« Qui se connaît bien, se protège bien »

Dans le cadre de leurs activités, les entreprises ont le devoir d'instaurer en interne des mesures de gestion et de protection des données. « La démarche passe notamment par des mesures de sécurité informatique appropriées. Mais gare aux sociétés, qui ne respectent pas leurs obligations ! », prévient Gaëlle Lipinski, juriste et Data Protection Officer auprès de la confédération luxembourgeoise du commerce.

Initié par la Commission Européenne, adopté par le Parlement Européen en avril 2016, et entré en vigueur dans l'UE le 25 mai 2018, le Règlement général sur la protection des données (RGPD) est encore loin, deux ans plus tard, d'être appliqué par la majorité des entreprises.
Cadre de référence sur le sujet, le dispositif vise à accroître la protection des personnes concernées, par un traitement de leurs données à caractère personnel. Il s'adresse aux personnes morales publiques et privées, tenues de respecter un certain nombre de règles dans ce domaine.
La mise en conformité au RGPD passe par des actions très précises : comme notamment la nomination en interne d'un délégué à la protection des données, le recensement des différents traitements des données, qui seront ensuite consignés dans le registre des activités de traitement (couramment appelé le Registre).
Une fois la démarche effectuée et documentée, les organisations doivent alors définir les éventuelles actions correctives, et analyser les risques pouvant avoir des conséquences sur la sécurité des données.
Elles doivent en outre mettre en place des procédures internes, afin d'assurer en permanence la protection des données personnelles traitées, mais aussi d'anticiper les événements éventuels pouvant impacter celle-ci.

«La sécurisation ne doit pas se limiter uniquement à l'aspect purement technique mais doit impliquer tous les acteurs concernés ...»

La sécurité informatique au centre du RGPD

« Si les grands groupes disposent des ressources financières et humaines suffisantes, pour intégrer de telles dispositions dans leurs activités, ce n'est pas toujours le cas des petites et moyennes entreprises, » reconnaît Gaëlle Lipinski, docteur en droit et Data Protection Officer (DPO), à la confédération luxembourgeoise du commerce (clc).

Aussi, l'organisation patronale dédiée à l'entreprise privée sensibilise ses membres aux risques possibles, en cas de non-conformité au RGPD. Elle leur propose également des sessions d'informations juridiques générales ou sectorielles sur le dispositif. De plus, elle accompagne en proposant un service de DPO externe les PME de moins de 100 salariés, dans la mise en place du règlement, puis dans la documentation du traitement de leurs données.

Le RGPD n'oublie pas la question de la sécurité informatique, l'un des points les plus sensibles en matière de gestion et de protection des données personnelles.

« Des actions appropriées doivent être mises en place par les entreprises et leurs sous-traitants, » prévient la juriste. « Ces mesures de sécurité doivent être adaptées aux risques visant les personnes concernées, au volume et à la sensibilité des données traitées ».

Sur son site, la Commission nationale pour la protection des données (CNPD) consacre d'ailleurs un dossier thématique sur le sujet : « La sécurisation ne doit pas se limiter uniquement à l'aspect purement technique mais doit impliquer tous les acteurs concernés (responsables du traitement, employés exécutants et sous-traitants, personnes dont des données sont traitées), » avertit l'autorité de contrôle luxembourgeoise. « Il s'agit donc de combiner des mesures techniques à des mesures organisationnelles (structure dans l'organisation, sensibilisation et vigilance de tous les acteurs) ».

Concrètement et conformément aux dispositions du RGPD, les outils et les applications TIC, ainsi que les dispositifs de sécurité mis en place, doivent donc être précisés et décrits par les entreprises.

Aussi, les connexions téléphoniques et Internet, ainsi que les outils de gestion, de sauvegarde et d'hébergement des données sur un serveur interne, un cloud externe ou un datacenter, voire même les caméras intérieures et extérieures de vidéo-surveillance, doivent être répertoriés et consignés dans le Registre.

Une prise de conscience et un état des lieux nécessaires

En suivant les recommandations de la CNPD, les sociétés s'appliquent une démarche préventive de sécurisation de leurs données. De plus, « elles limitent les risques de perte ou de piratage de leurs données sur leurs activités, salariés, clients, fournisseurs et sous-traitants. Et elles peuvent mieux se prémunir contre l'espionnage industriel, » ajoute Gaëlle Lipinski.

Gare à celles, cependant, qui n'adhèrent pas du tout (ou que partiellement) au règlement. À tout moment, la CNPD peut exiger de consulter le Registre, et prendre les sanctions nécessaires, en cas de non-conformité ou de violation.

Les amendes administratives peuvent en effet se monter jusqu'à 20 millions d'euros, ou jusqu'à 4% du chiffre d'affaires mondial généré par les groupes, lors de l'exercice précédent. Le manquement au RGPD peut être aussi sanctionné pénalement : d'une amende de 251 à 125.000 euros, assortie d'une peine d'emprisonnement de huit jours à un an.

Si au Luxembourg, aucune sanction n'a encore été prononcée, Gaëlle Lipinski conseille vivement aux PME de se mettre en règle au plus vite.

Et même si la démarche est contraignante et chronophage, la mise en conformité a toutefois le mérite d'initier chez ces dernières une introspection d'affaires, voire un véritable état des lieux. « Ce qui est important, c'est la prise de conscience : en passant en revue l'intégralité de leurs processus, activités et métiers, en listant leurs personnels, clients, sous-traitants et fournisseurs, les sociétés peuvent identifier les risques potentiels et existants, et apprennent en tout cas à mieux se connaître. Et qui se connaît bien, se protège bien », conclut la juriste de la clc.

Pour plus d'informations :
Auprès de la confédération luxembourgeoise du commerce: www.clc.lu, info@clc.lu
Auprès de la Commission nationale pour la protection des données (CNPD) : https://cnpd.public.lu/fr.html
Auprès de cegecom : info@cegecom.net