour toute question en lien avec l'objet du présent document.

1. La protection des données.

Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : la création de tout fichier contenant des informations nominatives doit faire l'objet d'une demande préalable auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

La Directive n° 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) s'applique plus spécifiquement au traitement des données à caractère personnel dans le secteur des télécommunications.

2. Le respect du droit de propriété.

La copie d'un logiciel constitue le délit de contrefaçon sanctionné pénalement (Code de la Propriété Intellectuelle). L'auteur d'une contrefaçon engage directement sa responsabilité, il peut être poursuivi devant les tribunaux répressifs et civils, même si la personne morale qui l'emploie, par exemple un établissement public, peut également être poursuivie.

3. Le respect de l'intégrité d'un système informatique.

Le simple accès à un système, sans autorisation, constitue un délit, même s'il n'en est résulté aucune altération des données ou du fonctionnement dudit système. Si de telles altérations sont constatées, les sanctions prévues sont doublées.

Il est à souligner que de tels actes (même de simples tentatives) sont susceptibles d'entraîner l'éviction de la fonction publique.

La répression des atteintes aux systèmes de traitement automatisé de données est prévue par la loi du 5 janvier 1988 (Loi dite "Godfrain"), dont les dispositions ont été reprises, depuis le 1er mars 1994, par les articles 323-1 à 323-7 du Nouveau Code Pénal.

B – LE CADRE MATERIEL

Dans le cadre de la gestion des ressources humaines déployées pour la mise en œuvre de ses missions, l'établissement met à la disposition de ses agents, en fonction de leurs attributions, un certain nombre de moyens, en matériels, en logiciels et en droits d'accès, l'ensemble constituant un environnement informatique et de communication.

Le CDG31 est propriétaire des matériels ou des droits afférents. Il assure la maintenance de ces biens ainsi que leur couverture pour les risques encourus. L'établissement assure également l'administration de la gestion des données.

L'ensemble de ces dispositions relève de sa libre administration dans le respect des dispositions légales et de la déontologie.

II – ADMINISTRATION DU SYSTEME D'INFORMATION ET DE COMMUNICATION PAR LE CDG31

A – LE ROLE DU CDG31

Le CDG31 gère et administre seul, ou avec le concours de prestataires extérieurs, la gestion et l'administration du système d'information et de communication du CDG31.

Il attribue les matériels et droits selon les nécessités de l'organisation et de l'exécution des missions du service public.

Il administre les conditions de gestion, de pérennité et de sécurité des moyens et données intégrés à ce système.

B – CONDITIONS D'ADMINISTRATION

Le CDG31 assure :

- le respect des dispositions légales concourant au respect des individus et à la gestion des ressources humaines ;
- le respect des dispositions légales encadrant l'usage d'un système d'information et de communication ;
- le respect des autorisations ou déclarations préalables vis-à-vis de la CNIL ;
- la mise en œuvre des dispositions visant à la sécurité, la conservation et la confidentialité des données qu'il gère ;
- la maintenance et la gestion technique de tous les éléments matériels et immatériels composant le système.

L'administration du Système d'Information s'effectue, soit par voie de mesures générales (notes de services), soit par voie de mesures individuelles (mise à disposition de moyens et définition de droits).

Dans le cadre de ce rôle, le CDG31 peut-être amené à contrôler l'usage des moyens mis à disposition des utilisateurs, tout en veillant au respect de leur information préalable, de leur vie privée et des règles de confidentialité. Le CDG31 peut mener des analyses des conditions d'usage des échanges via le réseau.

Les droits d'accès peuvent à tout moment être modifiés, retirés selon les besoins du service. Ils prennent fin à la cessation de leur activité dans l'établissement, pour quelque cause que ce soit.

Le CDG31 pourvoit à la réalisation des tâches correspondantes par l'intermédiaire des agents en charge de l'informatique. Ces derniers sont soumis aux mêmes obligations de confidentialité et de devoir de réserve applicables à l'ensemble des agents et utilisateurs.

Il veille à encadrer l'intervention des prestataires extérieurs dans le même sens.

III – DROITS ET OBLIGATIONS DES UTILISATEURS DANS LE CADRE DE L'UTILISATION DU SYSTEME D'INFORMATION ET DE COMMUNICATION PAR LE CDG31

A – DISPOSITIONS GENERALES

L'utilisation de toutes ressources mises à disposition par le CDG31 est réservée à des fins institutionnelles et professionnelles.

De manière générale, les agents du CDG31 sont tenus au respect des obligations de réserve, de discrétion et de secret professionnel inhérentes aux droits et obligations des agents publics tels que définis par la loi du 13 juillet 1983 portant droits et obligations des fonctionnaires et la loi n°84-53 du 26 janvier 1984 relative à la fonction publique territoriale.

Les utilisateurs se doivent d'adopter un comportement responsable excluant toute tentative d'accès à des sites dont les contenus sont étrangers à l'exercice de leurs missions, mais également à des données non autorisées ou à des sites qui, par leur nature, contreviendraient à la morale publique.

Ils se doivent de ne créer aucune situation préjudiciable pour l'établissement sur le plan de la sécurité informatique et sur le plan de l'image institutionnelle.

Tout utilisateur du système d'information et de communication du CDG31 est responsable à titre personnel de l'utilisation qu'il fait des ressources informatiques, de ses actes de recherche et des messages qu'il expédie.

En outre, chaque agent se doit de respecter le cadre hiérarchique et de mission dans lequel les moyens d'information et de communication ont été mis à sa disposition.

Le droit d'accès au système d'information consenti à chaque utilisateur est personnel. Un premier niveau de sécurité consiste en la mise en place d'un accès personnel par mot de passe, régulièrement modifié. Le mot de passe est strictement personnel et incessible. Il ne peut être communiqué à des tiers, quels qu'ils soient, y compris les collègues. Les mots de passe répondent à des règles de sécurité définies par le CDG 31.

La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde quotidienne des informations sous la responsabilité technique exclusive du CDG31. Ces dispositifs de sauvegarde ne concernent que les données conservées sur les serveurs de fichiers.

Tout document existant dans les bases de données de l'établissement est considéré comme professionnel.

Le caractère privé d'un document doit être clairement libellé sur le document ou sur le dossier qui le contient.

A la fin de l'activité au sein de l'établissement, les droits d'usage de tous ordres sont retirés et ils ne peuvent plus être utilisés. L'ensemble des matériels doit être restitué, en bon état.

B – CONDITIONS D'USAGE DU PARC MATERIEL

Tout élément du parc matériel remis reste la propriété du CDG31. L'utilisateur doit en prendre soin et signaler tout problème.

Toute intervention sur le matériel relève de la responsabilité exclusive du CDG31.

Ce matériel ne peut être connecté qu'à du matériel sous la responsabilité du CDG31. Seules les suites logicielles validées par le CDG31 peuvent y être installées ou développées.

L'utilisation des matériels n'est autorisée par principe que sur le site du siège du CDG31. Le CDG31 peut, cependant, autoriser l'utilisation de matériel à l'extérieur, au titre de missions nomades ou de

télétravail, dans un cadre d'utilisation défini par l'établissement permettant de garantir la sécurité, l'intégrité et la confidentialité des données de l'établissement et la garde des matériels.

Lorsqu'un utilisateur s'absente de son bureau, même quelques instants, son poste de travail doit être systématiquement verrouillé. En fin de journée de travail, l'utilisateur doit éteindre son poste et les périphériques associés.

Ces dispositions visent à garantir le respect de la confidentialité, de la conservation des données, de la sécurité matérielle et des contingences de consommation électrique.

C – CONDITIONS DE GESTION DES DONNEES ET DES INFORMATIONS

1. Devoirs de l'utilisateur.

Chaque utilisateur doit notamment respecter l'intégrité et la confidentialité des données, qu'il s'agisse du traitement des informations ou de leur communication interne et externe. Il veille :

- à ne pas perturber la disponibilité du système d'information ;
- à ne pas stocker ou transmettre d'informations portant atteinte à la dignité humaine ;
- à ne pas marquer les données exploitées d'annotations pouvant porter atteinte à la dignité humaine, à la vie privée, aux droits et images de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée ;
- à respecter les obligations afférentes aux déclarations préalables auprès de la CNIL pour toute création de fichiers contenant des informations nominatives ;
- à respecter le droit de propriété intellectuelle : non reproduction et/ou non diffusion de données soumises à un droit de copie non détenu, interdiction de copie de logiciel sans licence d'utilisation ;
- à ne pas introduire de ressources extérieures matérielles ou logicielles qui pourraient porter atteinte à la sécurité du système d'information ;
- à respecter les contraintes liées à la maintenance du système d'information ;
- à ne pas masquer son identité ou usurper celle d'un autre ;
- à procéder régulièrement à l'élimination des fichiers non utilisés et à l'archivage dans le but de préserver la capacité de stockage.

En outre, aucune donnée privée ne devra être stockée sur les serveurs de fichiers ou de messagerie. Le transport de données sur des supports mobiles (clés et disques USB, smartphone, pc portable) doit-être limité à des données "non sensibles". L'utilisateur s'engage à ne pas sortir ce type de données du CDG31 sans l'autorisation écrite de la direction. Afin de garantir la sauvegarde et la sécurité des données, l'utilisateur devra stocker les documents de travail sur les espaces dédiés et en aucun cas sur le disque local.

L'usage des services peer-to-peer, flux vidéo et audio, chat, et jeux en ligne sont interdits.

La continuité du service impose que tout utilisateur ne peut et ne doit en aucune manière appliquer des mesures de sécurité propres ou de limitation d'accès, non validées par le CDG31, et qui auraient pour conséquence de rendre inaccessibles des informations en lien avec le bon fonctionnement de l'établissement (chiffrement ou protection d'un fichier à l'aide d'un mot de passe non communiqué à son supérieur hiérarchique, par exemple).

L'utilisateur d'un logiciel ne peut en réaliser une quelconque reproduction ou une copie de sauvegarde.

2. Confidentialité des données - Déclarations CNIL

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, et ceux qui sont publics ou partagés. En particulier, il est interdit de prendre connaissance d'informations transitant sur le réseau ou détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées.

La diffusion d'informations nominatives n'est possible que dans le respect des prescriptions figurant à l'article 15 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Si l'utilisateur est amené à constituer des fichiers tombant sous le coup de la loi Informatique et Libertés, il devra impérativement informer sans délai le Pôle Administration Générale et Commande Publique pour la mise en œuvre des obligations déclaratives auprès de la CNIL (Commission Nationale Informatique et Libertés).

Les données médicales traitées par le CDG 31 font l'objet d'une annexe à la présente Charte, à destination, en particulier, des agents du CDG 31 associés à la gestion de ces données.

D – CONDITIONS D'UTILISATION SPECIFIQUES A LA MESSAGERIE

L'utilisation de la messagerie est réservée à des fins professionnelles. Néanmoins il est toléré en dehors des heures de travail un usage modéré de celle-ci pour des besoins personnels et ponctuels.

L'utilisateur est tenu de la consulter au minimum une fois par jour durant ses heures d'activité et dans la mesure où ses conditions d'accès le permettent.

L'utilisateur veillera à ne pas ouvrir les courriels dont le sujet paraîtrait suspect ou qui comporteraient des liens ou des pièces-jointes suspects.

Tout courrier électronique est réputé professionnel et est donc susceptible d'être ouvert par l'autorité territoriale en cas de nécessité de service. Les courriers à caractère privé et personnel doivent expressément porter la mention « personnel » ou «privé » dans leur objet.

L'utilisateur porte une attention particulière à la qualité des informations envoyées et à leur forme. Il s'engage à ne pas diffuser d'informations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et à l'image de chacun comme à ceux de l'établissement ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée.

L'utilisateur signera tout courriel professionnel. Cette signature comportera obligatoirement :
- son nom et son prénom ;
- son entité de rattachement ;
- les coordonnées postales, téléphoniques, fax et mèl de l'établissement.

L'utilisateur doit éviter de surcharger le réseau d'informations inutiles. Les messages importants sont à conserver et/ou archiver, dans une version unique, les autres à supprimer. Le dossier « éléments supprimés » doit être vidé périodiquement.

En cas d'absence prévisible, l'utilisateur devra mettre en place un message automatique d'absence indiquant sa date de retour prévue et une alternative de contact possible au sein de l'établissement.

Les agents du CDG31 ne doivent pas utiliser une adresse personnelle de messagerie électronique dans le cadre de la réalisation de leurs missions.

E – CONDITIONS D'UTILISATION SPECIFIQUES A INTERNET

L'utilisation d'Internet est réservée à des fins professionnelles et/ou syndicales dans le cadre de l'exercice des décharges d'activité et autorisations spéciales d'absence correspondantes. Néanmoins, il est toléré en dehors des heures de travail un usage modéré de l'accès à Internet pour des besoins personnels à condition que la navigation n'entrave pas l'accès professionnel.

L'utilisateur s'engage lors des consultations Internet au respect des lois et notamment celles relatives aux publications à caractère illicite, injurieux, raciste, pornographique, diffamatoire, ainsi qu'au respect des principes de neutralité religieuse, politique et commerciale. Il n'émettra pas d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice et atteinte à l'image du CDG31.

Le téléchargement, en tout ou partie, de données numériques soumises aux droits d'auteurs ou à la loi du copyright (fichiers musicaux, logiciels propriétaires, etc.) est strictement interdit.

Tout abonnement payant à un site web ou à un service via Internet relève de la compétence de l'établissement. L'abonnement à des sites gratuits est réservé à des sites clairement dévolus à l'alimentation de l'activité professionnelle.

Pour éviter les abus, l'autorité territoriale peut procéder, à tout moment, au contrôle des connexions entrantes et sortantes et des sites visités dans les conditions indiquées au II-B, 3è alinéa des présentes.

L'utilisation des services de messagerie instantanée de type « chat » ou des « réseaux sociaux » est limitée à des opérations dûment autorisées au préalable par l'administration du système d'information.

L'utilisation des services de messagerie personnelle n'est pas autorisée pour des raisons de sécurité.

F – CONDITIONS D'UTILISATION SPECIFIQUES A LA TELEPHONIE

L'utilisation des téléphones fixes, portables et des fax est réservée à des fins professionnelles. Néanmoins, un usage ponctuel du téléphone pour des communications personnelles locales est toléré à condition que cela n'entrave pas l'activité professionnelle. L'autorité territoriale peut procéder au contrôle de l'ensemble des appels émis.

En cas d'absence, l'utilisateur doit effectuer un renvoi sur le poste d'un autre agent du service.

L'utilisateur doit veiller à soigner sa présentation lors d'un appel pour faciliter son identification et/ou celle son service.

L'utilisation des téléphones portables personnels doit rester très occasionnelle et discrète.

G – DROIT SYNDICAL

Les dispositions présentes sont applicables aux organisations syndicales présentes au CDG 31, en sa qualité d'employeur public territorial. Elles participent du dialogue social de l'établissement avec les organisations syndicales créées en son sein et s'inscrivent dans le cadre du décret n° 85-397 du 3 avril 1985 relatif à l'exercice du droit syndical dans la fonction publique territoriale.

Les organisations syndicales sont autorisées à utiliser la messagerie de l'établissement dans le cadre de leur activité syndicale.

1. Respect du principe de finalité.

Les adresses de messagerie électronique des agents ne peuvent être utilisées par les organisations syndicales pour d'autres raisons que la mise à disposition de publications et tracts de nature syndicale.

L'utilisation du système de messagerie électronique de l'établissement pour la diffusion des « tracts électroniques » doit être compatible avec les exigences de bon fonctionnement de son réseau informatique et ne doit pas entraver l'accomplissement du travail.

2. Respect des droits d'information et d'opposabilité préalable.

Les agents sont informés, via la présente charte, de la prérogative ci-dessus reconnue aux représentants syndicaux. Ils disposent du droit de faire opposition par leurs soins à l'envoi de tout message syndical sur leur messagerie professionnelle, auprès des représentants syndicaux.

Le droit de s'opposer à recevoir les communications syndicales par mèl est systématiquement rappelé dans tout message afin que les agents puissent, à tout moment, manifester leur volonté de s'opposer à la réception de messages syndicaux.

Le caractère syndical du message doit systématiquement être mentionné en objet du message électronique adressé. La confidentialité des messages syndicaux peut être ainsi respectée dans la limite des contraintes d'administration et de sécurité du système d'information du CDG 31.

Les éventuelles listes de diffusion sont établies à la seule diligence des organisations syndicales, dans le respect des droits des agents et dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

IV – SANCTIONS

La loi, les textes réglementaires ainsi que la présente charte définissent les droits et obligations des personnes utilisant les ressources informatiques de l'Etablissement.

Tout utilisateur ne respectant pas les règles définies dans cette charte est passible de mesures qui peuvent être internes à l'établissement et/ou de sanctions disciplinaires proportionnelles à la gravité des manquements constatés par l'autorité territoriale, conformément aux dispositions du statut de la Fonction Publique Territoriale.

L'utilisateur pourra, en outre, voir ses droits d'accès aux ressources et système d'information et de communication suspendus ou supprimés, partiellement ou totalement. De plus, une poursuite pénale pourra être mise en œuvre à l'encontre de tout contrevenant.

Les principales sanctions sont rappelées en annexe.

V – CONDITIONS D'OPPOSABILITE ET DE RESPECT DE LA CHARTE

La charte est portée à la connaissance de tous les utilisateurs selon les moyens adaptés (remise initiale à la suite de l'élection ou à l'embauche/mise à disposition en continu à la Direction Générale des Services et via l'Intranet).

Tout complément ou modification est porté et maintenu à la connaissance des utilisateurs des moyens informatiques et électroniques.

Le Président du CDG31 et la Direction Générale des Services ont en charge l'application de la présente charte.

ANNEXE 1 RAPPEL DES DISPOSITIONS LEGALES APPLICABLES

Rappel des principales dispositions pénales applicables aux personnes utilisant des moyens informatiques (art. 226-16 à 226-24 du code pénal relatifs aux atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques ainsi que art. 323-1 à 323-7 du code pénal relatifs aux atteintes aux systèmes de traitement automatisé de données)

⇒ **Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques.**

Article 226-16
Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.
Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article 45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Article 226-16-1-A
Lorsqu'il a été procédé ou fait procéder à un traitement de données à caractère personnel dans les conditions prévues par le I ou le II de l'article 24 de la loi n° 78-17 du 6 janvier 1978 précitée, le fait de ne pas respecter, y compris par négligence, les normes simplifiées ou d'exonération établies à cet effet par la Commission nationale de l'informatique et des libertés est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

Article 226-16-1
Le fait, hors les cas où le traitement a été autorisé dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 précitée, de procéder ou faire procéder à un traitement de données à caractère personnel incluant parmi les données sur lesquelles il porte le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

Article 226-17
Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

Article 226-17-1
Le fait pour un fournisseur de services de communications électroniques de ne pas procéder à la notification d'une violation de données à caractère personnel à la Commission nationale de l'informatique et des libertés ou à l'intéressé, en méconnaissance des dispositions du II de l'article 34 bis de la loi n° 78-17 du 6 janvier 1978, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

Article 226-18
Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

Article 226-18-1
Le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

Article 226-19
Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à

la santé ou à l'orientation ou identité sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.
Est puni des mêmes peines le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté.

Article 226-19-1
En cas de traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende le fait de procéder à un traitement :
1° Sans avoir préalablement informé individuellement les personnes sur le compte desquelles des données à caractère personnel sont recueillies ou transmises de leur droit d'accès, de rectification et d'opposition, de la nature des données transmises et des destinataires de celles-ci ;
2° Malgré l'opposition de la personne concernée ou, lorsqu'il est prévu par la loi, en l'absence du consentement éclairé et exprès de la personne, ou s'il s'agit d'une personne décédée, malgré le refus exprimé par celle-ci de son vivant.

Article 226-20
Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi.
Est puni des mêmes peines le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa.

Article 226-21
Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission Nationale de l'Informatique et des Libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en oeuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

Article 226-22
Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.
La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 Euros d'amende lorsqu'elle a été commise par imprudence ou négligence.
Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit.

Article 226-22-1
Le fait, hors les cas prévus par la loi, de procéder ou de faire procéder à un transfert de données à caractère personnel faisant l'objet ou destinées à faire l'objet d'un traitement vers un Etat n'appartenant pas à la Communauté européenne en violation des mesures prises par la Commission des Communautés européennes ou par la Commission Nationale de l'Informatique et des Libertés mentionnées à l'article 70 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

Article 226-22-2
Dans les cas prévus aux articles 226-16 à 226-22-1, l'effacement de tout ou partie des données à caractère personnel faisant l'objet du traitement ayant donné lieu à l'infraction peut être ordonné. Les membres et les agents de la Commission Nationale de l'Informatique et des Libertés sont habilités à constater l'effacement de ces données.

Article 226-23
Les dispositions de l'article 226-19 sont applicables aux traitements non automatisés de données à caractère personnel dont la mise en oeuvre ne se limite pas à l'exercice d'activités exclusivement personnelles.

Article 226-24
Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies à la présente section encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par les 2° à 5° et 7° à 9° de l'article 131-39.
L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

⇒ **Des atteintes aux systèmes de traitement automatisé de données.**

Article 323-1
Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende.
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.
Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende.

Article 323-2
Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.
Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende.

Article 323-3
Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.
Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende.

Article 323-3-1
Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.
Article 323-4
La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-5
Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :
1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;
2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;
4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;
6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;
7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

Article 323-6
Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39.
L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

Article 323-7
La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines

ANNEXE 2 RELATIVE AUX DONNEES MEDICALES DU CDG31

I. Principes généraux applicables aux données de santé et situation du CDG 31.

Dans le cadre de l'exercice de ses missions statutaires, le CDG 31 procède à la collecte et à la conservation de données de nature médicale. Les missions conduisant au recueil de données médicales sont nombreuses : il s'agit notamment, de la médecine préventive, de la gestion du secrétariat des instances médicales, de l'assurance statutaire. Dans ce cadre, il convient que chaque acteur concerné soit sensibilisé au respect des données de santé gérées par le CDG 31.

- **Collecte**

Les données relatives à la santé sont considérées par la loi Informatique et Libertés (article 8) comme des données sensibles dont le traitement et la collecte sont par principe interdits.

Toutefois, les données de santé peuvent être utilisées et communiquées dans des conditions déterminées par la loi et dans l'intérêt des patients (assurer le suivi médical, faciliter sa prise en charge par l'assurance maladie...) ou pour les besoins de la santé publique.

La loi Informatique et Libertés énumère les cas dans lesquels le traitement ou la collecte des données de santé est possible. Les traitements nécessaires aux fins de suivi médical des personnes, de prévention, de diagnostic, d'administration de soins ou de traitements, ou de gestion de services de santé font partie des cas de figure prévus par la loi.

- **Interdictions.**

Les données médicales concernant les patients ne peuvent pas faire l'objet de cession ou d'exploitation commerciale.
La constitution et l'utilisation à des fins de prospection ou de promotion commerciale de fichiers composés à partir de données issues directement ou indirectement des prescriptions médicales ou des données personnelles de santé sont interdites (même rendues anonymes à l'égard des patients) dès lors que ces fichiers permettent d'identifier directement ou indirectement le professionnel prescripteur (article L. 4113-7 du code de la santé publique).

- **Les tiers autorisés**

Les tiers autorisés au sens de la loi sont les personnes habilitées par des textes législatifs ou réglementaires à obtenir un accès ponctuel et limité aux données.
Il s'agit :
- des autorités judiciaires
Le procureur de la République, les juges, les officiers de police judiciaire de la police ou de la gendarmerie nationale doivent être considérés, lorsqu'ils agissent par réquisition judiciaire dans le cadre d'une enquête de flagrance, d'une enquête préliminaire ou d'une instruction préparatoire éventuellement sur commission rogatoire, comme des tiers autorisés à obtenir communication des données contenues dans les dossiers ;
- des experts
Les experts désignés par une juridiction administrative ou civile peuvent obtenir communication des données sous réserve du consentement du patient concerné.

II. Situation des parties prenantes du CDG 31 vis-à-vis des données médicales.

- **Obligations du médecin.**

Le médecin de prévention est responsable de la tenue du dossier médical en santé au travail et des données qu'il contient. Il veille à son intégrité. La conservation du dossier est assurée sous sa responsabilité, conformément au code de déontologie médicale. Le médecin recourt, en tant que de besoin, à l'assistance du Service Informatique du CDG 31 lorsque le dossier est dématérialisé.

Il peut habiliter les personnes qui l'assistent dans sa mission à accéder au dossier, dans le strict cadre de l'exercice de leur mission d'assistance, cela dans la conformité « de la notion de secret médical partagé ».

Le médecin de prévention veille à ce que les personnes qui l'assistent dans son exercice soient instruites de leurs obligations en matière de respect du secret professionnel et s'y conforment.

- **Obligations de l'ensemble des personnels (administratifs et médicaux).**

Chaque agent qui, par fonction, est amené à accéder aux dossiers et données médicaux est informé qu'il est soumis à une obligation de discrétion professionnelle et est astreint au respect du secret professionnel.
Le non-respect de l'obligation de discrétion professionnelle est passible de sanctions disciplinaires. L'atteinte au secret professionnel est passible de sanctions pénales.

- Situation des personnels associés au traitement informatique.

Les agents associés au traitement informatique, en particulier les agents du Service Informatique, sont obligés au respect des données médicales auxquelles ils peuvent être amenés à avoir accès dans le cadre de l'exercice des fonctions et tâches qui leurs sont assignées.
Les agents se prémunissent contre toute indiscrétion volontaire ou involontaire et contre toute utilisation abusive.

- Rappel des textes

Article 26 de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires

« Les fonctionnaires sont tenus au secret professionnel dans le cadre des règles instituées par le code pénal.
Les fonctionnaires doivent faire preuve de discrétion professionnelle pour tous les faits, informations ou documents dont ils ont connaissance dans l'exercice ou à l'occasion de l'exercice de leurs fonctions. En dehors des cas expressément prévus par la réglementation en vigueur, notamment en matière de liberté d'accès aux documents administratifs, les fonctionnaires ne peuvent être déliés de cette obligation de discrétion professionnelle que par décision expresse de l'autorité dont ils dépendent ».

Article 226-13 du code pénal
« La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende ».

Article L1110-4 du Code de la santé publique
« Le fait d'obtenir ou de tenter d'obtenir la communication de ces [informations] est puni d'un an d'emprisonnement et de 15 000 euros d'amende ».

- **Obligations du CDG 31.**

Le CDG 31 assure l'intégrité, la sécurité et la confidentialité des données.
Sous la responsabilité de l'autorité territoriale et du médecin coordonnateur, le Service Informatique veille au respect des standards informatiques applicables.

- Traçabilité.

Si l'application informatique dédiée à la gestion des données médicales le prévoit, le Service Informatique est en mesure d'assurer la production d'une liste exhaustive des personnes ayant consulté un DMST dématérialisé ainsi que le type d'accès (création, modification etc.).

- Protection des données.

Le CDG 31 veille à la protection des installations informatiques, dans le respect du Référentiel Général de Sécurité.
La protection mise en œuvre par le CDG 31 comprend, à titre non exhaustif :
- le contrôle de l'accès aux locaux où sont stockées les données ;
- la sécurité physique du réseau, des serveurs et des supports d'archivages de données ;
- la protection contre les attaques extérieures et intérieures ;
- la régulation des usages et modes opératoires en interne.

Le présent document est notifié par l'autorité territoriale ou par le médecin de prévention à tout agent ayant à en connaître.

Fait à Labège, le

Le Président,

Pierre IZARD

Je soussigné(e)

NOM
PRENOM
AFFECTATION

Déclare avoir pris connaissance de l'Annexe à la charte informatique du CDG31 relative aux données médicales et je m'engage à m'y conformer.

Notifié le :
Signature