Dossier Covid-19 – Télétravail, sécurité informatique et RGPD

Les bons tuyaux pour sécuriser l'environnement informatique du télétravail

L'agence européenne de cybersécurité (ENISA) a profité du contexte d'épidémie du Covid-19 et de confinement pour publier une fiche sur les bonnes pratiques en matière de sécurité informatique pour le travail à distance (en anglais). Cette fiche s'adresse aux directions informatiques et aux employeurs afin de vérifier que les bases de l'hygiène informatique sont respectées (connexion Wifi sécurisée, système anti-virus entièrement mis à jour, logiciel de sécurité à jour, sauvegardes régulières des fichiers, verrouillage automatique des écrans si le salarié travaille dans un espace partagé, connexion sécurisée, éventuellement outils de chiffrement).
Elle recommande notamment aux employeurs :

- de fournir régulièrement des consignes au personnel sur la façon de réagir en cas de problème (numéro du service informatique, heures de service, procédures en cas d'incident de sécurité…) ;
- de fournir des solutions d'accès à distance telles que des capacités d'authentification et de session sécurisée ;
- d'assurer un accompagnement en cas de problème ;
- de sensibiliser le personnel aux risques de phishing, très couru en cette période de crise sanitaire.

RGPD et Covid-19

Le Contrôleur européen de protection des données a rappelé dans un communiqué de presse que la protection des données personnelles devait être assurée même en cas de crise sanitaire. Il rappelle également que le RGPD (articles 6 et 9) prévoit qu'un employeur (et les autorités publiques de santé) peut traiter les données personnelles de ses salariés sans leur consentement pour des raisons d'intérêt public tenant à la santé publique et pour protéger les intérêts vitaux. En période d'épidémie, l'employeur peut donc tenir une liste des personnes hospitalisées ou atteintes du Covid-19, notamment pour assurer la sécurité de ses employés.