GMSI 2016

CESI de PAU

OBERMANN
Michaël

[PROJET SAS]

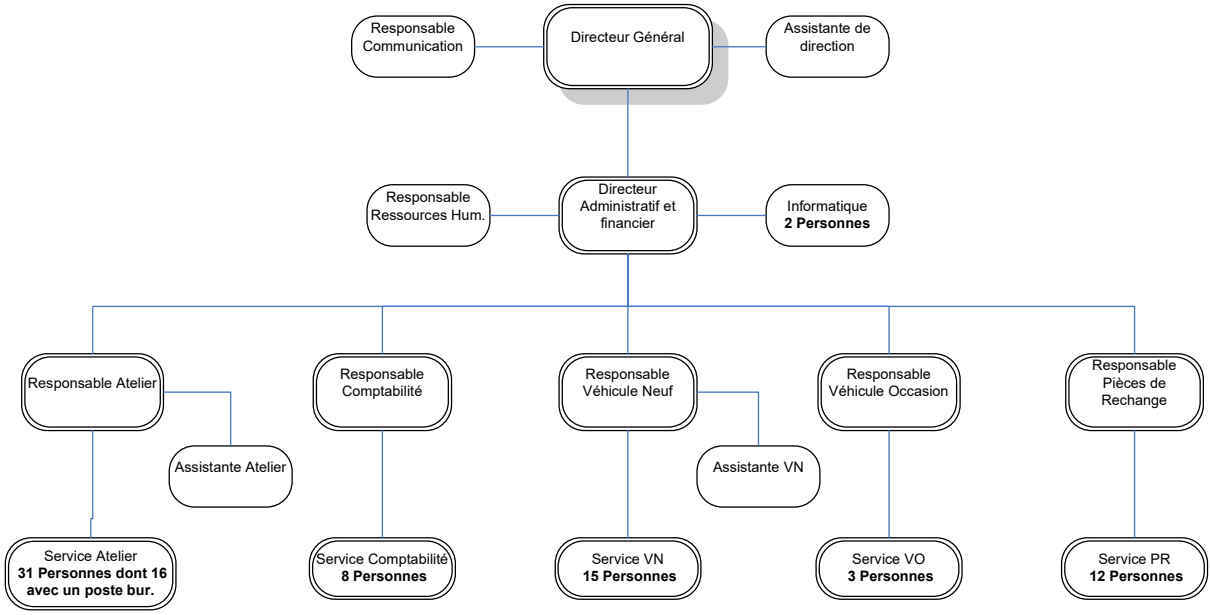
SOMMAIRE

I) CONTEXTE DE REALISATION

Ce rapport est réalisé dans le cadre de l'étude avant-vente réalisée par la société SUPPORT 2000, pour répondre à l'appel d'offre d'obtention de la gestion du parc informatique de la société AutoConcept.

La société AutoConcept est une concession automobile possédant un parc informatique de 76 postes, géré par deux informaticiens appartenant à l'entreprise.

Organigramme de la société AutoConcept :



Suite à de nombreux dysfonctionnements dans les prestations du service informatique actuel de la société AutoConcept, dans le support, la gestion et la prévention d'incidents, mais aussi des comportements inappropriés, voire à risque du personnel vis-à-vis de l'outil informatique, cette dernière souhaite externaliser la gestion du parc informatique. (Voir **Annexe 1 : Compte-rendu des problèmes rencontrés par la société AutoConcept avec son service informatique actuel**).

De plus, en cas d'obtention du marché, un des deux informaticiens actuels de la société AutoConcept rejoindra notre structure. Il conviendra d'effectuer une sélection selon les profils des deux candidats le plus en adéquation avec notre culture du travail.

Afin de répondre à ces problématiques, il est réalisé :
- Une note de synthèse suivant l'étude de la législation en vigueur dans le monde de l'entreprise concernant l'utilisation de l'outil informatique, les moyens à mettre en œuvre pour la sécurité des fichiers, la fonction et la valeur d'une charte informatique, et le filtrage de contenu
- Un plan de sécurisation des données via une politique de mots de passe, et les mesures de protection et de sauvegarde des données
- Une charte Qualité Service Client, recensant les propositions sur les engagements qualités, qui sera remise au client AutoConcept
- Un mémo à diffuser en interne sur la conduite à tenir au contact de clients.

II) LEGISLATION EN VIGUEUR SUR L'INFORMATIQUE

A) Utilisation de l'outil informatique en entreprise

Un employé a le droit au respect de sa vie privée et au secret de ses correspondances privées (article 9 du code civil, étendu au milieu professionnel par l'arrêt « Nikon » du 2 octobre 2001 de la Cour de cassation). Puisqu'il s'agit d'outils professionnels, un employeur peut ouvrir et contrôler les courriels échangés, les sites Internet qui ont été consultés, et les fichiers ou documents stockés par l'utilisateur car ils sont présumés avoir un caractère professionnel. Pour qu'ils soient protégés, et donc non consultable par l'employeur, les messages personnels, fichiers et documents doivent être expressément identifiés comme étant « Personnel » ou « Privé », ou en les stockant dans un répertoire portant là aussi une mention « Personnel » ou « Privé ». (Cour de cassation, 30 mai 2007 pour les courriels, Cour de cassation, 18 octobre 2006 pour les fichiers).

Attention : Les courriels, fichiers et documents ne seront pas considérés comme personnels du simple fait de leur classement dans un répertoire nommé « Mes Documents » ou dans un dossier identifié par les initiales de l'employé.

Dans le cas où des fichiers sont identifiés comme personnels, l'employeur peut y accéder en présence de l'employé ou après l'avoir appelé, ou en cas de risque ou évènement particulier qu'il appartient aux juridictions d'apprécier.
Pour les courriers personnels, seule une procédure judiciaire saurait lever cette protection.

Attention : Le fait de volontairement porter atteinte à l'intimité de la vie privée d'autrui, et la violation du secret des correspondances sont des infractions pénalement sanctionnées respectivement par les articles L.226-1 et L.226-15 du Code pénal.

Conformément à l'article L.1321-4 du Code du travail, les instances représentatives du personnel (Comité d'Entreprise, ou Comité Technique, ou délégué du personnel, et Comité d'Hygiène et de Sécurité) doivent être informées puis consultées avant la mise en œuvre d'un dispositif de contrôle de l'activité des salariés. Les employés doivent être aussi être préalablement informés individuellement (articles L.1222-3 et L.1222-4 du Code du travail) de la finalité du dispositif et de la durée pendant laquelle les données de connexion sont conservées ou sauvegardées. En cas d'archivage automatique des messages électroniques, ils doivent en outre être informés des modalités de l'archivage, de la durée de conservation des messages, et des modalités d'exercice de leur droit d'accès.

La messagerie professionnelle doit faire l'objet d'une déclaration de conformité en référence à la norme simplifiée n° NS-046 (gestion des personnels des organismes publics et privés). Si un dispositif de contrôle individuel de la messagerie est mis en place, il doit être déclaré à la Commission Nationale de l'Informatique et des Libertés (CNIL) sauf désignation d'un Correspondant Informatique et Libertés (CIL).

Attention : Tout fichier ou traitement automatisé contenant des informations à caractère personnel doit être déclaré avant sa création, en ligne ou par courrier adressé à la CNIL, sauf désignation d'un CIL, et les salariés doivent être informés :
- des finalités poursuivies par le dispositif
- des destinataires des données
- de son droit d'opposition pour motif légitime
- de son droit d'accès et de rectification des données le concernant

B) Contrôle de l'utilisation d'Internet et filtrage

Selon la CNIL[1], Il est possible pour l'employeur de contrôler et limiter l'utilisation d'Internet (filtrage de sites, détection de virus, empêchement des téléchargements,…) et de la messagerie (outils de mesure de la fréquence des envois et/ou de la taille des messages, filtres «anti-spam»,...), afin d'assurer la sécurité des réseaux qui pourraient subir des attaques (virus, cheval de troie,...) et de limiter les risques d'abus d'une utilisation trop personnelle d'Internet ou de la messagerie (consultation de sa messagerie personnelle, achats de produits, de voyages, discussions sur les réseaux sociaux,…).
Toutefois, en lien avec l'article L.1121-1 du code du travail, certaines limites s'appliquent au pouvoir de l'employeur. Par exemple il serait jugé excessif que celui-ci reçoive une copie automatique de tous les messages écrits ou reçus par ses employés. De même l'utilisation de « keylogger » (enregistrement de toutes les actions accomplies sur un ordinateur) est considérée illicite, sauf dans des circonstances exceptionnelles de sécurité.

[1] https://www.cnil.fr/sites/default/files/atoms/files/_travail-vie_privee_outils_informatiques_travail.pdf

L'article 6-1 de la Loi pour la Confiance dans l'Economie Numérique obligeant les fournisseurs d'accès Internet de mettre en place des filtres et de conserver pendant un an les données de connexions est étendu à tous ceux qui offrent un accès à Internet via la loi antiterroriste du 23 janvier 2006, et donc aux entreprises. Il y a donc obligation pour l'employeur mettre en œuvre les moyens pour interdire les accès à des sites illicites par leur contenu selon le droit français (protection des mineurs, protection des droits d'auteur, racisme, incitation à la haine, négationnisme, jeux en lignes illicites, commercialisation de certains produits,…), et de téléchargements de fichiers ou logiciels piratés.
Ces moyens doivent rester non-discriminatoires.

De plus :
- Selon les articles 121-1 et 121-2 du Code pénal, l'entreprise et le dirigeant sont responsables au pénal de leurs propres actes ainsi que des actes de leurs salariés si l'entreprise est bénéficiaire de l'acte déviant.
- Selon les articles 1383 et 1384 du Code Civil, l'entreprise et le dirigeant sont responsables de ne pas avoir mis en œuvre les moyens nécessaires pour éviter toutes déviances et sont responsables des actes des salariés.
Ces fautes peuvent retomber sur la direction du service informatique pour négligence fautive, incompétence professionnelle, ou pour l'exécution de demandes illicites de l'employeur (notamment en matière de filtrage).

A nouveau**,** les instances représentatives du personnel doivent avoir été informées et consultées (article L.1321-4 du Code du travail) sur les dispositifs et la mise en place des modalités de contrôle de l'utilisation d'Internet, et les salariés informés préalablement (articles L.1222-3 et L.1222-4 du Code du travail) de la finalité du dispositif de contrôle et de la durée pendant laquelle les données de connexion sont conservées.

Attention : La mise en place d'une solution de filtrage Internet collectant des données personnelles (logs, durée de visite de sites Web …) doit être déclarée à la CNIL, et entraine l'obligation de la mise en place d'une Charte informatique. Selon la loi, les logs doivent être conservés 1 an, et les modalités de conservation doivent figurer dans ladite Charte.

C) Obligation de sécurisation des données

L'article 34 de la loi 78-17 du 6 janvier 1978, dite Loi Informatique et Libertés, encadre le traitement des données à caractère personnel et impose que « le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »

La CNIL a ainsi publié un rapport recensant « 10 conseils pour la sécurité de votre système d'information »[2]. Ces recommandations constituent la formalisation d'un plan de sécurité, via :

- la mise en place d'un système d'authentification via des comptes utilisateurs nominatifs, qui détermineront d'ailleurs l'accès limité des fichiers aux seules personnes identifiées comme en ayant besoin
- une politique de mot de passe forts, renouvelables fréquemment, et modifiés par l'utilisateur à chaque renouvellement
- la sécurisation des postes de travail (verrouillage des postes, limitation des copies via USB), du réseau local (pare-feu, routeur filtrant, VPN, cryptage et authentification pour les accès sans fils, HTTPS) et des locaux (gardiennage, clés/digicode/badge)
- s'assurer de la confidentialité des prestataires
- sensibiliser les utilisateurs aux risques et au bon comportement à adopter (via des notes internes, des fiches pratiques ou une Charte informatique notamment)
- anticiper la fuite et la perte de données avec un stockage sécurisé et à part des données, la mise en place d'une procédure de secours en cas d'urgence ou de sinistre, et le nettoyage du matériel dont on se sépare.

D) Fonction et valeur d'une Charte informatique

La Charte informatique est un outil recommandé par la CNIL, qui permet de définir les risques, les règles et les limites de l'utilisation du système d'information par tout utilisateur (salarié, stagiaire, employeur, visiteur,…). Elle permet aussi de les informer sur les moyens de surveillances et les données conservées, et doit rester conforme à l'article L.1121-1 du Code du travail, stipulant que les restrictions des droits des personnes et des libertés individuelles doivent rester proportionnelles au but recherché. En effet, l'interdiction pure et simple de toute utilisation privée d'Internet et des outils informatiques rendrait cette Charte caduque, et donc l'assistance d'un juriste spécialisé est fortement conseillée pour la rédaction d'une Charte valide. Pour rappel : Une Charte est obligatoire dès que l'on met en place une collecte des données à caractère personnel.

Pour qu'elle soit opposable aux utilisateurs, la Charte doit être déployée comme faisant partie du règlement intérieur. Pour cela, en accord avec l'article L.1321-4 du Code du travail, il faut la présenter aux instances représentatives du personnel un mois avant de les consulter, en sachant qu'un avis négatif n'empêche pas la mise en place de la Charte (ni d'ailleurs d'une solution de filtrage). Dans un second temps, la Charte doit ensuite être diffusée aux utilisateurs individuellement, et collectivement par affichage public dans un espace accessible sur le lieu de travail. (article R1321-1 du Code du travail).

[2] https://www.cnil.fr/fr/10-conseils-pour-la-securite-de-votre-systeme-dinformation

Enfin dans le cas où des employés dépendent du droit du travail, la Charte doit être déposée au Greffe du conseil des prud'hommes, et transmise à l'Inspection du travail en deux exemplaires. (articles R.1321-2 et R.1321-4 du Code du travail).

Attention : A chaque modification de la Charte, il faudra à nouveau procéder de la même manière.

III) Plan de sécurisation des données

A) Politique de mots de passe

Selon les précautions de l'ANSSI et de la CNIL, nous allons mettre en place l'utilisation de mots de passes fort, c'est-à-dire :
- des mots de passes longs (8 caractères minimum)
- constitués de caractères variés (varier minuscules/majuscules, garder la ponctuation, écrire les nombres en chiffres de 0 à 9)
- faciles à retenir (pour éviter d'avoir à écrire le mot de passe pour ne pas l'oublier).

Exemple avec la méthode des premières lettres :
C'est un fameux trois-mâts, hisse et ho => **C'e1F3M,hEo**

Un mot de passe initial sera fourni à l'utilisateur, qui devra obligatoirement le modifier après sa première connexion, en se conformant à la politique de mots de passe en vigueur. Ceux-ci auront une date de validité maximale de 3 mois, au bout de laquelle le mot de passe devra à nouveau être changé, avec impossibilité de réutiliser un des 3 derniers mots de passe créés. En parallèle, au bout de 5 tentatives échouées de connexion, le verrouillage du compte s'effectuera pendant 10 minutes.

Enfin, via un document récapitulatif envoyé individuellement par courriel à chacun, les utilisateurs seront sensibilisés sur :
- le danger que représentent les logiciels ou navigateurs proposant de retenir le mot de passe pour les futures utilisations
- la nécessité de veiller à la confidentialité de leur mot de passe et les erreurs à éviter, telles qu'écrire son mot de passe dans un fichier ou sur un papier, choisir un mot de passe ayant un lien direct avec l'utilisateur, ou de communique le mot de passe à un tiers
- l'habitude à prendre de verrouiller son poste quand on doit s'en éloigner
- la nécessité de changer son mot de passe dès qu'on à le moindre soupçon qu'il à été compromis.

B) Authentification et droits d'accès aux fichiers

Utilisation d'Active Directory pour :
- centraliser l'identification et l'authentification des utilisateurs
- cloisonner les accès aux fichiers selon les groupes d'utilisateurs créés dans Active Directory, régit par les administrateurs. Chaque compte utilisateur sera intégré dans un groupe définissant les accès possibles aux ressources partagées sur le réseau, dans la limite de ses besoins pour son activité
- réaliser une gestion des téléchargements et le déploiement des logiciels uniquement par les administrateurs.

C) Sécurisation des postes

Afin d'assurer une bonne sécurisation des postes, nous allons mettre en place, selon les recommandations de la CNIL, et en plus des mesures déjà décidées :
- un verrouillage automatique des postes après 10 minutes d'inactivité
- le déploiement sur chaque poste d'une protection antivirale **«** Symantec Endpoint Protection Small Business Edition », déployable aussi sur le serveur d'AutoConcept
- un pare-feu logiciel lui aussi pris en compte par la solution « Symantec Endpoint Protection Small Business Edition **»**, où l'on pourra limiter les ports de communication non nécessaires au fonctionnement de l'entreprise
- un VPN utilisant le chiffrement pour sécuriser les accès à distance.

D) Mesures de sauvegarde

Dédié uniquement à la sauvegarde, on mettra en place un NAS, configuré en RAID 5.
Le RAID 5 est très intéressant, autant pour ses performances que sa fiabilité. En effet, avec la segmentation des données, et la répartition entre les disques avec une information de parité sur chaque donnée, Le RAID 5 offre de très bonnes performances en écriture et en lecture, et supporte la panne d'un disque dur. Les données seront alors régénérées sur le nouveau disque après remplacement.

Nous choisirons une sauvegarde différentielle, car elle présente l'intérêt d'avoir un temps de restauration des données plus court que l'incrémentielle, mais en prenant plus d'espace de stockage. Toutefois avec un NAS à 5 baies on peut facilement obtenir entre 16 à 24 To de capacité selon les disques durs choisis, ce qui devrait être largement suffisant pour le parc de 76 postes d'AutoConcept. La sauvegarde totale s'effectuera chaque vendredi à 18, et tous les jours à 12h et 18h pour les différentielles, où chaque sauvegarde contiendra donc toutes les modifications et nouveautés apportés depuis la dernière sauvegarde totale. Ainsi pour la restauration on aura uniquement à déployer la sauvegarde totale, et celle du jour la plus récente.

Les sauvegardes du NAS seront aussi toutes systématiquement copiées sur un disque dur qui sera conservé dans un coffre ignifugé et étanche dans un endroit différent.

Enfin on utilisera des onduleurs afin de protéger le serveur et le NAS alloués à AutoConcept des coupures de courant et de stabiliser les tensions arrivant à ces appareils, qui seront surélevés par rapport au sol pour éviter de potentiels dégâts d'inondation, et dans des salles pourvues de détecteurs de fumées et d'extincteurs.

Charte Qualité Service Client

SUPPORT 2000 S'ENGAGE AUPRES DE VOUS !

Nos techniciens sont des professionnels qualifiés dans le support et le relationnel client au sein d'une structure présente depuis **plus de 15 ans**, et sont à votre écoute sur notre **Hotline du lundi au samedi, de 8h à 19h**.

Un matériel tombe en panne ? Afin d'assurer une **continuité de service**, nous vous remplaçons votre matériel par **l'équivalent** en terme de performances, de qualité et de confort dès le jour de signalement de la panne.

Dès le signalement d'une panne, il vous est confié un **numéro d'intervention** qui vous permet de consulter sur notre site le suivi en détail de votre dépannage.

Nos interventions répondent de manière rapide et proportionnée à votre problème, avec :

- Un **délai moyen de 15 min maximum** pour la résolution d'incidents à distance *
- Une intervention sur site possible **dès le jour du signalement de l'incident** **
- Une priorisation des interventions selon leur gravité et leur impact sur le système d'information.

SUPPORT 2000 C'EST AUSSI :

L'assurance de l'utilisation et du déploiement de logiciels certifiés et légaux avec notre **gestion des licences**.

Une **charte de confidentialité** signée par chacun de nos techniciens afin de protéger l'intégrité de votre système d'information et de toute information qui nous est confiée.

Des **rendez-vous** réguliers pour vous informer des avancées technologiques, et **vous conseiller** dans l'évolution de votre parc informatique.

La possibilité à la fin du dépannage d'utiliser votre **numéro d'intervention** pour signaler à nos équipes d'éventuelles **améliorations à apporter à notre service**. **Votre voix à de l'importance !**

**Délai moyen maximum constaté dans 90% des interventions à distance*
*** Jusqu'à J+2 maximum selon la gravité et la disponibilité des techniciens*

Note à l'attention du personnel :
Conduite à tenir auprès des clients

EN HOTLINE

- Présentez-vous en prenant l'appel, adoptez une attitude polie, conviviale et sérieuse
- Expliquez la nature de l'intervention qui va être réalisée (remplacement de matériel, dépannage a distance, intervention sur site, et délais)
- Adaptez votre vocabulaire en fonction de la personne en face, vous vous adressez peut-être à un néophyte
- Réalisez l'ouverture de la fiche d'intervention, communiquez le numéro d'intervention

EN INTERVENTION

- Gardez une attitude polie, conviviale et sérieuse
- Respectez les horaires et délais fixés, et si cas exceptionnel : informez le plus tôt possible le client en cas de retard ou de changement de programme
- Expliquez simplement les procédures que vous allez réaliser
- Assurez-vous que le matériel de remplacement correspond à celui qui est changé
- Confirmez avec l'utilisateur que le problème est bien résolu avant de terminer l'intervention
- Vous représentez le professionnalisme et le sérieux de l'entreprise, une tenue correcte est exigée

EN GENERAL

- Assurez le suivi et la traçabilité de vos actions de dépannage, informer en cas de délais supplémentaires
- Restez respectueux de la confidentialité de toute information dont vous pourriez avoir connaissance
- Signalez toute infraction à la légalité à votre responsable (ex : produits pirates) et réalisez la mise en conformité par rapport aux règles ou à la loi
- Soyez pédagogue, si possible expliquez la cause de la panne et comment l'éviter
- Chaque panne est importante, ne négligez aucune demande sous prétexte qu'elle n'est pas prioritaire

ANNEXES

Annexe 1 : Compte-rendu des problèmes rencontrés par la société AUTOCONCEPT avec son service informatique actuel

- La société AutoConcept a choisi d'amortir son matériel sur 3 ans. La chef comptable est très réticente à tout renouvellement avant la fin de la période d'amortissement.
- Lenteur de certains postes.
- Crash disque du poste d'un commercial : perte d'exploitation 80 000 euros.
- Intrusion d'un client sur un poste d'une commerciale dépourvu de mot de passe
- Plaintes des utilisateurs sur le service informatique :
    - Délais d'intervention : un poste d'une secrétaire commerciale est parti en SAV durant 2 jours. Elle n'a pas pu terminer un document pour conclure une affaire. Perte : 60 000 euros.
    - Attitude des techniciens : absence d'explication sur les interventions, ou discours parfois trop technique.
    - Messages intempestifs de « version de Windows pirates »
    - Tenue des informaticiens : « un matin, l'un d'eux est arrivé en jogging pour dépanner un poste alors qu'un commercial était avec un client ». Un autre a répondu de manière déplacée à la demande d'un utilisateur de le dépanner.
    - Une intervention urgente planifiée pour le lundi 10h a été traitée le mercredi à 10h.
    - Un utilisateur du service commercial se plaint que son poste, après plusieurs séjours au SAV, présente toujours les mêmes symptômes.
    - Un utilisateur de la comptabilité soupçonne le SAV d'avoir consulté des documents confidentiels sur son poste lors d'une intervention. Ces informations ont été divulguées à des tiers.
    - Un utilisateur de l'atelier rapporte qu'il a dû insister auprès du service informatique pour retrouver son écran d'origine. Un écran plus petit lui avait été remis après une intervention.
    - Un utilisateur du service « Véhicules d'occasion » se plaint depuis plusieurs mois d'avoir des problèmes avec sa souris. Personne n'a répondu à son problème.
    - Plusieurs utilisateurs se plaignent de l'accueil téléphonique du service informatique.
    - Une bonne partie des utilisateurs se plaignent de voir leurs postes partir en SAV sans savoir quand il reviendra.
    - Un utilisateur signale que son MSN ne fonctionne pas et souhaite que son poste soit réparé rapidement. (NB : la direction a demandé au service informatique de bloquer MSN. Depuis la productivité a considérablement augmenté).

Annexe 2 : Textes de lois

CODE DU TRAVAIL

Article L.1121-1 : Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.

Article L.1222-3 : Le salarié est expressément informé, préalablement à leur mise en œuvre, des méthodes et techniques d'évaluation professionnelles mises en œuvre à son égard.
Les résultats obtenus sont confidentiels.
Les méthodes et techniques d'évaluation des salariés doivent être pertinentes au regard de la finalité poursuivie.

Article L.1222-4 : Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance

Article L.1321-4 : Le règlement intérieur ne peut être introduit qu'après avoir été soumis à l'avis du comité d'entreprise ou, à défaut, des délégués du personnel ainsi que, pour les matières relevant de sa compétence, à l'avis du comité d'hygiène, de sécurité et des conditions de travail.

Le règlement intérieur indique la date de son entrée en vigueur. Cette date doit être postérieure d'un mois à l'accomplissement des formalités de dépôt et de publicité.
En même temps qu'il fait l'objet des mesures de publicité, le règlement intérieur, accompagné de l'avis du comité d'entreprise ou, à défaut, des délégués du personnel et, le cas échéant, du comité d'hygiène, de sécurité et des conditions de travail, est communiqué à l'inspecteur du travail.

Ces dispositions s'appliquent également en cas de modification ou de retrait des clauses du règlement intérieur.

Article R.1321-1 : Le règlement intérieur est porté, par tout moyen, à la connaissance des personnes ayant accès aux lieux de travail ou aux locaux où se fait l'embauche.

Article R.1321-2 : Le règlement intérieur est déposé, en application du deuxième alinéa de l'article L. 1321-4, au greffe du conseil de prud'hommes du ressort de l'entreprise ou de l'établissement.

Article R.1321-4 : Le texte du règlement intérieur est transmis à l'inspecteur du travail en deux exemplaires.

CODE PENAL

Article 121-1 : Nul n'est responsable pénalement que de son propre fait

Article 121-2 : Les personnes morales, à l'exclusion de l'Etat, sont responsables pénalement, selon les distinctions des articles 121-4 à 121-7, des infractions commises, pour leur compte, par leurs organes ou représentants.

Toutefois, les collectivités territoriales et leurs groupements ne sont responsables pénalement que des infractions commises dans l'exercice d'activités susceptibles de faire l'objet de conventions de délégation de service public.

La responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits, sous réserve des dispositions du quatrième alinéa de l'article 121-3.
Article 121-3 : Il n'y a point de crime ou de délit sans intention de le commettre.

Toutefois, lorsque la loi le prévoit, il y a délit en cas de mise en danger délibérée de la personne d'autrui.

Il y a également délit, lorsque la loi le prévoit, en cas de faute d'imprudence, de négligence ou de manquement à une obligation de prudence ou de sécurité prévue par la loi ou le règlement, s'il est établi que l'auteur des faits n'a pas accompli les diligences normales compte tenu, le cas échéant, de la nature de ses missions ou de ses fonctions, de ses compétences ainsi que du pouvoir et des moyens dont il disposait.

Dans le cas prévu par l'alinéa qui précède, les personnes physiques qui n'ont pas causé directement le dommage, mais qui ont créé ou contribué à créer la situation qui a permis la réalisation du dommage ou qui n'ont pas pris les mesures permettant de l'éviter, sont responsables pénalement s'il est établi qu'elles ont, soit violé de façon manifestement délibérée une obligation particulière de prudence ou de sécurité prévue par la loi ou le règlement, soit commis une faute caractérisée et qui exposait autrui à un risque d'une particulière gravité qu'elles ne pouvaient ignorer.

Il n'y a point de contravention en cas de force majeure.

Article L.226-1 : Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :

1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;

2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.

Lorsque les actes mentionnés au présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé.

Article L.226-15 : Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende.

Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions.

CODE CIVIL

Article 1383 : Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence.

Article 1384 : 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, ou des choses que l'on a sous sa garde.

Toutefois, celui qui détient, à un titre quelconque, tout ou partie de l'immeuble ou des biens mobiliers dans lesquels un incendie a pris naissance ne sera responsable, vis-à-vis des tiers, des dommages causés par cet incendie que s'il est prouvé qu'il doit être attribué à sa faute ou à la faute des personnes dont il est responsable.

Cette disposition ne s'applique pas aux rapports entre propriétaires et locataires, qui demeurent régis par les articles 1733 et 1734 du code civil.

Le père et la mère, en tant qu'ils exercent l'autorité parentale, sont solidairement responsables du dommage causé par leurs enfants mineurs habitant avec eux.

Les maîtres et les commettants, du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés ;

Les instituteurs et les artisans, du dommage causé par leurs élèves et apprentis pendant le temps qu'ils sont sous leur surveillance.

La responsabilité ci-dessus a lieu, à moins que les père et mère et les artisans ne prouvent qu'ils n'ont pu empêcher le fait qui donne lieu à cette responsabilité.

En ce qui concerne les instituteurs, les fautes, imprudences ou négligences invoquées contre eux comme ayant causé le fait dommageable, devront être prouvées, conformément au droit commun, par le demandeur, à l'instance.

AUTRES TEXTES DE LOI :

Article 34 de la loi 78-17 du 6 Janvier 1978 : Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Article 6-1 de la Loi pour la Confiance dans l'Economie Numérique : Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens.
Les personnes visées à l'alinéa précédent les informent également de l'existence de moyens de sécurisation permettant de prévenir les manquements à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle et leur proposent au moins un des moyens figurant sur la liste prévue au deuxième alinéa de l'article L. 331-26 du même code.

Annexe 3 : Glossaire

CNIL : Créée en janvier 1978, La Commission Nationale de l'Informatique et des Libertés est une autorité administrative indépendante française. Composée de parlementaires, de représentants des hautes juridictions et de personnalités qualifiées, la CNIL est chargée de veiller au respect des droits et des libertés de chacun dans l'univers informatique.
La CNIL ne reçoit d'instruction d'aucune autorité, et on ne peut s'opposer à son action. Enfin, ses délibérations peuvent faire l'objet de recours devant le Conseil d'État.

CIL : Le Correspondant Informatique et Liberté est une personne morale, nommée au sein d'une entreprise (ou d'une collectivité) pour assurer un rôle d'intermédiaire entre celle-ci et la CNIL. Avec des compétences en informatique et en droit, il veille au respect de la loi Informatique et Libertés

ANSSI : L'Agence Nationale de la Sécurité des Systèmes d'Information est un service à compétence nationale rattachée au Secrétaire général de la défense et de la sécurité nationale. Elle propose des règles visant à protéger les systèmes d'information de l'Etat, et assure une veille face aux attaques informatiques sur les réseaux de l'Etat.

VPN : Un Réseau Privé Virtuel (*Virtual Private Network*) permet de relier deux ordinateurs distants (avec possibilité de chiffrement pour rester privé) comme s'ils étaient connectés en local, via Internet

NAS : Un NAS (*Network Attached Storage*) est un boitier de stockage en réseau, fonctionnant comme un serveur de fichiers.

RAID : Technologie de stockage permettant de copier des données sur plusieurs disques durs, par répartition ou en redondance (selon le type de raid choisi)

RAID 0 : Les données sont séparées en autant de disques durs, et chaque partie est copiée sur un disque différent, ce qui augmente les performances en écriture et en lecture, mais la perte d'un disque entraine la perte de l'intégralité des données.

RAID 1 : Les données sont copiées intégralement sur chaque disque dur, en miroir. Cela offre un bon niveau de protection, mais des performances plus faibles et requiert plus d'espace de stockage.

RAID 5 : Avec un minimum de trois disques durs, les données sont réparties entre les disques avec des informations de parité. Ainsi en cas de panne, les données manquantes sont reconstruites à partir de ces informations. Le RAID 5 offre une très bonne sécurité et une bonne performance en lecture.

Annexe 4 : Sources utilisées pour la rédaction de ce document

« Guide LA SECURITE DES DONNEES PERSONNES », Edition 2010, CNIL
« LE GUIDE DE LA CHARTE DES SYSTEMES D'INFORMATIONS », Olféo et Cabinet Alain BENSOUSSAN Avocats
« LIVRE BLANC JURIDIQUE : Filtrage et Internet au bureau : Enjeux et cadre juridique en France », Olféo et Cabinet Alain BENSOUSSAN Avocats
Note technique « Recommandations de sécurité relatives aux mots de passe », ANSSI
https://www.cnil.fr/professionnel
http://www.ssi.gouv.fr/
https://www.legifrance.gouv.fr/
https://www.service-public.fr/professionnels-entreprises
http://www.juritravail.com/
http://www.net-iris.fr/
http://www.egedian.com/
https://www.olfeo.com/
http://www.cil.cnrs.fr/CIL/