Charte informatique : Mode d'emploi

La plupart des employeurs mettent aujourd'hui à la disposition de leur personnel des moyens informatiques pour l'exécution des missions qu'ils leur confient. Une « *charte de bonne utilisation des nouvelles technologies de l'information et de la communication* », appelée couramment « *charte informatique* » dont tous les employés doivent prendre acte s'avère alors indispensable pour contrôler l'accès à ces moyens informatiques (poste de travail, réseau commun, internet….) et la sécurité des données qui y transitent, y sont stockées et échangées.

Ce document rédigé à l'attention des utilisateurs se présente ainsi comme un ensemble de règles qui permettent d'encadrer les responsabilités des différents acteurs et de concilier d'une part les intérêts de l'employeur (préserver l'intégralité des systèmes d'information de l'entreprise ou de l'administration) et d'autre part ceux du personnel (garantir leurs droits et libertés individuelles et collectives).

La mise en place de la charte informatique permet d'éviter toute forme d'abus de l'usage des outils informatiques et constitue un cadre de référence en cas de conflit si elle est correctement déployée.

Enfin, bien que ce document ne soit pas obligatoire, il permet d'informer les utilisateurs de la collecte de leurs données à caractère personnel pour les besoins du système d'information et de la mise en œuvre des outils informatiques.

Un code de bonne conduite

Destiné à être un outil clair de rappel des droits et obligations à la fois des employés et des employeurs, la charte informatique est désormais un élément essentiel de la politique globale de sécurité du système d'information (SI). En établissant un cadre normatif et de bonnes pratiques pour une utilisation optimale des ressources informatiques, elle informe notamment les utilisateurs sur :

- les comportements à risque susceptibles de porter atteinte à l'intérêt collectif de l'entreprise ou de l'administration, et les exigences de sécurité ;
- les éventuelles mesures de surveillance (écoutes téléphoniques, vidéosurveillance…) mises en place par l'employeur sur le lieu de travail ;
- l'encadrement de l'utilisation des outils informatiques en définissant la frontière entre usage personnel et usage professionnel ;
- les sanctions encourues en cas de manquement aux dispositions de la charte informatique.

Son objectif est de définir une politique cohérente entre réalité technique et politique des ressources humaines afin de maîtriser l'ensemble des risques.

Elle doit par ailleurs être annexée au contrat de travail ou au règlement intérieur.

Le contenu de la charte informatique

La charte informatique ne peut pas être un document standard. En effet, elle doit toujours être élaborée en tenant compte de l'activité spécifique de l'entreprise ou de l'administration qui la met en place et de ses contraintes de sécurité. Sa rédaction nécessite donc une réflexion approfondie, souvent entre plusieurs services et/ou départements, et doit obéir au principe de proportionnalité en fonction du but poursuivi, ce qui peut conduire à des mises à jour fréquentes.

La charte informatique doit notamment impérativement préciser les sujets suivants :

L'administration des accès à internet et au réseau de la structure

Cette rubrique permet de définir les règles relatives aux identifiants et mots de passe communiqués aux employés leur permettant de se connecter au réseau de l'entreprise et à internet.

Il peut être indiqué que les données d'authentification (identifiant et mot de passe) de l'utilisateur étant strictement personnelles, il est nécessaire d'en interdire la divulgation à un autre employé ou à un tiers, sauf dans les cas prévus dans la rubrique dédiée à la « *gestion des absences* ».

Il est également recommandé de demander aux utilisateurs de verrouiller leur session personnelle (mise en veille automatique avec mot de passe) lorsqu'ils s'absentent de leur poste de travail et de prévoir le blocage du compte utilisateur après un certain nombre de tentatives de connexion erronées.

Par ailleurs, les droits d'accès concernant certains fichiers ou dossiers peuvent être restreints aux seules personnes habilitées. Cette politique d'habilitation doit alors être définie en tenant compte des attributions respectives de chaque utilisateur et, le cas échéant, de la nature particulièrement sensible des données traitées.

Les conditions d'utilisation de la messagerie professionnelle

Il peut être précisé dans cette rubrique qu'une utilisation limitée et raisonnable de la messagerie professionnelle à des fins privées est tolérée.

Le respect du secret des correspondances privées étant un principe intangible, l'employeur ne peut accéder aux contenus des messages privés de ses employés envoyés ou reçus à partir de la messagerie professionnelle, sans que ledit employé soit présent.

Toutefois, pour que les messages soient considérés comme personnels, il convient pour les employés de les identifier comme tels, par exemple :

- en précisant dans l'objet du message des mots clés comme « *privé* », « *[PRV]* » ou encore « *personnel* » ;
- en incluant dans l'objet du message une mention laissant manifestement supposer que ledit message est privé, telle que « *vacances au Japon* » ;
- en stockant les messages dans un répertoire intitulé « *personnel* » ou « *privé*».

Il convient par ailleurs de rappeler que la messagerie ne saurait être utilisée afin de commettre une quelconque infraction à la législation, que ce soit par les contenus véhiculés ou les propos qui y seraient échangés. Elle ne saurait en outre comporter des contenus susceptibles de mettre en péril la sécurité du système d'information (ex: pièces jointes trop lourdes ou à risques). Des applications antispam et antivirus peuvent ainsi mettre en quarantaine certains messages.

Il est également nécessaire d'indiquer si les fichiers journaux de la messagerie sont susceptibles d'être vérifiés à des fins de sécurité du SI et de maintenance et/ou pour détecter tout éventuel abus dans l'usage de la messagerie au regard des règles établies (ex : nombre d'envoi de messages identifiés comme personnels trop important, volume ou nature des pièces jointes problématique).

Les conditions d'utilisation d'internet

Il peut être rappelé dans cette rubrique que la connexion internet mise à la disposition par l'employeur doit être utilisée à des fins professionnelles mais qu'un usage privé est toléré dans la mesure où il reste raisonnable. Ce critère raisonnable peut par exemple prendre la forme d'un créneau (ou durée) de connexion au-delà duquel (ou de laquelle) l'utilisation d'internet à titre privé sera considérée comme excessive.

Il convient en outre de rappeler que l'employé est tenu de s'abstenir de commettre des faits constituant des infractions à la législation, ou de compromettre la sécurité du système d'information de quelque façon que ce soit, à travers un usage inapproprié d'internet (téléchargements, consultations de sites à risques, etc.)

L'employeur peut également décider d'interdire l'accès à certains sites (pornographiques, discriminatoires, violents, ou d'une manière générale contraires à l'ordre public et aux bonnes mœurs, réseaux sociaux, etc.).

Par ailleurs, lorsque les fichiers journaux reflétant l'usage global d'internet au sein de l'entreprise ou de l'administration font l'objet de vérifications à des fins de sécurité du SI et de maintenance, il convient de le mentionner dans cette rubrique.

Les conditions d'utilisation du téléphone

Cette rubrique doit préciser si les appels d'ordre privé sont tolérés de manière ponctuelle et si un contrôle de l'usage est effectué.

Lorsqu'un dispositif d'enregistrement des conversations téléphoniques est mis en place, il convient de décrire avec précision, notamment, le déroulement de la procédure de contrôle, ses modalités, les appareils téléphoniques concernés (fixes ou mobiles), la finalité des contrôles envisagés et les modalités de droit d'accès.

Par ailleurs, l'APDP préconise que soit instaurée dans cette charte une possibilité de désactiver la fonction d'enregistrement en appuyant sur une touche prévue à cet effet sur le téléphone avant une conversation d'ordre privé, dans le cas où l'entreprise tolère une utilisation du téléphone à cette fin. Dans le cas contraire, il convient d'autoriser le collaborateur à utiliser un téléphone non soumis à enregistrement sur son lieu de travail, ou son téléphone mobile personnel.

La gestion des absences

La charte doit nécessairement prévoir la procédure d'accès à la messagerie électronique par les personnes habilitées, en cas d'absence temporaire ou définitive de l'utilisateur. A cet égard, elle doit indiquer qu'il n'est possible d'accéder à la messagerie de la personne absente que si cela est strictement nécessaire aux fins d'assurer la continuité des activités de l'entreprise ou de l'administration.

La charte peut par exemple prévoir la mise en place d'une réponse automatique d'absence du bureau à l'expéditeur d'un message électronique avec indication de la personne à contacter en cas d'urgence, la désignation d'un suppléant disposant d'un droit d'accès personnalisé à la messagerie de son collègue ou encore le transfert à un suppléant de tous les messages entrants.

Elle devra toutefois également préciser qu'il ne pourra en aucun cas être pris connaissance des messages identifiés en objet comme « *personnels* » ou « *privé* » et que le salarié devra être informé de l'identité de son suppléant.

Les mêmes règles sont applicables en ce qui concerne l'accès au poste de travail du collaborateur absent.

Enfin, en cas de départ définitif de l'entreprise ou de l'administration, les comptes utilisateur et messagerie du collaborateur doivent être désactivés dans les trois mois qui suivent le départ dudit collaborateur.

L'obligation de confidentialité et de sécurité

Il est important d'astreindre les utilisateurs à une obligation de confidentialité concernant l'ensemble des données auxquelles ils ont accès.

Les collaborateurs doivent par ailleurs faire preuve de bon sens et de loyauté dans la gestion des ressources informatiques mises à disposition.

La protection des données personnelles

La charte informatique doit impérativement informer les utilisateurs de tous les traitements automatisés d'informations nominatives mis en œuvre par l'entreprise ou l'administration.

Conformément à l'article 11 de la Loi n° 1.565 du 3 décembre 2024, cette information doit inclure les informations suivantes :

- **l'identité et les coordonnées professionnelles du responsable du traitement**, et le cas échéant de son **représentant** à Monaco ;
- les **finalités** du traitement et son **fondement juridique** ;
- **les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers lorsque le traitement est réalisé sur un tel fondement ;**
- les **catégories de données** personnelles concernées ;
- la **durée de conservation** des données ou, lorsque cela n'est pas possible, **les critères utilisés** pour déterminer cette durée ;
- le **caractère obligatoire ou facultatif des réponses**, et les conséquences à l'égard de la personne concernée d'un défaut de réponse ;
- lorsque le traitement est fondé sur le **consentement** de la personne, le droit de celle-ci de retirer ce consentement **à tout moment** ;
- les **destinataires** ou **catégories** de destinataires ;
- les moyens d'exercer ses **droits d'accès, d'opposition, de rectification, d'effacement, de limitation** ou **de portabilité** ;
- le **droit de s'opposer à l'utilisation pour le compte de tiers**, ou à **la communication** à des tiers de données personnelles la concernant **à des fins de prospection,** notamment commerciale ;
- le droit **d'introduire une réclamation auprès de l'Autorité de Protection des Données Personnelles (APDP) ;**
- le cas échéant, les **coordonnées du Délégué à la protection des données** ;
- le cas échéant, l'existence d'une **prise de décision automatisée**, y compris le **profilage**, et le **raisonnement** qui sous-tend le traitement ;
- le cas échéant, le fait que le responsable du traitement effectue ou a l'intention d'effectuer un **transfert de données hors de la Principauté** ;
- la **source de provenance** des données personnelles lorsque celles-ci ne sont pas collectées directement auprès de la personne concernée.

Les sanctions

Il est impératif d'indiquer si un manquement aux dispositions de la charte peut donner lieu à l'ouverture d'une procédure disciplinaire ou judiciaire en cas d'infractions à la législation. Ces sanctions peuvent être mentionnées, étant toutefois précisé qu'elles ne peuvent pas être contraires aux règles prévues par le droit du travail et doivent respecter le principe de proportionnalité.

Une charte administrateur

Parallèlement à cette charte informatique qui concerne tous les utilisateurs, l'APDP recommande également la mise en place d'une charte spécifique aux administrateurs informatiques. Ces derniers disposent en effet de droits et d'obligations particuliers, notamment par rapport à leur accès à des données qui peuvent être privées et à leur obligation de confidentialité. Il convient donc de fixer les règles de déontologie qu'ils s'engagent à respecter.

L'administrateur informatique doit ainsi notamment :

- ne pas prendre connaissance de données personnelles d'utilisateurs, sauf, ponctuellement, sur demande formelle de l'utilisateur lui-même, et ne doit autoriser quiconque à y accéder, sauf cas particulier prévus par la loi (par exemple, enquête judiciaire) ou habilitations formelles et légitimes préalablement déclarées ;
- respecter ses engagements de confidentialité et de non divulgation en ne faisant pas état et en n'utilisant pas les informations qu'il peut être amené à connaître dans le cadre de ses fonctions ;
- ne pas se connecter à une ressource du SI sans autorisation explicite de la personne à qui elle est attribuée, notamment dans le cas de l'utilisation d'un logiciel de prise de main à distance sur un poste de travail utilisateur ;
- ne pas abuser de ses privilèges et limiter ses actions aux ressources informatiques dont il a la charge, dans le respect de la finalité de sa mission (il ne doit notamment modifier les configurations et les droits d'accès que dans le respect des procédures d'administration ou d'exploitation définies) ;
- ne pas prendre ses consignes d'une personne non identifiée et faire remonter auprès de son responsable hiérarchique toute requête lui paraissant inappropriée ;
- ne pas contourner les procédures de sécurité établies, et en particulier ne pas désactiver de sa propre initiative les mécanismes de traçabilité, et ne pas porter atteinte à l'intégrité des fichiers de journalisation ;
- tracer toutes ses actions.