La Journée e-tourisme de l'Ain

Compte-rendu de la table-ronde
Animée par Julien Tavernier, de la CCI de l'Ain et Anaïs Pauze, consultante C'Pro

Le Règlement Général de la Protection des Données (RGPD) : comment se mettre en conformité ?

NB : Ces notes complètent et précisent la présentation Powerpoint annexe, qui comporte tous les éléments de définition et de compréhension nécessaires.

Ce règlement remplace les textes de 1995 régissant déjà la protection des données, celui-ci va dans le même sens mais avec plus de rigueur. Le RGPD c'est avant tout un enjeu de transparence et donc de confiance. Il y a donc un intérêt certain à jouer le jeu !
Il concerne tous les acteurs, déjà quelques mois après sa mise en place, des violations ont été remontés. Les cas de piratage notamment impliquent la responsabilité des gestionnaires de fichiers. La prise de conscience est nécessaire. C'est une obligation morale et une obligation de moyens.

A retenir

1. **Tout le monde est concerné.**
2. **Une donnée personnelle, cela peut être autre chose que le nom : si 3 informations peuvent, par une simple recherche, être rattaché à une personne physique cela suffit.**
3. **Si l'on ne compte rien faire d'une information, alors il ne faut pas la collecter (exemple courant: date de naissance).**
4. **Les sanctions existent et ne touchent pas forcement que les plus « gros » acteurs. La jurisprudence sera à suivre.**

Le saviez-vous ?

NB : Le RGPD a déjà contraint Facebook à rendre effective la possibilité de supprimer son compte et de récupérer ses données personnelles postées au fil du temps. C'est bien plus facile maintenant.

Bonnes pratiques :

- Pour se prémunir des plaintes et du risque de contentieux, il faut s'interdire toute utilisation indue. Pour cela, il est nécessaire de bien identifier où sont ses données et traiter au fur et à mesure toutes les demandes reçues dans le cadre du droit à la modification et au retrait.
- Traiter sous 1 mois ces demandes, ou s'il y a une impossibilité à le faire, informer le demandeur du délai et le justifier.
- Le registre de traitement précise la durée de conservation de chaque donnée. Cela permet de différencier selon les types et les usages. Ainsi, les données de police pour un hébergeur peuvent avoir une durée de conservation fixée par la loi et différente du cadre général.
- Minimiser les risques, c'est déjà prendre les mesures de sécurités les plus simples : limiter les accès aux fichiers, maitriser l'usage des clefs USB, des smartphones en dehors des locaux de l'entreprise, du fait des risques de perte et de vol.
- En cas d'accident, de fuite des données, il est obligatoire et conforme à leur intérêt de prévenir le plus tôt possible les personnes concernées. Cela contribue aussi à une bonne gestion de la relation client.

Inst'Ain Numériques

A retenir

Je ne peux pas collecter des adresses e-mails visibles sur des profils de personnes sur les réseaux sociaux, car ils n'ont pas consenti à me donner cette information pour un usage précis auquel ils consentiraient, ils n'ont tout simplement pas cette information.

Le DPO (Délégué à la Protection des données) a l'obligation de coopérer avec la CNIL (Commission Nationale de l'Informatique et des Libertés). Il ne peut pas être le dirigeant de l'entreprise car il doit être en mesure de dénoncer des irrégularités. Sa responsabilité est engagée par la déclaration de son nom à la CNIL. Il est possible de prendre pour cela un prestataire externe, un juriste.

Le registre, dont un modèle est disponible auprès de la Cnil, est en fait le résumé de toutes les questions à se poser.