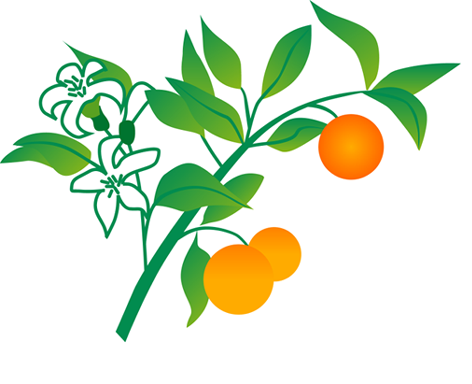
## CHARTE INFORMATIQUE



## Etablissement d’Hébergement pour

## Personnes Agées Dépendantes

« Les Orangers »

🕿 : 04.93.40.68.00

🖷 : 04.93.40.68.30

📫 : [direction@ehpad-lesorangers.fr](mailto:direction@ehpad-lesorangers.fr)

📫 : rh@ehpad-lesorangers.fr

Edition 2024

### SOMMAIRE

### PREAMBULE

1°) Le contexte et les enjeux

2°) L’objectif

3°) Le champ d’application

### I – LES REGLES GENERALES D’UTILISATION

A - Les droits et devoirs des utilisateurs

1°) Un accès aux ressources réglementé

2°) Une utilisation professionnelle des ressources

3°) Confidentialité et accessibilité

4°) Données

B - Les droits et devoirs de l’établissement

C – L’analyse et le contrôle

D - Les sanctions

E - Les évaluations

### III – LES POSTES INFORMATIQUES

### IV – LA MESSAGERIE

A – Conseils généraux

B – L’utilisation personnelle de la messagerie

### V – L’INTERNET

### VI – LE TELEPHONE

### VII – CYBER ATTAQUE

### VIII – LES BASES LEGALES

A – Les textes législatifs

B – Le code pénal

C – La réglementation européenne

### PREAMBULE

**1°) Le contexte et les enjeux**

Les différents outils technologiques utilisés offrent au personnel des collectivités une grande ouverture vers l’extérieur. Cette ouverture peut apporter des améliorations de performances importantes si l’utilisation des outils informatiques est faite à bon escient et selon certaines règles.

A l’inverse une mauvaise utilisation de ces outils peut avoir des conséquences extrêmement graves. En effet, ils augmentent les risques d’atteinte à la confidentialité, de mise en jeu de la responsabilité, d’atteinte à l’intégrité et à la sécurité des fichiers de données personnelles (virus, intrusions sur le réseau interne, vol de données).

De plus, mal utilisés, les outils informatiques peuvent être aussi une source de perte de productivité et de coûts additionnels.

**2°) L’objectif**

La présente charte informatique est un code de déontologie formalisant les règles légales et de sécurité relatives à l’utilisation de tout système d’information et de communication au sein de l’établissement : applications métiers, bureautique, messagerie, micro-ordinateurs, périphériques, téléphones fixes et portables, etc.

Tout manquement, selon la gravité, est susceptible d’entraîner pour l’utilisateur des sanctions disciplinaires, et ce sans exclusion d’éventuelles actions pénales ou civiles à son encontre.

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.

**3°) Le champ d’application**

La présente charte s’applique à l’ensemble du personnel tous statuts confondus, ainsi qu’au personnel temporaire.

Elle s’applique également à tout prestataire extérieur ayant accès aux données et aux outils informatiques de l’établissement.

Dès l’entrée en vigueur de la présente charte, chaque agent de l’établissement s’en verra remettre un exemplaire, il devra en prendre connaissance et devra s’engager à la respecter.

### I – LES REGLES GENERALES D’UTILISATION

Les utilisateurs sont supposés adopter un comportement responsable, s’interdisant par exemple toute tentative d’accès à des données ou à des sites qui leurs seraient interdits.

Tout utilisateur est responsable de l’utilisation qu’il fait des ressources informatiques, ainsi que du contenu de ce qu’il affiche, télécharge ou envoie et s’engage à ne pas effectuer d’opérations, qui pourraient avoir des conséquences néfastes sur le fonctionnement du réseau. Il doit en permanence garder à l’esprit que c’est sous le nom de l’établissement qu’il se présente sur Internet et qu’il doit se porter garant de l’image de restitution.

Au même titre que pour le courrier, le téléphone ou la télécopie, chacun est responsable des messages envoyés ou reçus, et doit utiliser la messagerie dans le respect de la hiérarchie, des missions et fonctions qui lui sont dévolues et des règles élémentaires de courtoisie et de bienséance.

**A - Les droits et devoirs des utilisateurs**

**1°) Un accès aux ressources réglementé**

Des personnes travaillant dans l’établissement disposent d’un droit d’accès au système d’information. Ce droit d’accès est strictement personnel et incessible.

**2°) Une utilisation professionnelle des ressources**

Les ressources informatiques mises à disposition constituent un outil de travail nécessaire.

Chaque utilisateur doit adopter une attitude responsable et respecter les règles définies sur l’utilisation des ressources, et notamment :

* Respecter l’intégrité et la confidentialité des données. Cette règle s’applique tant pour le traitement des informations que pour leur communication interne et externe ;
* Ne pas perturber la disponibilité du système d’information ;
* Ne pas stocker ou transmettre d’informations portant atteinte à la dignité humaine ;
* Ne pas marquer les données exploitées d’annotations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et images de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race, ou nation déterminée (loi informatique et libertés du 06/01/1978). Une déclaration à la CNIL est obligatoire pour toute création de fichiers contenant des informations nominatives ;
* Respecter le droit de la 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 ;
* Ne pas reproduire de « ressources extérieures » matérielles ou logicielles qui pourraient porter atteinte à la sécurité du système d’information ;
* Ne pas masquer son identité ou usurper celle d’un autre.

L’usage de ces outils de communication ne modifie en rien les obligations de validation et d’information vis-à-vis de la hiérarchie.

La continuité du service étant une priorité, l’utilisateur s’interdit, cependant, d’appliquer des mesures de sécurité non validées par la direction et qui auraient pour conséquence de rendre inaccessibles des informations intéressant 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 ou au responsable informatique).

**3°) Confidentialité et accessibilité**

L’accès à certains éléments du système d’information (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, certains services interactifs ou applications) est protégé par des paramètres de connexion (identifiant, mot de passe).

Ces paramètres sont personnels à l’utilisateur et doivent être gardés confidentiels. Ils permettent en particulier de contrôler l’activité des utilisateurs.

Toutefois, pour des raisons de sécurité et de persistance des données, ils doivent être communiqués à la direction ou au responsable informatique.

Dans la mesure du possible, ces paramètres devront être mémorisés par l’utilisateur et ne pas être conservés, sous quelque forme que ce soit.

En tout état de cause, ils ne doivent pas être transmis à des tiers ou aisément accessibles.

Ils doivent être saisis par l’utilisateur à chaque accès et ne pas être conservés en mémoire dans le système d’information.

Lorsqu’ils sont choisis par l’utilisateur, les paramètres devront respecter un certain degré de complexité et être modifiés régulièrement.

Au niveau du choix de son mot de passe, les recommandations suivantes s’imposent. Ils doivent présenter au moins huit caractères, et notamment :

* 2 Majuscules
* 4 Minuscules
* 2 Chiffres
* 2 Caractères spéciaux.

Sauf demande formelle de la direction, aucun utilisateur ne dois se servir pour accéder au système d’information de l’établissement d’un autre compte que celui qui lui a été attribué. Il ne doit pas non plus déléguer à un tiers les droits qui lui ont été attribués.

Les droits d’accès peuvent être modifiés ou retirés à tout moment, selon les besoins du service, et prennent fin lors de la cessation de l’activité professionnelle.

**4°) Données**

Chaque utilisateur est responsable pour ce qui le concerne du respect du secret professionnel et de la confidentialité des informations qu’il est amené à détenir, consulter ou utiliser.

Il est également responsable des ressources qui lui sont confiées dans le cadre de l’exercice de ses fonctions. Il doit concourir à la protection des dites ressources, en faisant preuve de prudence et de vigilance. En particulier, il doit signaler à la direction toute violation ou tentative de violation de l’intégrité de ces ressources et, de manière générale, tout dysfonctionnement, incident ou anomalie.

Sauf autorisation expresse de la direction, l’accès au système d’information avec du matériel n’appartenant pas à l’établissement est interdit. De même, la sortie de matériel appartenant à l’établissement doit être justifiée par des obligations professionnelles et nécessite l’accord exprès de la direction.

L’utilisateur ne doit pas non plus modifier les paramétrages de son poste de travail ou des différents outils mis à sa disposition, ni contourner aucun des systèmes de sécurité mis en œuvre dans l’établissement. Il doit dans tous les cas en alerter la direction.

**B - Les droits et devoirs de l’établissement**

L’établissement doit veiller à la disponibilité et à l’intégrité du système d’information.

En ce sens, il s’engage à :

* Mettre à disposition les ressources informatiques matérielles et logicielles nécessaires au bon déroulement de la mission des utilisateurs ;
* Mettre en place des programmes de formations adaptés et nécessaires aux utilisateurs pour une bonne utilisation des outils ;
* Informer les utilisateurs des diverses contraintes d’exploitation (interruption de service, maintenance, modification de ressources, etc) du système d’information susceptibles d’occasionner une perturbation ;
* Effectuer les mises à jour nécessaires des matériels et logiciels composant le système d’information afin de maintenir le niveau de sécurité en vigueur dans le respect des règles d’achat et des budgets alloués ;
* Respecter la confidentialité des « données utilisateurs » auxquelles il pourrait être amené à accéder pour diagnostiquer ou corriger un problème spécifique ;
* Définir les règles d’usage de son système d’information et veiller à leur application.

**C – L’analyse et le contrôle**

Pour des nécessités de sécurité, de maintenance et de gestion technique, l’utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent, sous le contrôle du responsable informatique, être analysés et contrôlés dans le respect de la législation applicable et notamment de la loi relative à l’informatique, aux fichiers et aux libertés.

**D - Les sanctions**

La loi, les textes règlementaires et la présente charte définissent les droits et obligations des personnes utilisant les ressources informatiques.

Tout utilisateur du système d’information de l’établissement, n’ayant pas respecté la loi, pourra être poursuivi pénalement.

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

L’utilisation à des fins personnelles de certains systèmes payants à travers le système de communication de l’établissement donnera également lieu à remboursement de la part de l’utilisateur concerné.

**D - Les évaluations**

Avant son entrée en vigueur, la présente charte a été soumise à l’avis du Comité social d’établissement.

### III – LES POSTES INFORMATIQUES

Un ensemble « matériels-système d’exploitation-logiciels » est mis à disposition de chaque utilisateur.

Le matériel informatique est fragile, il faut en prendre soin et redoubler d’attention pour les écrans plats.

Les supports amovibles (disquettes, Cd-Rom, clé USB, etc) provenant de l’extérieur doivent être soumis à un contrôle antivirus préalable.

Toute installation logicielle est à la charge du prestataire informatique désigné par le directeur de l’établissement. Les téléchargements à l’initiative de l’utilisateur, et sans autorisation préalable du responsable informatique, sont interdits.

En cas d’absence momentanée, l’utilisateur doit verrouiller son PC (ex. : maintenir enfoncées les touches « CTrl+ Alt+Suppr ») et cliquer sur verrouiller l’ordinateur.

En cas d’absence, l’utilisateur doit quitter les applications, et verrouiller systématiquement son PC.

A la fin de sa journée de travail, l’utilisateur doit quitter les applications, arrêter le système par arrêt logiciel, éteindre l’écran et l’imprimante.

L’utilisateur doit signaler tous dysfonctionnements ou anomalies au service économat, qui fera remonter au responsable informatique en cas de besoin. Il doit également procéder régulièrement à l’élimination des fichiers non utilisés et à l’archivage dans le but de préserver la capacité de mémoire.

### IV – LA MESSAGERIE

**A – Conseils généraux**

Chaque salarié dispose, pour l’exercice de son activité professionnelle, d’une adresse de messagerie électronique normalisée et attribuée par l’établissement. Les messages électroniques reçus sur la messagerie professionnelle font l’objet d’un contrôle antiviral et d’un filtrage anti-spam.

Les agents sont invités à informer la direction des dysfonctionnements qu’ils constateraient dans ce dispositif de filtrage.

L’attention des utilisateurs est attirée sur le fait qu’un message électronique a la même portée qu’un courrier postal : il obéit donc aux mêmes règles, en particulier en matière d’organisation hiérarchique. En cas de doute sur l’expéditeur, compétent pour envoyer le message, il convient d’en référer à son supérieur.

Un message électronique peut être communiqué très rapidement à des tiers et il convient de prendre garde au respect d’un certain nombre de principes, afin d’éviter les dysfonctionnements du système d’information, de limiter l’envoi de messages non sollicités et de ne pas engager la responsabilité civile ou pénale de l’établissement et de l’agent.

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

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

Il doit également envisager l’opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l’ensemble des destinataires.

Le risque de retard, de non remise et de suppression automatique des messages électroniques doit être pris en considération pour l’envoi de correspondances importantes. Les messages importants doivent donc être envoyés avec un accusé de réception ou signés électroniquement. Ils doivent être, le cas échéant, doublés par un envoi par fax ou de courrier postal.

Les agents doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers.

Les correspondances électroniques ne doivent pas comporter d’éléments illicites, tels que des propos diffamatoires, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

L’utilisateur soigne la qualité des informations envoyées à l’extérieur et s’engage à ne pas diffuser d’informations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et image de chacun ou faisant référence à une quelconque appartenance à une ethnie, race ou nation déterminée.

L’utilisateur est tenu de consulter sa messagerie au minimum une fois par jour, hormis en période d’absence. Il doit accorder la même importance aux messages électroniques qu’aux courriers postaux ou fax et se doit de les traiter.

L’utilisateur veillera à ne pas ouvrir les courriels, dont le sujet paraît suspect.

L’utilisateur signera tout courriel professionnel. Il comportera obligatoirement :

* Le nom et prénom de l’expéditeur ;
* Son entité de rattachement ;
* Les coordonnées postales de l’établissement.

L’utilisateur doit vérifier la liste de destinataires et respecter les circuits de l’organisation ou la voie hiérarchique le cas échéant.

L’utilisateur doit éviter de surcharger le réseau informatique d’informations inutiles. Les messages importants sont à conserver et/ou archiver, 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 la date de retour prévue ou rediriger ses messages sur un autre utilisateur.

Une équivalence juridique est établie entre le courrier électronique et le courrier sur support papier. Ils doivent en conséquence être traités dans les mêmes délais.

**B – L’utilisation personnelle de 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.

Les messages à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, de ne pas perturber et de respecter les principes posés dans la présente charte.

Les courriers à caractère privé et personnel doivent expressément porter la mention « personnel et confidentiel » dans leur objet. Ces derniers ne pourront alors être ouverts par le directeur ou le responsable informatique, que pour des raisons exceptionnelles de sauvegarder la sécurité ou de préservation des risques de manquement aux droits des tiers ou à la loi.

Les messages envoyés doivent être signalés par la mention « Privé » ou « Perso » dans leur objet et être classés dès l’envoi dans un dossier lui-même dénommé de la même façon.

Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé « privé » ou « Perso ».

En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

### V – L’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 d’autorisations spéciales d’absence.

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’utilisation d’Internet à des fins commerciales personnelles en vue de réaliser des gains financiers ou de soutenir des activités lucratives est strictement interdite.

Il est aussi prohibé de créer ou mettre à jour au moyen de l’infrastructure de l’établissement tout site internet, notamment des pages personnelles.

Il est interdit de se connecter à des sites internet dont le contenu est contraire à l’ordre public, aux bonnes mœurs ou à l’image de marque de l’établissement (pédopornographie, apologie des crimes contre l’humanité et provocation à la discrimination, à la haine ou à la violence à l’égard d’une personne à raison de leur origine ou de leur appartenance ou non à une ethnie, une nation, une race ou une religion déterminée, etc) ainsi qu’à ceux pouvant comporter un risque pour la sécurité du système d’information de l’établissement ou engageant financièrement celui-ci.

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

Le stockage sur le réseau de données à caractère non professionnel téléchargés sur Internet est interdit.

Toute saisie d’informations sur un site internet professionnel nécessite l’autorisation préalable de la direction.

Toute procédure d’achats personnels sur Internet est formellement interdite.

L’utilisation de forums de discussion est autorisée pour un usage professionnel. Tout utilisateur participant à un forum fait figurer en bas de chacun des messages publiés la mention suivante : « Le contenu de ce message n’engage que son auteur et en aucun cas l’établissement EHPAD Les Orangers ».

L’utilisation des services de messagerie instantanée « Chat » est interdite, sauf autorisation expresse de la direction.

Les utilisateurs sont informés que la direction enregistre leur activité sur Internet et que ces traces pourront être exploitées à des fins statistiques, contrôle et vérification dans les limites prévues par la loi.

Pour éviter les abus, la direction peut procéder, à tout moment, au contrôle des connexions entrantes et sortantes et des sites les plus visités.

### VI – LE TELEPHONE

L’utilisation des téléphones fixes et portables 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.

La direction peut procéder au contrôle de l’ensemble des appels émis.

L’utilisation des téléphones portables personnels doit rester occasionnelle et discrète. Par conséquent, il est demandé au personnel de mettre leur téléphone portable en mode vibreur et de ne pas l’utiliser dans les étages ni dans les parties communes.

Le téléphone portable peut par contre être utilisé durant le temps de pause, et en salle du personnel.

En cas d’absence, l’utilisateur doit effectuer un renvoi sur le poste d’un autre agent du service ou sur l’accueil téléphonique.

L’agent, qui quitte définitivement la collectivité, doit restituer le téléphone portable professionnel.

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

Les utilisateurs sont informés que le service informatique enregistre leur activité téléphonique, aussi bien sur les postes fixes que sur les mobiles.

Ces traces seront exploitées à des fins de statistiques, contrôle et vérification dans les limites prévues par la loi. Un accès aux numéros détaillés est possible.

### VII – CYBER ATTAQUE

Les systèmes sont de plus en plus vulnérables et il convient d’être très vigilant.

Les établissements ont l’obligation de déclarer tous les incidents informatiques qu’ils rencontrent.

Aujourd’hui, les établissements sont essentiellement confrontés à des « cryptovirus », qui s’installent sur les postes de travail ou sur les serveurs.

Les « cryptovirus » rentrent dans les ordinateurs, bien souvent par l’intermédiaire d’un mail, ils chiffrent les données et rendent l’accession à ces données tout à fait impossible, sauf à payer une rançon. Mais les sauvegardes peuvent être chiffrées.

Le mode opératoire est traditionnellement le suivant :

* Un mail frauduleux est envoyé, avec ou sans pièce jointe. Le fait d’ouvrir le mail ou la pièce jointe déclenche le virus, qui rentre ainsi dans le système.
* Une rançon est demandée, généralement de 300 euros par poste et aux alentours de 20 000 euros par établissement. En fait, tout dépend de la taille de l’établissement.
* La faille peut aussi venir de l’intérieur.

Pour prévenir ces attaques, un certain nombre de précautions s’imposent aux utilisateurs :

* Il ne faut pas utiliser de mots de passe simples ;
* Il ne faut pas ouvrir les mails écrits en anglais ;
* Il ne faut pas cliquer trop rapidement sur certains liens ;
* Il faut désactiver par défaut les composants Active X et Javascript ;
* Il ne faut pas utiliser de compte administrateur pour naviguer ;
* Il ne faut pas relayer les canulars ;
* Il ne faut pas donner son identité numérique ;
* Il faut faire attention aux messages dont l’expéditeur est inconnu ;
* Il faut se méfier des messages n’ayant pas d’objet professionnel.

En cas d’attaques, il convient immédiatement d’une part de déconnecter physiquement l’appareil, et d’autre part, d’appeler en urgence le prestataire informatique.

Il faut être vigilant par rapport au « Darknet », c’est-à-dire le net sombre. La police repère très facilement les utilisateurs de cet espace et peut débarquer dans l’établissement.

### VIII – LES BASES LEGALES

L’utilisation doit respecter les obligations de réserves, de discrétion et de secret professionnel conformément 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°86-33 du 9 janvier 1986 portant dispositions statutaires relatives à la fonction publique hospitalière.

Cette présente partie a pour objectif d’informer les utilisateurs des textes législatifs et réglementaires applicables dans le domaine de la sécurité des systèmes d’information.

**A – Les textes législatifs**

* **Loi du 21 juin 2004** pour la confiance dans l’économie numérique. Elle est destinée à favoriser le développement du commerce par internet, en clarifiant les règles pour les consommateurs et les prestataires aussi bien techniques que commerciaux ;
* **Loi du 13 mars 2000** portant adaptation du droit de la preuve aux technologies de l’information et relative à la signature électronique ;
* **Loi du 10 juillet 1991** relative au secret des correspondances émises par voie des télécommunications
* **Loi du 5 janvier 1988** sur la fraude informatique.

Cette loi, dite de Godefrain, vise à lutter contre la fraude informatique en réprimant :

* Les accès ou maintien frauduleux dans les systèmes d’information ;
* Les atteintes accidentelles ou volontaires au fonctionnement ;
* La falsification des documents informatiques et leur usage illicite ;
* L’association ou l’entente en vue de commettre un de ces délits.
* **Loi du 3 juillet 1985** relative aux droits d’auteur et aux droits des artistes interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle. Elle interdit à l’utilisateur d’un logiciel toute reproduction de celui-ci autre que l’établissement d’une copie de sauvegarde.
* **Loi du 17 juillet 1978** portant diverses mesures d’amélioration des relations entre l’administration et les public et les diverses dispositions d’ordre administratif, social, etc.
* **Loi du 6 janvier 1978** relative à l’informatique, aux fichiers et aux libertés. Elle a pour objet de protéger les libertés individuelles susceptibles d’être menacées par l’utilisation de l’informatique.

**B – Le code pénal**

Sont concernés les articles suivants : art. 323-1, art. 323-2, art. 323-3, art. 323-3-1, art. 323-4, art. 323-5, art. 323-6, et art. 323-7.

**C – La réglementation européenne**

**La convention européenne du** **28 janvier 1991** pour la protection des personnes à l’égard du traitement informatisé des données à caractère personnel définit les principes de base à la protection des données que les Etats parties doivent concrétiser dans leur ordre juridique interne. Elle exclut en principe les entraves aux flux transfrontières de données entre les Etats parties. Elle règle la coopération entre Etats pour la mise en œuvre de la Convention, en partie l’assistance qu’un Etat partie doit prêter aux personnes concernées ayant leur résidence à l’étranger. Enfin, elle met en place un comité consultatif chargé en particulier de faciliter et d’améliorer son application.

**La directive 95/46/CE** relative à la protection des données personnelles et à la libre circulation de ces données, publiée au Journal Officiel des Communautés Européennes du 23 novembre 1995 vise à réduire les divergences entre les législations nationales sur la protection des données afin de lever tout obstacle à la libre circulation des données à caractère personnel à l’intérieur de l’Union européenne.

**La directive de la CEE du 21/12/1988** sur l’harmonisation de la protection juridique des logiciels protège les droits d’auteur, elle interdit en particulier à l’utilisateur d’un logiciel toute reproduction que l’établissement d’une copie de sauvegarde.

**RECEPISSE DE LA CHARTE INFORMATIQUE**

Je soussigné (e)

Nom : ………………………………………………………………………………………………………………………………………………………….

Prénom : …………………………………………………………………………………………………………………………………………………….

Service : …………………………………………………………………………………………………………………………………………………….

Fonction : …………………………………………………………………………………………………………………………………………………….

Utilisateur des moyens informatiques et réseaux de l’établissement EHPAD Les Orangers, situé au Bar sur Loup, déclare avoir pris connaissance de la présente charte et m’engage à la respecter.

Fait à ……………………………………………………………………………, Le ……………………………………………

Signature :

Fait en deux exemplaire :

* Un pour l’intéressé (e)
* Un pour l’établissement