5.1 : Sécurisation des données

Q1 :

Le patrimoine informationnel peut être considérer comme l'ensemble des données et des connaissance, protégés ou non, valorisable ou historique d'une personne physique ou morale. IL s'agit donc d'assurer la protection et la valorisation de l'information. A ce titre l'information doit être sécurisé depuis sa création ou sa collecte tant pendant la phase de transmission tant pendant la phase de conservation.

Q2 :

Le patrimoine informationnel est constitué par l'ensemble des informations dont dispose la société et notamment des données clients et fournisseurs, des logiciels maisons et documenté, du savoir-faire de l'entreprise, des brevets, ou encore des bdd. En conséquence ce sont toutes les données techniques, commerciales, stratégiques, économiques et financières. Leurs valeurs économiques est certaine pour l'entreprise. Ces données numériques doivent donc faire l'objet d'une grande vigilance de la part du responsable informatique en premier lieu et de tous les collaborateurs de l'entreprise.

Q3 :

On put distinguer 2 types de risques pour l’entreprise, premièrement un risque interne dans l’entreprise dû à l’agissement des collaborateurs. (ex : la sécurisation insuffisantes des accès aux services informatique, un non-respect des habilitations qui ont été posé au préalable, une divulgation ou perte volontaire ou par négligence d’information confidentielle voire sensible, mais également en raison de la défaillance des équipements matériels. Le deuxième risque est dû à l’extérieur de l’entreprise souvent malveillant, cela peut se caractérise par une altération volontaire de l’info, ou un vol de l‘info, des destructions de données à la suite d’un intrusion info, ou encore un espionnage économique. Donc le droit pénal sanctionne la criminalité informatique ou cyber -criminalité. La cybercriminalité est définie comme une activité illégale commise à l’égard des systèmes d’information à l’aide des technologies de l’info et des communications. Sont ainsi sanctionné par le code pénal : 1er les intrusions illégales dans un ordinateur ou le fait d’accéder ou de se maintenir frauduleusement dans tout ou partie du système de traitement automatisé. 2eme les atteintes au système de données autrement dit toute perturbation de l’info, le fait d’entravé ou de faussé le fonctionnement d’un système de traitement automatisé de données ou encore le fait de supprimer ou modifier les données qu’il contient. La tentative est punie par le code pénal.

Q4 :

La charte informatique est un document contractuel qui répertoriée notamment les règles en matière de sécurité informatique. Cette charte est généralement intégrée au règlement intérieur de l’entreprise et qu’elle s’impose à tous les salariés. Et que cette charte a pour vocation de posé les droits et obligations lié au système informatique de tous les collaborateurs de l’entreprise. Le non-respect de cette charte peut entrainer des sanctions disciplinaires pouvant aller jusqu’au licenciement.

Q5 :

Les contrats de travail peuvent comporter des clauses explicites en matière de sécurité informatique. Ces clauses prennent généralement 2 formes, la première étant la clause de confidentialité : cette clause oblige au salarié, une obligation de silence devant être déterminé dans le temps et en fonction de projet spécifique. La deuxième est une clause en cas de départ de l’entreprise, cette clause put prendre la forme d’une clause de non-concurrence. La clause de restitution des mémoires externe en cas de départ de l’entreprise, clause à travers laquelle le salarié rend les mémoires qu’il acquit dans l’entreprise.

Cas particulier des prestataires externe : la relation avec la prestataire externe peut être également encadrés par les clauses spécifiques. En pratique avec les prestataires externes est posé la clause de réversibilité (c’est une clause qui prévoit le sort des donnes confié au partenaire potentielle si la relation contractuelle n’aboutisser pas) et qui est sanctionné par des dommages et intérêt en cas de non-respect.

Q6 :

Les audits de sécurité du systèmes informatique afin d’en identifier les failles, la sécurisation du système informatiques contre des attaques externe (anti-virus, firewall,.. ), la mise en place d’un contrôle d’accès au information avec différentes habilitation, des moyens d’identification et d’authentification des utilisateurs, une procédure de chiffrement des données ou encore un recours au signature électroniques.

Q7 :

C’est toute information relative à une personne physique identifié ou identifiable, directement ou indirectement par référence à un numéro d’identification, ou un ou plusieurs éléments qu’il lui sont propres.

Q8 :

Les données sensibles peuvent être caractérisé comme les informations relatives à l’origine, la santé, la sexualité, ou encore les empreintes digitales. IL est en principe interdit de collecter les données sensibles sauf consentement express de l’interecet.

Q9 :

Un traitement de données à caractère personnel est caractérisé par toute opération ou ensemble d’infos qui portent sur des donnés personnels, quelque soit le procédé utilisé et notamment la collecte, l’enregistrent, l’organisation, la conservation, l’adaptation ou modification, l’extraction, la consultation, l’utilisation, la communication par transmission, la diffusion ou tout autre forme de disposition, le rapprochement, ainsi que l’effacement ou la destruction.

Q10 :

La collecte et traitement des données personnels doivent être effectué de façon licite et loyale (ce qui a été dit doit être respecté), et que l’utilisateur doit être informé de la collecte de ses données, les finalités du traitement de ces données doivent être déterminés, explicites et légitimes.

La CNIL doit être informé de toute collecte de données à caractère personnel. En revanche certains fichiers requièrent une autorisation expresse de la CNIL et notamment les fichiers à caractère sensibles (ceux lié à la santé).

L’obligation de sécurité à caractère personnel vise principalement les tiers, la loi oblige le collecteur de mettre en place des procédure techniques afin de les protéger.

En cas de conservation interne il convient d’élaborer une charte concernant les bonnes pratiques à adopter. En cas de conservation externe de données le tiers archiveur doit prendre toutes les mesures afin de garantir que les documents archivés soit accessible à la seule personne habilitée et qu’elles ne soient pas endommagées.

L’information d’archivage doit être délivré au personnel auxquels on collecte les données. Ces personnes doivent être informés de leur droit en matière de collecte de données. Il existe 4 droits à la personne où l’on collecte les données : le droit d’opposition, le droit d’accès, le droit de rectification, le droit de suppression.

IV)

Q11 :

Le montant à partir duquel un écrit constatant l’exitance d’un contrat électronique entre un consommateur et un professionnel doit être conservé sur un support électronique est de 120€.

Q12 :

Le professionnel dispose de l’obligation de conservé l’écrit pendant 10 ans, de plus il doit en vertu de l’obligation de transparence garantir à tout moment l’accès de ces informations au co-contractant des lors qu’il en fait la demande. Le professionnel doit évidemment respecter la licéité et l’ordre public en matière de conservation de ces données.