**LPD – Loi sur la protection des données**

**RGPD (règlement général sur la protection des données)**

Avec la mise en place de la RGPD au niveau européen, et la révision de la LPD au niveau suisse, une réflexion sur l’état actuel de la situation a été menée, qui amène plusieurs entreprises à se mettre à niveau en parlant de traitement des données.

**LPD**

La loi fédérale sur la protection des données a entrée en vigueur le 1 juillet 1993, cette dernière vise à protéger la personnalité et les droits fondamentaux des personnes qui font l’objet d’un traitement de données (LPD art1).

**RGPD**

L’Union Européenne représentée par son parlement a voté une Loi afin d’assurer le bon traitement des données personnelles ses citoyens, la **RGPD** (règlement général sur la protection des données). Cette dernière, entrée en vigueur le 25 mai 2018, vise à donner aux citoyens plus de contrôle sur leurs données personnelles, à responsabiliser davantage les entreprises et à renforcer le rôle des autorités de protection des données.

**Première chose à se demander : Qu’est qu’une donnée personnelle ?**

Toutes les informations qui se rapportent à une personne identifiée ou identifiable (art3 LPD). Par exemple : Nom et prénom, numéro de passeport, etc.

**En vrai, à quoi sert ces deux lois ?**

La LPD et RGPD ont été mises en place afin d’éviter la mauvaise utilisation des données de la personne, comme par exemple le profilage, vu dernièrement dans le scandale Facebook et Cambridge Analytica.

**Qui est concerné ?**

Toutes les entreprises, organes fédéraux ou personnes privées traitant des données personnelles d’un tiers, avec quelques exceptions, comme par exemple : LPD art2 al2a « elle ne s’applique pas aux données personnelles qu’une personne physique traite pour un usage exclusivement personnel et qu'elle ne communique pas à des tiers; ».

**Mise en conformité**

**Principes Juridiques (liste pas exhaustive):**

*Licéité, bonne foi, proportionnalité, finalité, réconnaissabilité et exactitude.*

•Principe de la **bonne foi**: la collecte doit se faire dans la loyauté, de manière transparente

• Principe de la **proportionnalité**: les données doivent être aptes, objectivement nécessaires pour atteindre le but poursuivi ;

• Principe de **reconnaissabilité**: la collecte et la finalité du traitement doivent être reconnaissables pour la personne concernée ;

• Principe de **finalité**: la collecte, le traitement des données doivent se faire dans un but préalablement défini. Quid du big data ?

• Principe **d’exactitude** des données (droit de rectification)

• Principe de **sécurité** : des mesures techniques et opérationnelles doivent être prises pour protéger les données et éviter tout traitement non autorisé

**Organisation et actions:**

* Nommer Un DPO (Digital protection Officer), responsable par but principalement permettre à un organisme effectuant des traitements de données personnelles de s'assurer qu'il respecte bien la réglementation applicable à leur protection.
* Mentions d’informations : Les personnes concernées doivent être informées de qui est derrière la collecte, de combien de temps seront conservés les fichiers, la finalité des données collectées et les informer sur comment elles peuvent exercer leurs droits.
* Être en mesure de répondre aux sollicitations d’une personne à accéder à ses données, aussi les modifier et supprimer selon sa volonté. Par exemple la mise en place d’un formulaire de contact.
* Demander l’accord aux personnes et leur donner la possibilité de retirer cet accord.
* Mettre en place des mesures de sécurité adaptées à la sensibilité de la donnée sauvegardée. Données sensibles, exemple : ethnie ou race, religion, option sexuelles, etc.
* Analyser les fichiers et tenir un registre de traitements des données.

**Mesures techniques adéquates**

**RGPD** oblige le responsable du traitement à mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

Elle assure aussi l’obligation de notifier à l'autorité de contrôle les violations 72h au plus tard.

Voici une liste de mesures de sécurité à prendre :

* Sensibiliser les utilisateurs ;
* Authentifier les utilisateurs ;
* Tracer les accès et gérer les incidents ;
* Sécuriser les postes de travail ;
* Sécuriser l’informatique mobile ;
* Protéger le réseau informatique interne ;
* Sécuriser les serveurs ;
* Sécuriser les sites web ;
* Sauvegarder et prévoir la continuité d’activité ;
* Archiver de manière sécurisée ;
* Encadrer la maintenance et la destruction des données ;
* Sécuriser les échanges avec d’autres organismes ;
* Protéger les locaux ;
* Encadrer les développements informatiques ;
* Chiffrer, garantir l’intégrité ou signer.

**Casino de Montreux**

**Introduction.**

Le casino de Montreux est le premier casino de Suisse en termes de résultat brut des jeux, il appartient au Groupe Barrière, groupe français de divertissement (hôtels, casinos, spas…). Le groupe possède deux autres casinos en Suisse : Fribourg (Granges-Paccot) et Courrendlin (Jura).

**Concerné**!

Le Casino de Montreux traite un nombre considérable de données, principalement en raison du Club Barrière (programme de fidélité du casino) et aussi pour des raisons juridiques, une fois que toutes les entrées sont sauvegardées par le but de prestation de comptes à la CFMJ (Commission Fédérale des maisons de jeux). Donc beaucoup de données sensibles.

**Actions et mesures prises.**

Le casino a formé deux DPO et nommé des responsables de traitement par secteur (exemple RH, Marketing, etc.) ainsi comme des suppléants aussi formés pour le traitement de données.

Le rôle des responsables de traitement de donnée est de tenir un registre à jour de tous les fichiers contenant des données personnelles (selon procédure mise en place par le DPO). Ensuite tout est validé par le DPO. Le DPO met en place des nouvelles mesures de traitement et sécurité, il doit aussi former les utilisateurs selon les principes juridiques et mesures de sécurité.

La sécurité des données est déjà en place avec des backups journaliers, clustering, firewall, portes sécurisées, entre autres.