SECURITE DES DONNEES
Aspects juridiques et pratiques

FICHE INFO DU PPDT

DU MOYEN-AGE A NOS JOURS

Au Moyen-Âge, on protégeait ses deniers (et non pas ses données), ainsi que les joyaux de la couronne, et ce généralement dans l'enceinte d'un château fort situé autant que faire se peut dans un endroit stratégique difficilement accessible, par exemple en haut d'une colline.

L'invention de l'imprimerie a multiplié les documents en circulation, et donc les documents à protéger. L'apparition des photocopieuses et imprimantes de bureau au XXème siècle a encore accéléré le mouvement. De la forteresse, on est passé au coffre-fort.

Le XXIème siècle marque un nouveau tournant avec l'extension d'Internet et l'électronisation des documents, sans oublier, en parallèle, la multiplication des supports de données, tant immobiles que mobiles et même volatiles (pour les données stockées dans le cloud).

La quantité de données à protéger suit désormais une courbe exponentielle. Du coffre-fort, on passe au coffre-fort électronique (l'e-coffre-fort).

CADRE JURIDIQUE

La multiplication des données et des supports a pour conséquence une complexification croissante de la protection des données. Toute entité, qu'elle soit publique ou privée, est soumise au respect d'un cadre juridique où le principe de sécurité doit guider toutes les actions.

LIPAD et loi fédérale sur la protection des données (LPD)

A Genève, les institutions publiques cantonales, communales et intercommunales sont soumises au champ d'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD; RSGE A 2 08).

La loi fédérale sur la protection des données (LPD; RS 235.1) constitue ce cadre juridique pour les autorités fédérales et le secteur privé. Les associations subventionnées par une entité publique genevoise, les fondations de droit privé et autres entreprises qui travaillent avec l'Etat ne sont pas soumises à la LIPAD, mais à la LPD. La LPD est placée sous l'autorité du Préposé fédéral à la protection des données et à la transparence (PFPDT).

Ces lois visent une protection très stricte de la vie privée, en interdisant pratiquement tout traitement de données non explicitement autorisé par la personne intéressée, le but étant de protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données. Elles traitent aussi bien des personnes physiques que morales.

Le principe fondamental de sécurité

En vertu de ce principe, toutes les mesures nécessaires, tant techniques qu'opérationnelles, doivent être mises en place pour protéger les données personnelles (sensibles ou non) et éviter tout traitement non autorisé de celles-ci. Il est posé par l'art. 37 LIPAD.

Outre ce dernier, toute institution doit par ailleurs veiller au respect des autres principes suivants :

- ***Principe de légalité/licéité*** : tout traitement de données doit être licite et les données ne doivent pas être obtenues par crainte ou usurpation.
- ***Principe de bonne foi*** : le traitement et la collecte de données doivent être effectués en toute bonne foi, loyalement et de façon transparente.
- ***Principe de finalité*** : le but du traitement et de la collecte de données doit être clairement et préalablement défini. Dans le cas de données sensibles, le consentement de la personne concernée doit être explicite.
- ***Principe de proportionnalité*** : les données collectées ne doivent être traitées que dans le but indiqué lors de leur collecte.

- ***Principe de reconnaissabilité*** : la collecte des données et les finalités du traitement de celles-ci doivent être reconnaissables pour la personne concernée.
- ***Principe d'exactitude*** : les données collectées doivent être exactes et mises à jour quand c'est nécessaire.

NOTION DE DONNEE PERSONNELLE

Qu'entend-on par données personnelles ?

Il s'agit de toute donnée qui se rapporte à une personne identifiée ou identifiable, comme le lieu et la date de naissance, le numéro de téléphone, le nom et le prénom, l'adresse (physique ou électronique), le numéro AVS, le numéro d'une carte de crédit, les données médicales, génétiques et biométriques. Les photos d'une personne sont aussi considérées comme des données personnelles.

Qu'entend-on par données sensibles ?

Il peut s'agir d'opinions ou activités religieuses, philosophiques ou politiques, de l'ethnicité, de tout ce qui a trait à la sphère intime, de tout ce qui touche à la santé, de poursuites pénales ou administratives, etc.

L'ACCES AUX DONNEES

La problématique principale, en matière de sécurité des données, ne change pas au fil du temps. Il s'agit de déterminer qui a le droit d'accéder à quelle donnée et de mettre en place les garde-fous adéquats, qui a le droit à une copie de la clé de la salle du trésor (Moyen-Âge), qui a le droit d'être en possession du code secret pour ouvrir le coffre-fort (Temps Modernes), qui a la responsabilité du mot de passe pour accéder au serveur de données de l'entreprise, que celui-ci soit situé dans les locaux de l'entreprise ou sur un serveur accessible via le cloud (XXIème siècle).

Qui a accès aux données de l'institution ?

Comment accède-t-on au système d'information de l'entreprise ? Qui peut y accéder ? Qui gère ces accès ?

La gestion des accès est un domaine clé en matière de sécurité de l'information. ***Il est par conséquent important que ce domaine soit géré en interne***. Le service interne compétent doit veiller au respect des accès en instaurant une politique claire et précise à ce sujet : ***accès nominatifs*** (par le biais d'un "login" ou "nom d'utilisateur") et ***contraignants*** (par le biais d'un mot de passe), ***accès ciblés*** (selon le rôle de l'employé-e dans l'entreprise), ***accès restreints*** (dans le cas d'éventuels intervenants externes). Un-e employé-e du service informatique n'a pas à avoir accès aux documents du service des ressources humaines (fiches salaires par exemple) et inversement.

Le plus important est de déterminer quelles sont les données sensibles et de maîtriser les accès à ces données sensibles, en les restreignant au maximum et en les ouvrant au compte-goutte. Plus fine est la gestion des droits d'accès, meilleure elle s'avère.

De plus, il est nécessaire de limiter les tentatives d'accès, pour contrer les tentatives frauduleuses. Une bonne pratique consiste à bloquer l'accès au système d'information au bout de ***trois essais*** erronés lors de l'introduction du mot de passe, que ces essais se fassent sur un appareil fixe (ordinateur de bureau) ou mobile (ordinateur portable, tablette ou téléphone mobile).

Lorsque l'utilisation d'un outil de prise de contrôle à distance de l'ordinateur des employé-es s'avère nécessaire, le service autorisé à utiliser un tel outil – en général, le support informatique – doit utiliser des accès spécifiques et être formé en conséquence. En effet, ce genre d'outil permet de voir ou d'accéder à des informations qui ne seraient pas accessibles en temps normal. En tout cas, l'accès distant au poste de l'employé-e doit être impérativement validé par ce dernier et n'être valide que de façon temporaire, ni plus ni moins que le temps nécessaire à l'intervention de la personne autorisée. Ainsi, les données seront bien gardées.

Comment protéger l'accès aux informations sensibles ?

Qui connaît les mots de passe ? Quelle est leur complexité ? Quid de l'accès physique aux documents et aux bâtiments ?

Un mot de passe se doit d'être personnel. Même son conjoint ne devrait pas le connaître. Dès qu'il est connu de quelqu'un d'autre ou écrit quelque part (par exemple sur un post-it), le mot de passe perd toute sa valeur. L'idéal consiste donc à se servir d'un outil de gestion des mots de passe, dans lequel les mots de passe n'apparaissent jamais en clair.

Le risque du stockage de mots de passe n'est pas limité au cas de l'employé-e. Si tous les mots de passe sont archivés sur un fichier, ce fichier peut être piraté. Il peut aussi devenir accessible aux yeux d'un fournisseur de service externe si celui-ci a accès au fichier en question, via une connexion à distance.

Qu'importe le niveau de protection du fichier contenant les mots de passe, les pirates ont toujours un coup d'avance. Par contre, ils ne peuvent pas lire dans votre cerveau. ***D'où l'importance aussi de définir des mots de passe dits forts***, c'est-à-dire contenant ***au moins 8 caractères***, et ***un savant mélange de majuscules, de minuscules et de caractères spéciaux*** (chiffres, signes de ponctuation). La fréquence à laquelle chaque mot de passe doit être changé ne devrait pas dépasser un semestre.

Dernier point mais pas le moindre : il faut veiller, lors de chaque déplacement (même un court déplacement vers la machine à café ou les toilettes !), à ***verrouiller sa station de travail***. En effet, à quoi bon définir un mot de passe conforme aux bonnes pratiques de sécurité si le poste de l'employé-e est accessible sans devoir entrer ce mot de passe ?

Au vu du casse-tête chinois que constitue la multiplication des mots de passe, les solutions biométriques commencent à s'imposer, qu'il s'agisse de reconnaissance des empreintes digitales, de reconnaissance faciale ou rétinienne. Ces technologies s'appliquent autant au poste de travail qu'à l'accès physique aux bâtiments de l'entreprise. Elles permettent de gérer l'accès à des salles sensibles, et ce de façon plus efficace que par la multiplication des jeux de clés.

Il est en effet important de savoir qui accède physiquement aux bâtiments de l'entreprise. Si l'accès à la réception principale est généralement et logiquement ouvert aux heures de bureau, au-delà, l'obtention d'un badge – en guise de passe-droit – est recommandée, afin d'éviter que des personnes peu recommandables ne puissent accéder à des postes qui n'auraient pas été verrouillés, ou qu'elles puissent laisser "trainer" leur regard au mauvais endroit, ou pire, s'emparer de documents au format papier...

S'il paraît évident de protéger sa messagerie électronique par un mot de passe et de gérer adéquatement les autorisations pour y accéder, ***on ne prend pas forcément les mêmes précautions pour le courrier physique, les fax ou les documents imprimés***.

Pourtant, ils peuvent aussi renfermer des informations vitales. Il faut donc veiller à utiliser des boîtes aux lettres fermées à clé (même à l'intérieur d'une entreprise), veiller à ce que les fax arrivant ne soient pas visibles aux yeux de tous. De même, il faut avoir la discipline nécessaire pour se rendre à l'imprimante aussitôt un document sensible imprimé et en faire bon usage plutôt que de le laisser bien en vue sur l'imprimante, dans le cas où l'imprimante elle-même ne peut pas être installée loin des regards indiscrets. L'installation d'un système reliant l'imprimante aux badges des employé-es, ne permettant l'impression qu'une fois la personne concernée présente devant l'imprimante, est une solution envisageable pour résoudre la problématique de la localisation de l'imprimante et pour éviter de devoir installer une imprimante dans chaque bureau !

Il faut aussi veiller à prendre en compte le ***cycle de vie des documents*** papier dans son entier, c'est-à-dire jusqu'à ***l'archivage*** des documents dans un lieu adéquatement protégé et en vertu des obligations légales (pour Genève : loi sur les archives publiques du 1er décembre 2000, LArch; RSGe B 2 15) et/ou jusqu'à la destruction de ceux-ci en temps opportuns (idéalement par incinération).

Les données sur supports et appareils mobiles

Les données électroniques ne sont plus cantonnées aux ordinateurs de bureau. De plus en plus mobiles, il est donc de plus en plus facile de les perdre. Ces données peuvent être copiées sur des supports physiques prévus exclusivement à cet effet : CD-Rom, DVD, clés USB, disques durs externes, etc. ***Ces supports sont d'excellents vecteurs de virus informatiques*** ! Il convient donc de bloquer par défaut les ports USB ou les lecteurs de disques des postes de travail des employé-es et de ne les ouvrir que lors d'un besoin avéré, et sous réserve d'un passage au peigne fin dudit support ***par un programme anti-virus adéquat avant tout transfert de données*** ! En outre, il ne faut pas oublier de "faire le ménage" après utilisation, c'est-à-dire d'effacer soigneusement du support amovible tout document qui n'a plus sa raison d'y être.

La mobilité au XXIème siècle ne se limite pas aux supports de données amovibles précités. Ordinateurs portables, smartphones et tablettes foisonnent et font partie intégrante de notre quotidien, tant au niveau privé que professionnel. ***Concernant ces appareils mobiles, les mêmes précautions doivent être appliquées que pour les appareils fixes : vérifications anti-virus, protection par mots de passe*** (un code pin est insuffisant) et ***traitement adéquat des données confidentielles***. Si l'appareil mobile interagit avec le parc informatique de l'entreprise, il est en outre recommandé de se doter d'un outil de gestion des appareils mobiles (MDM). Cet outil a pour but de permettre le blocage des appareils mobiles à distance et l'effacement des données qu'il contient (en cas de vol ou de perte). L'installation de logiciels et la gestion des comptes des utilisateurs doit, elle, se faire avec la même politique qu'au niveau des postes de travail fixes, c'est-à-dire une politique qui ne laisse pas l'employé-e "bidouiller" l'objet par lui-même.

Lors de déplacements professionnels, les appareils mobiles doivent être traités avec la même diligence que s'il s'agissait d'une valise contenant des billets de banque. Dans le cas de déplacements via le réseau de transports publics, il faut veiller aux regards indiscrets et/ou doter l'appareil mobile d'un "flouteur" d'écran. En matière de téléphonie, il faut prendre garde aussi aux oreilles indiscrètes, cet avertissement s'appliquant aussi lors de "business-lunchs".

FICHE INFO DU PPDT

SECURITE DES DONNEES

Aspects juridiques et pratiques

La protection des données : l'affaire de tous

Entourés que nous sommes d'outils technologiques de plus en plus performants pour protéger les systèmes d'informations professionnels (firewalls, logiciels de cryptage, DMZ, antivirus, antispams), la tentation est grande de se croire à l'abri. Même si la technologie contrecarre la plupart des attaques informatiques classiques, cela ne suffit pas, car 80% des attaques informatiques ne sont pas classiques, mais le fait du social engineering (ingénierie sociale). Le social engineering utilise une personne en l'attendrissant et en l'escroquant dans le but d'obtenir des renseignements exploitables sur le système d'information qu'elle utilise, voire pire, pour ouvrir une porte d'entrée sur le système informatique et/ou celui de l'entreprise.

L'idée n'est pas de devenir complètement paranoïaque, mais dans un monde en perpétuel changement, mieux vaut prévenir que guérir. Et la meilleure prévention, c'est la sensibilisation. Sensibiliser chaque employé-e de l'entreprise aux risques qui menacent le système d'information et l'inciter à agir avec prudence et en respectant les règles en vigueur dans l'entreprise.

Mais comment être au courant de ces règles ?

En mode proactif, en se référant, s'il existe, au règlement d'utilisation du système d'information de l'entreprise. En mode réactif, en suivant des formations de sensibilisation à la sécurité de l'information. Les deux approches sont complémentaires et il est fortement recommandé de les mettre à disposition de ses employé-es, en incluant dans la mesure du possible la plupart des thèmes suivants : traitement des données personnelles et sensibles, utilisation du matériel mis à disposition par l'entreprise, utilisation d'Internet, des réseaux sociaux et de la messagerie électronique, utilisation du téléphone, courrier interne et externe, accès aux locaux, dispositifs de contrôles, etc.

ENVOI ET RECEPTION D'E-MAILS

Concernant le courrier électronique, en matière d'envoi...

Il faut être bien conscient qu'il n'y a pas de garantie à 100 % qu'un courrier électronique envoyé parvienne au destinataire souhaité, même si c'est le cas la plupart du temps. L'envoi de données sensibles par ce biais est donc à éviter autant que faire se peut. Si cette pratique s'avère toutefois nécessaire, il faut protéger les fichiers adéquatement (mot de passe), chiffrer l'e-mail (afin qu'il ne soit lisible que par le destinataire en possession de la clé de déchiffrage) ou utiliser un service d'envoi de message sécurisé.

Concernant le courrier électronique, en matière de réception...

Il faut prendre garde à ce que l'expéditeur d'un courrier électronique reçu soit bien celui qui est attendu et contacter le support informatique sans attendre en cas d'expéditeur inattendu ou suspect.

Il faut faire preuve d'une attention toute particulière dans le cas de la réception d'une pièce jointe inattendue. Il s'agit de prendre d'abord contact avec le support informatique avant de procéder à l'ouverture d'un document potentiellement dommageable pour le poste de travail et donc pour le réseau informatique de l'entreprise !

Se référer au support informatique et/ou au règlement d'utilisation du système d'information de l'entreprise sont deux réflexes à avoir en tête en tout temps en cas de doute.

POUR EN SAVOIR PLUS

Sur le site du Préposé fédéral à la protection des données et à la transparence (PFPDT) – De nombreux articles sur la protection des données - https://www.edoeb.admin.ch/datenschutz/index.html?lang=fr

Sur le site du Préposé fédéral à la protection des données et à la transparence (PFPDT) – Différents guides sur les droits de la personne concernée en matière de traitement des données personnelles, sur les mesures techniques et organisationnelles de la protection des données et sur le traitement des données personnelles dans le secteur du travail et le secteur privé - https://www.edoeb.admin.ch/datenschutz/00628/00629/index.html?lang=fr

Sur le site de la CNIL en France :

- Les principes clés de la protection des données personnelles - https://www.cnil.fr/fr/comprendre-vos-obligations/les-principes-cles
- La protection des données dans le monde - https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde
- Garantir la sécurité des données - https://www.cnil.fr/fr/garantir-la-securite-des-donnees

PPDT – Màj : 29.01.2019

Le Préposé cantonal à la protection des données et à la transparence (PPDT) est une autorité indépendante qui renseigne, conseille et surveille l'application de la LIPAD par les autorités et institutions publiques genevoises. N'hésitez pas à appeler en cas de questions au n° de téléphone 022 546 52 40 ou à adresser un courriel à ppdt@etat.ge.ch.