GROUPE INTERSUD
FACILITATEUR DE CHIFFRE D'AFFAIRES

Lettre d'information n°62- Mai 2018
Cette lettre vous est proposée par INTERSUD, AFRECO et G2C et sera diffusée à leurs fidèles clients

Protéger les données personnelles : une impérieuse obligation

Le 25 mai entre en vigueur en Europe le Règlement Général sur la Protection des Données Personnelles (RGPD). Quatre lettres qui donnent des migraines à bien des entreprises.

Clients, fournisseurs, partenaires, visiteurs du site internet, … : des données, les entreprises en accumulent désormais des quantités phénoménales. A l'heure du e-commerce et du big data, de la traçabilité des commandes et des livraisons, difficile de renoncer à cette nouvelle « matière première » des affaires.
Mais pas question, cependant, de les manipuler sans contrôle, ni protection.
De Yahoo à Orange, de Linkedin à Dropbox, les exemples de vols de données personnelles par millions font régulièrement la Une des journaux. Sans parler de leur détournement, comme le scandale Facebook-Cambridge Analytica.

Une réforme en 6 points

A partir du 25 mai, le Règlement Général sur la Protection des Données Personnelles (RGPD) contraindra toutes les entreprises européennes manipulant des données personnelles à de nouvelles règles. Petite revue en 5 points.

1-Consentement exigé
Le RGPD consacre le « opt in » : pour recueillir les données personnelles d'une personne, son accord explicite est obligatoire. La demande de consentement doit être formulée *« sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples »*. Le client peut aussi revenir sur son consentement sans justification selon une procédure simple. Cette règle s'applique bien entendu tout particulièrement aux mineurs : en deçà de 16 ans, un mineur ne peut pas consentir seul à céder à ses données personnelles. Entre 13 et 16 ans, les pays disposent cependant d'une certaine marge de manœuvre pour autoriser l'usage autonome des réseaux sociaux par les adolescents.

2-Droit à l'oubli
Le RGPD sanctuarise également le droit à l'effacement des données, dans le respect cependant du droit à la liberté d'expression et à l'information. Pas question ainsi de demander l'effacement de « posts » mentionnant des faits publics réels et avérés.

3-Portabilité des données
Là réside sans doute l'une des grandes révolutions de la RGPD : chacun pourra demander à ce que ses données soient transférées vers un nouvel opérateur. Exactement de la même façon que l'on peut garder à vie son numéro de téléphone portable, quel que soit l'opérateur choisi. Ainsi, l'on pourra télécharger ses emails pour les utiliser dans un autre service de messagerie, ou encore demander à ce que les préférences musicales passent d'un service de streaming à un autre.

4-Les étrangers aussi
Le règlement européen s'applique bien entendu à toutes les organisations étrangères ayant une activité dans l'Union européenne. Pas question donc pour les géants américains du Net d'en faire abstraction. Pas question non plus pour les entreprises européennes transférant des données en dehors du continent de s'abstenir de les protéger.

5-Communication obligatoire
Tout problème de fuite ou de sécurité des données doit être immédiatement communiqué aux personnes concernées « si cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés ».

6-Des sanctions élevées
En cas de conflit avec une entreprise même étrangère, c'est à la CNIL (commission nationale informatique et libertés) qu'il faudra s'adresser. Celle-ci recevra également, et c'est une nouveauté, les actions collectives. La CNIL pourra infliger des amendes allant jusqu'à 4% du chiffre d'affaires ou 20 millions d'euros.

Pour les entreprises, l'occasion de s'organiser

Si, sans nul doute, les intentions de ce règlement sont louables et adaptées aux problèmes du moment, s'y adapter est un vrai cauchemar pour bien des entreprises. Car il faut mettre à jour les conditions générales, les formulaires (papier ou internet), préparer les systèmes à tous les cas de figure envisageables (révocation du consentement, droit à l'oubli, portabilité, etc…). Et bien entendu - si cela n'est pas déjà fait- veiller à une protection accrue des données collectées.
La CNIL a élaboré un petit vade-mecum qui récapitule des actions à mener.

1-Désigner un pilote des données
Certaines entreprises devront nommer un DPO (délégué à la protection des données). Mais même les autres ont intérêt à identifier un responsable des données qui aura pour mission de clarifier, chapoter et superviser toutes les actions de l'entreprise dans ce domaine.

2-Cartographier ses données
Quel service de l'entreprise recueille quelles données pour quoi faire ? Où ces données sont-elles stockées, comment, et jusqu'à quand ? Avec la RGPD, finie l'ère de l'éparpillement : il va falloir mettre de l'ordre dans sa politique de données ! Cela permettra aussi de prioriser les actions à mener.

3-Déterminer les risques
Cette cartographie permettra de mettre en évidence les risques les plus élevés pour les droits et libertés des personnes concernées. Il faudra alors réaliser un PIA : Privacy Impact Analysis. C'est un outil d'évaluation d'impact sur la vie privée.

4-Organiser la sécurité des données
Il s'agit ensuite d'établir des process stables prenant en compte tous les événements susceptibles d'intervenir (piratage, etc.).

5-Documenter la conformité
Et, bien évidemment, il faut à tout instant être en mesure de prouver que les méthodes de l'entreprise permettent d'atteindre la conformité au règlement.

Pour les entreprises, et tout particulièrement pour les TPE et PME, l'effort d'adaptation est important. Bonne nouvelle cependant : en contrepartie, quasiment toutes les formalités CNIL vont disparaître ! LA CNIL a par ailleurs réalisé un très important effort de vulgarisation, et notamment édité un guide spécialement dédié aux TPE-PME.

Vos partenaires, Intersud, Afreco et G2C, ont pris les mesures nécessaires et sont en conformité au RGPD.

Intersud 04 91 19 02 00
Afreco 04 78 53 12 99
G2C 04 72 88 69 00