

Guide de la Charte Informatique

Chapitre 1 : Préambule.....	2
Chapitre 2 : La démarche de charte.....	2
Chapitre 3 : Le contenu de la charte.....	7
Chapitre 4 : La charte idéale	14
Chapitre 5 : Le déploiement de la charte Internet.....	15
Chapitre 6 : Les meilleures pratiques en marge du déploiement de la charte	17
Chapitre 7 : Conclusion	19

Chapitre 1 : Préambule

Ce guide a pour objectif d'aider les directions informatiques dans l'élaboration de leur charte. Ce n'est en aucun cas une charte type à personnaliser dans la mesure où il n'existe pas de charte type de part la diversité des entreprises.

Il s'agit ici d'aborder pourquoi et comment mettre en œuvre une charte, comment construire son contenu et quelles sont les démarches de mise en œuvre pour qu'elle soit juridiquement opposable aux salariés.

La démarche de charte

Cette première partie a pour objectif de comprendre pourquoi aujourd'hui il est nécessaire de mettre en place une charte Internet et de définir comment la mettre en œuvre.

Chapitre 2 : La démarche de charte

Qu'est ce qu'une charte Internet ?

La Charte définit les conditions générales d'utilisation de l'Internet, des réseaux et des services multimédias au sein d'une entreprise ou d'une administration

Pourquoi mettre en place une charte ?

La mise en œuvre d'une charte est indispensable pour au moins deux raisons majeures :

- Pour limiter les responsabilités pénales et civiles
- Parce que c'est un concept admis par tous

Limiter les responsabilités pénales et civiles

Y a-t-il des obligations générales de responsabilité ?

- 1er élément de réponse :

Art1383 du code civil : « Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence »

Cet article ne porte pas sur la responsabilité d'avoir commis quelque chose mais de ne pas avoir mis en place les moyens pour éviter toutes sortes de déviations. En matière de sécurité le 0 bug ou le 0 insécurité n'existe pas, mais votre responsabilité peut être recherchée pour ne pas avoir mis les facteurs clés de succès pour éviter ce genre de déviation. On parle ici de « négligence fautive ».

- 2ème élément de réponse :

Art 1384 du code civil : « on est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre (...) les maîtres et les commettants du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés »

Cet article porte sur la « responsabilité spéciale » causée par les autres. De la même manière que les parents sont responsables des actes de leurs enfants, le dirigeant est responsable des actes de ses salariés.

D'ailleurs, il y a eu beaucoup de jurisprudences où l'employeur s'est vu condamné à cause des actes de ses salariés car il n'avait pas mis en place les moyens de réguler les accès illicites.

➤ 3ème élément de réponse :

Art 121-2 du code pénal : « Les personnes morales, à l'exclusion de l'Etat, sont responsables pénalement (...) des infractions commises, pour leur compte, par les organes dirigeants ou représentants »

En matière pénale nul ne peut être puni pour une faute qu'il n'a pas commise lui-même. Seulement quand l'infraction pénale sert les intérêts de l'entreprise, dans ce cas, la responsabilité pénale de l'entreprise et de ses dirigeants peut être engagée.

Parce que c'est un concept admis par tous

➤ La loi

On ne retrouve pas le mot « charte » mais plus généralement le mot « règlement intérieur ». Il est clairement établi qu'une charte est un règlement intérieur y compris dans son mode de déploiement.

➤ La jurisprudence

On trouve le mot « charte » puisque les entreprises utilisent le mot « charte » pour qualifier ce document. Par conséquent, on retrouve ce mot dans certaines jurisprudences. On a donc une reconnaissance implicite

de ce mot et donc de ce document.

➤ La CNIL

La CNIL parle également de charte et la recommande dans son guide pratique « employeur – employé »¹. Si l'on veut respecter la loi informatique et liberté d'un côté et du droit du travail de l'autre, on se doit de mettre en place des chartes.

➤ Forum des droits sur l'Internet²

Une structure associative qui rédige plusieurs documents sur le monde de l'Internet et édite plusieurs recommandations dont quelques unes sur la nécessité de mettre en place une charte.

➤ Les meilleures pratiques

Aujourd'hui la majorité des entreprises ont une charte et cela amène forcément un impact juridique. Etant donné que 80% des entreprises possède une charte, il pourra vous être reproché de ne pas avoir mis en œuvre cette bonne pratique.

➤ Dans le droit

Il n'existe pas aujourd'hui de disposition particulière sur la mise en place d'une charte Internet. A priori il n'y en aura pas puisque c'est un règlement intérieur mais pourquoï pas un futur projet de loi.

1 Guide de la CNIL :

http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_GuideTravail.pdf

2 <http://www.foruminternet.org/>

La démarche et le mécanisme de charte

Une charte s'inscrit dans une démarche d'explication et de sensibilisation quant aux enjeux et aux risques. L'objectif est de faire adhérer les collaborateurs puisque ce sont principalement eux « les maillons faibles ». Il faut donc que la charte soit claire et à la portée de tous.

Pour cela il y a tout un mécanisme à maîtriser afin de mettre en place une charte pertinente :

- La connaissance des risques
- L'apprentissage de la problématique
- La responsabilisation des acteurs,
- Pour définir des chartes,
- Pour définir des moyens techniques
- Pour mettre en place une politique de contrôle et d'audit
- Enfin pouvoir sanctionner

Il s'agit de définir une politique cohérente entre réalité technique et politique RH afin de maîtriser l'ensemble des risques. C'est d'ailleurs la réelle raison d'être d'une charte. Cette charte doit être déployée en annexe du règlement intérieur si le souhait est de contrôler et de sanctionner les collaborateurs.

Chapitre 3 : Le contenu de la charte

Préambule

Le préambule de la charte permet de faire comprendre les enjeux liés à certains outils aux salariés afin d'arriver à faire adhérer l'ensemble des collaborateurs aux règles du jeu.

L'objectif est de démontrer que la mise en place de cette charte a pour vocation de protéger à la fois l'entreprise et également le salarié.

Le préambule de la charte Internet peut également mentionner des cas de jurisprudence ou les textes de la CNIL pour légitimer sa mise en œuvre.

Portée et opposabilité de la charte :

Dans cette partie il s'agit de décrire d'une part qui est concerné par cette charte. Il est évident de mentionner les collaborateurs et également les personnes tierces qui peuvent avoir accès aux réseaux de l'entreprise et qui ne dépendent pas directement de l'entreprise : les visiteurs, les stagiaires, les prestataires, ... Il est également important de préciser que cette charte est valable aussi bien sur les postes fixes, nomades, les connexions à l'extérieur comme les connexions à domicile à partir de l'outil de travail fourni au salarié.

Enfin ce paragraphe est également l'occasion de préciser votre politique de sécurité concernant la connexion des postes personnels au réseau de l'entreprise.

L'opposabilité est généralement en interne assez simple à préciser dans la mesure où elle respecte les procédures de mise en œuvre (CE + Inspection du travail + Prud'hommes) mais beaucoup plus compliqué quand il s'agit de préciser l'opposabilité d'un sous-traitant par exemple. Dans le cadre d'un sous-traitant il faudra notamment faire référence au contrat qui vous lie à ce

dernier préalablement modifié et dans l'idéal prévoir une charte d'accès.

Champs d'application

Ce paragraphe va reprendre comment s'organise cette application et à quels moments l'entreprise va pouvoir contrôler, regarder et sanctionner.

Les conditions d'utilisation

C'est de loin la partie la plus compliquée de la charte aujourd'hui puisque c'est dans ce paragraphe que l'on va spécifier à quels moments le salarié est en zone privative et à quel moment le salarié est en zone professionnelle.

C'est clairement ici le piège à éviter : on ne peut interdire l'usage privatif et donner l'exclusivité à la zone professionnelle au nom de la liberté résiduelle des salariés. Si cette règle n'est pas respectée la charte n'est pas opposable aux salariés selon l'arrêt Nikon. Puisque l'entreprise ne peut interdire l'usage privatif, elle se doit de l'organiser.

Par conséquent il est important de spécifier :

- Ce qu'est la liberté résiduelle
- Comment elle est organisée
- Comment la traiter
- Quelles sont les moyens mis en œuvre par l'entreprise pour satisfaire cette obligation afin de donner au salarié cette part « résiduelle »

Il s'agit par exemple de décrire des choses qui sont socialement admises : appeler l'école si un enfant est malade, déclaration assurance suite à un accident, ... Une fois que l'on a bien expliqué cela, il reste à s'attaquer à la zone professionnelle.

Il faut spécifier également que la « zone privative », ne veut pas dire que le salarié a droit de tout y faire. Heureusement l'entreprise peut contrôler ces zones privées et particulièrement le DSI, administrateurs, ... L'entreprise a le droit de contrôle de ces zones si cela met en péril le système d'information. Encore faut-il le préciser dans la charte et surtout avoir la preuve que l'activité d'un salarié dans sa zone privée met en cause la bonne marche du système d'information en cas de litige.

Définition des conditions d'accès et d'identification

Aujourd'hui il est primordial qu'un collaborateur comprenne l'enjeu des login/mdp. On retrouve bien souvent ces identifications sur des post-it, ... Il est donc nécessaire de préciser l'importance des identifiants et des enjeux comme l'usurpation d'identité qui peuvent donc potentiellement engager leur responsabilité et remettre en cause leur emploi.

La CNIL aborde d'ailleurs précisément ce point dans son document sur les 10 points clés de la sécurité³.

Au-delà des identifiants il est également important d'en préciser les bonnes pratiques comme le verrouillage des sessions en cas d'absence, ...

Mobilité et gestion des absences / départs

Dans la loi I&L art 34, le personnel informatique, administrateur, RSSI, DSI, ... sont responsables de la sécurité de l'accès aux données à caractère personnel. Selon cet article, il est nécessaire de prendre des mesures utiles pour gérer ces problématiques. Il est donc

3 <http://www.cnil.fr/dossiers/banque-finance/fiches-pratiques/article/10-conseils-pour-securer-votre-systeme-dinformation-1/>

primordial de préciser les démarches à suivre en cas de vol ou de perte d'un pc portable par exemple pour pouvoir déposer plainte et donc protéger l'entreprise. La CNIL a également édité un nouveau guide⁴ en octobre 2010 sur la sécurité de données personnelles visant à préciser certaines obligations et interdictions en matière de données personnelles.

Gestion des connaissances et de l'espace collaboratif

Les collaborateurs doivent être sensibilisés à ces nouveaux espaces de travail en leur expliquant que les postes en accès libre auront plus de traçabilité, de rigueur d'accès et que le risque majeur dans ces conditions est la dilution de la responsabilité.

Propriété intellectuelle

C'est un problème depuis toujours et encore plus aujourd'hui avec HADOPI. Il s'agit ici de faire le point sur les téléchargements de logiciels, d'œuvres ou d'images et sensibiliser les collaborateurs aux démarches licites et illicites.

Préservation du secret et de la confidentialité

Le secret est un principe déterminé par la loi, la confidentialité, elle, est contractuelle. Il faut donc expliquer aux collaborateurs les règles de secret et de confidentialité. C'est d'autant plus vrai aujourd'hui avec le web 2.0 qui est une large porte ouverte à la divulgation d'informations à « ses amis » mais également à ses « ennemis ».

⁴ http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite%20VD.pdf

Protection des données à caractère personnel

D'une part, toutes les personnes sur lesquelles l'entreprise collecte des données à caractère personnel doivent être averties. Les collaborateurs doivent donc être informés sur les conditions dans lesquelles l'entreprise exploite ces données.

D'autre part, cette partie doit également préciser l'importance d'utiliser les logiciels de l'entreprise et de ne pas utiliser des fichiers Excel dispatchés à droite et gauche.

Vidéosurveillance

Il convient ici de communiquer sur l'existence du dispositif, des destinataires des images, ainsi que des modalités concrètes d'exercice de leur droit d'accès aux enregistrements visuels les concernant et la durée de conservation de ces logs.

Consommations téléphoniques

Les salariés doivent être informés si la téléphonie permet de comptabiliser leurs communications ou enregistrer leur communication. Les objectifs poursuivis par l'installation d'un tel système doivent être expliqués ainsi que les conséquences individuelles qui pourront en résulter. Il devra également être abordé les modalités d'exercice de leur droit d'accès et la durée de conservation de ces données.

Sécurité

Cette partie permet d'expliquer simplement la notion de « sécurité SI » et de sensibiliser les collaborateurs aux enjeux.

Traçabilité et filtrage

Il ne s'agit pas ici de dire pourquoi on filtre mais simplement comment on filtre, ce qui est logué et combien de temps sont gardées ces données.

Mesures d'urgence et plan de continuité d'activité

Cette partie reprend la planification des procédures mises en œuvre en réaction à une catastrophe ou à un sinistre grave. L'objectif est de minimiser les impacts d'une crise ou d'une catastrophe naturelle, technologique ou sociale sur l'activité.

Contrôle et audit

Il s'agit de décrire quand le service audit et contrôle et comment.

Règles de conservation et de sauvegarde

On définit ici les règles de sauvegardes : Quoi ? Combien de temps ? ..., Il est recommandé en marge de ce paragraphe de disposer d'un code de l'archivage. La CNIL aborde l'archivage dans la fiche 13 de son guide sur la sécurité des données personnelles.

Responsabilité et sanctions

Ce paragraphe a vocation d'expliquer qui est responsable de quoi et quelle sanction j'applique. Il ne s'agit pas ici de dire la sanction c'est « le licenciement ». Il s'agit ici de définir des «sanctions spéciales charte» comme réduire l'accès à certains sites Internet à un collaborateur, ... C'est d'ailleurs ici qu'il faut spécifier par exemple que l'accès à certains services peut être restreint si l'utilisateur porte atteinte à la bonne marche du SI. Ainsi vous aurez averti les collaborateurs et vous pourrez sanctionner sans être poursuivi pour

« discrimination », puisque à poste égal le filtrage doit être le même pour les collaborateurs.

Dérogation

Il peut y avoir des dérogations particulières. Par exemple une recherche d'un journaliste ou d'un avocat sur la pédophilie. Il faut donc définir les méthodes à suivre pour demander une dérogation : Qui peut demander des dérogations ? Comment ? et à qui ?

Entrée en vigueur

On précisera ici la date de mise en vigueur.

Chapitre 4 : La charte idéale

- On retrouve des règles éthiques et de régulation.
- C'est un vrai code avec de vraies sanctions
- On parle également de représentant du personnel et des salariés
- On parle également de vie privée résiduelle, de responsabilité et de contrôle
- Enfin on parle évidemment d'Internet, de Web 2.0, de mobilité et de filtrage

Ce qui est à bannir : c'est une charte par technologie. Pourquoi ? Parce qu'il y aura toujours une technologie de retard et c'est généralement là d'où vient la faille.

D'autre part, cela imposera une mise à jour régulière de la charte et renouveler tout le mode de déploiement de la charte : consultation du CE, diffusion, ...

Il faut donc sortir de l'approche technique. Ce qui n'exclut pas de rédiger un guide technique dans lequel se trouve les bonnes pratiques par technologie. Par exemple : précision sur la mise à jour d'un mot de passe : nombre de caractères, majuscules, minuscules, ...

Il faut donc privilégier une charte fonctionnelle c'est-à-dire une charte selon les usages : correspondance, surf, discussion, édition, ...

Chapitre 5 : Le déploiement de la charte Internet

Le respect du code du travail

Le principe de discussion collective

Le comité d'entreprise (ou comité paritaire dans les administrations) doit être consulté lors de l'introduction d'une charte.

1 mois avant la consultation, les membres du comité doivent avoir reçu les éléments d'information sur le projet et les conséquences sur les conditions de travail. Un avis négatif du comité d'entreprise n'empêche pas la mise en place de la solution, en revanche la non consultation constitue un délit d'entrave sanctionné par le code du travail.

Le principe de transparence

Les salariés doivent être informés de la mise en place d'une nouvelle technologie, de ses objectifs, des règles d'utilisation et de la durée de conservation des données. Autrement dit une charte doit être établie et portée à la connaissance de tous individuellement et collectivement.

Pour être opposable aux salariés la charte doit être déployée de la même manière qu'un règlement intérieur, à savoir :

- La diffuser individuellement
- La diffuser collectivement, à une place accessible sur le lieu de travail
- La soumettre au comité d'entreprise, ainsi qu'à l'avis du comité d'hygiène et de sécurité
- La déposer au greffe du conseil des prud'hommes

- La transmettre à l'inspection du travail en 2 exemplaires

La gestion des logs nominatifs

Aujourd'hui il n'y a pas vraiment de statut sur la durée de conservation des logs nominatifs.

Néanmoins il existe plusieurs textes :

- Directive européenne : 1 à 2 ans
- L'article 6 de la LCEN : 1 an
- Loi sur la lutte contre le terrorisme : 1 an
- CNIL : 6 mois

Au vu d'une part des textes de lois du « code des postes de télécommunication » complété par la « loi pour la lutte contre le terrorisme » et au d'autre part du cas de jurisprudence BNP, condamné pour ne pas avoir pu fournir les logs nominatifs lors d'une réquisition judiciaire, Olfeo recommande au minimum 1 an de conservation de logs.

La conservation de ces logs doit être proportionnelle au but recherché et par conséquent ils ne peuvent être conservés à l'infini.

Chapitre 6 : Les meilleures pratiques en marge du déploiement de la charte

La charte Internet a pour objectif de fixer les règles du jeu. Elle peut souvent s'accompagner de divers guides, chartes et codes spécifiques pour répondre à des enjeux qui peuvent être évolutifs. L'avantage non négligeable de ces différents documents est qu'ils n'ont pas besoin d'être soumis au CE, ...

Guide technique

La charte Internet doit s'inscrire dans une logique fonctionnelle et non technique pour pouvoir répondre pertinemment et de manière intemporelle aux différents enjeux liés à l'utilisation du SI. Pour être plus explicite sur les différentes technologies, on peut simplement créer « un guide technique » qui a pour objectif d'aborder par type de technologie les procédés. Par exemple : comment renouveler son login / mdp – que doit contenir le mdp : lettre, chiffre, ...

Charte administrateur

Les administrateurs disposent de droits et d'obligations particulières, notamment en par rapport à leur accès à des données qui peuvent être privées et à leur obligation de confidentialité. Par conséquent, la CNIL recommande chaudement la mise en place d'une Charte spécifique aux administrateurs, DSI, RSSI, ...

Charte d'accès pour les visiteurs

L'émergence des nouveaux espaces de travail destinés aux publics externes à l'entreprise nécessite de rédiger ce que l'on appelle « une charte d'accès ». Si la charte peut mentionner ce mode de connexion au réseau de l'entreprise, il apparaît aujourd'hui important de rédiger

un document spécifique. On y trouvera succinctement les points abordés dans la charte et ses spécificités (contrôle, sanction, autorité, ...). Il est également nécessaire d'en définir les règles d'opposabilité avec par exemple l'acceptation des règles du jeu par un clic de la charte d'accès.

Code de la sécurité et de maintien des preuves

C'est un code important en cas de litige. Il définit les conditions d'accès à la preuve et les conditions de maintien de la preuve. C'est ici qu'il sera expliqué comment selon les cas, l'accès à la preuve se fera en présence ou non d'un salarié, avec un huissier, avec la police, ... De la même manière, il sera présenté combien de copie de la preuve sera effectuée, ...

Les bonnes pratiques imposent au moins 3 copies : 1 pour l'huissier, 1 pour l'entreprise qui peut être amenée à manipuler cette copie pour avoir accès à certaine informations et une dernière pour la personne mise en cause.

Il est également recommandé d'éditer des codes éthiques, d'archivage, ...

Chapitre 7 : Conclusion

La démarche de charte s'inscrit donc dans une logique de cohérence entre contrainte technique et politique RH. La charte a avant tout pour objectif de fixer clairement les règles du jeu quant à l'utilisation des ressources informatiques pour bénéficier de l'adhésion des collaborateurs.

Le contenu doit privilégier un périmètre fonctionnel plutôt que technologique afin d'avoir une durée de vie plus longue. Dans les meilleurs pratiques la charte est accompagnée de différents guides, codes, ... pour compléter la charte.