EDITIONS LEGISLATIVES
actuEL RH
Le quotidien des professionnels des ressources humaines

Télétravail et protection des données personnelles

30/09/2020

Chaque mois, Avosial publie une chronique pour actuEL-RH. Ce mois-ci, Emmanuel Daoud, associé fondateur du cabinet d'avocats Vigo, rappelle les précautions à prendre afin d'assurer la protection des données personnelles des salariés et de l'entreprise avec le développement du télétravail.

Afin de poursuivre leurs activités au cœur de la crise sanitaire liée à la pandémie du Covid-19, les employeurs ont été contraints de mettre en place des solutions de télétravail, pour pallier les risques de propagation du virus et assurer la sécurité et la santé de leurs employés. Aujourd'hui et plus que jamais, ce déplacement du travail est au cœur des entreprises, tous secteurs d'activité confondus, et engendre une profonde mutation de l'organisation du travail.

Avant la mise en œuvre de ces mesures, il convient de souligner que l'employeur garantissait la protection des données de ses salariés par le biais des infrastructures : un accès aux locaux sécurisé, des infrastructures informatiques protégées et des postes de travail le plus souvent clairement attribués et dont l'utilisation est soumise à des règles internes strictes. Le télétravail vient remettre en cause cette infrastructure sécurisée, nécessitant des adaptations et une vigilance accrue de la part des employeurs.

A ce titre, la Commission nationale de l'informatique et des libertés (Cnil) a publié une fiche pratique destinée à fournir un socle de recommandations pratiques afin de limiter les atteintes aux données de l'entreprise, qu'il s'agisse de données personnelles ou de toutes autres données liées à leur activité qui nécessite une confidentialité accrue pour protéger les actifs de l'entreprise.

Une sensibilisation et une information claire à fournir auprès des salariés quant aux risques et aux bonnes pratiques à mettre en œuvre

La Cnil conseille de rédiger une nouvelle charte de sécurité, spécifiquement dédiée au télétravail, qui devra être communiquée à l'ensemble des collaborateurs. Celle-ci indiquera l'ensemble des bonnes pratiques à mettre en place pour favoriser une bonne sécurité et limiter les risques d'atteintes aux serveurs et aux fichiers.

En outre, une sensibilisation plus pratique des salariés pourrait être mise en place, par le biais d'un module de formation en ligne ou par la distribution d'un guide pratique visant à identifier les risques et les mauvaises pratiques pouvant conduire à la survenance de ces derniers.

Cette sensibilisation doit impérativement préciser aux salariés que, l'exercice de leurs missions en dehors de la structure de l'entreprise, ne les exempte pas de leurs obligations de vigilance et de confidentialité habituelles.

Une accentuation des outils de protection informatique pour compenser l'absence d'infrastructure fixe

La Cnil cible spécifiquement une plus grande sécurisation du système d'information. Le niveau de sécurité des outils informatiques devant être maintenu alors même que de nouvelles vulnérabilités sont susceptibles d'être reconnues.

Il est ainsi recommandé d'équiper tous les postes de travail des salariés au minimum d'un pare-feu, d'un anti-virus et d'un outil de blocage de l'accès aux sites malveillants, et cela, plus spécifiquement si les employés sont contraints de travailler sur leurs outils informatiques personnels.

Dans la mesure où les services de l'entreprises seraient accessibles depuis internet, il convient d'utiliser des protocoles garantissant la confidentialité et l'authentification du serveur destinataire.

Afin de limiter les risques d'attaques informatiques et d'intrusions malveillantes, il est nécessaire d'une part, de veiller à ce que les derniers correctifs de sécurité soient effectivement intégrés à tous les logiciels et équipements utilisés et d'autre part, de s'assurer que les services accessibles à distance ne fassent pas l'objet d'une intrusion malveillante. Pour cela une authentification à double facteur doit être implémentée.

Enfin, le télétravail bouleversant les moyens de communication interne au sein des équipes, il doit être mis à disposition des salariés une liste d'outils de communication et de travail collaboratifs pouvant protéger les échanges et le partage des données. Les outils jusqu'alors utilisés par le grand public, semblent inadaptés au cadre du travail et à l'impératif de confidentialité devant s'imposer à ce dernier.

Emmanuel Daoud
