Quand RGPD rime avec sanction...Déjà ????

Passée inaperçue, il a été publiée sur le site de la CNIL une première sanction post RGPD. 250.000 euros (quand même !!!) contre une chaîne bien connue d'opticiens.On a eu de grandes craintes à l'approche du 25 mai. Puis on a été rassuré de voir tous ces mails et pop-up tous différents nous demandant (ou pas) notre accord pour continuer à recevoir des services, des informations...et on acceptait un peu mécaniquement, du fait de ne pas vouloir se palucher les 10 pages taille 6 du pop-up. Rassuré aussi par la CNIL qui, grande princesse, comprend qu'on ne soit pas près depuis le 25 mai mais qu'il est important d'avoir une feuille de route.

Oui mais voilà. Une sanction est tombée le 8 juin sur des faits remontant à juillet 2017.

Les faits :

Il était possible, en renseignant plusieurs URL dans la barre d'adresse d'un navigateur, d'accéder à des centaines de factures de clients de la société. Ces factures contenaient des données telles que les nom, prénom, adresse postale ainsi que des données de santé (correction ophtalmologique) ou encore, dans certains cas, le numéro de sécurité sociale des personnes concernées.

Les causes

Absence de fonctionnalité permettant de vérifier qu'un client est bien connecté à son espace personnel (« espace client ») avant de lui afficher ses factures et possibilité d'accéder ainsi à d'autres factures en indiquant d'autres références.

La sanction :

250.000 euros avec publicité.

Notre avis

Intéressant que la CNIL sorte la sanction après le 25 mai. Car entre les lignes, tout avait été assez vite réglé compte tenu de la sensibilité des données. La société avait reçu une sanction sur le même motif en 2015 pour 50.000 euros.

Mais on voit bien que l'esprit RGPD plane. 334.000 clients en "libre accès" sur des données biométriques et numéro de sécurité sociale (DCP sensibles) valaient au moins cette sanction aux yeux de la CNIL. Elle considère aussi qu'au regard du contexte actuel dans lequel se multiplient les incidents de sécurité et de la nécessité de sensibiliser les internautes quant aux risques pesant sur la sécurité de leurs données, il y a lieu de rendre publique sa décision.

C'est vrai aussi que ce réseau, c'est 500 magasins en France et à l'étranger, donc pas un petit indépendant.

Enfin, une conclusion à retenir et à prendre en compte, c'est aussi que RGPD n'est donc pas que des tableaux à remplir et des courriers à envoyer. Il y a une dimension informatique à ne pas négliger.

Texte de la sanction :

- en résumé sur le site CNIL
- in extenso sur Legifrance

OPADEO CONSEIL accompagne également ses clients sur la mise en place du RGPD