LEGAL FLASH COVID-19
#EPISODE 3 : TÉLÉTRAVAIL ET CYBERSÉCURITÉ

1 CYBERSÉCURITÉ ET PROTECTION DES DONNÉES - OBLIGATIONS DE L'ENTREPRISE

- Le RGPD impose aux entreprises de mettre en place des mesures efficaces pour sécuriser les données personnelles qu'elles traitent
- Les mesures techniques et organisationnelles mises en place par l'entreprise doivent garantir la confidentialité, la disponibilité et l'intégrité des données personnelles et éviter leur consultation non autorisée par des tiers
- Une **cartographie des risques** ainsi qu'un registre des traitements de données doivent être mis en place par l'entreprise
- En cas de faille de sécurité et d'incidents liés aux données, la responsabilité de l'entreprise peut être engagée. Des sanctions, notamment financières, peuvent être prononcées contre l'entreprise.

2 RISQUES EN MATIÈRE DE CYBERSÉCURITÉ LIÉS AU TÉLÉTRAVAIL

- La période actuelle intensifie les usages numériques et les risques qui y sont associés en matière de sécurité des données
- Le **télétravail** implique notamment de pouvoir accéder à distance aux serveurs de l'entreprise et de se connecter via un réseau Wifi nouveau
- Les données de l'entreprise sont alors exposées et le risque de piratage augmente (hameçonage, rançongiciels, vol de données, faux ordres de virement, etc.)
- L'utilisation de nouveaux outils pour faciliter le travail à distance (conférence, audio, etc.) **impose de s'assurer que l'outil utilisé respecte bien la règlementation applicable en matière de données personnelles** (notamment lorsque l'éditeur de l'outil se situe en dehors de l'Union Européenne et qu'il y a un transfert de données hors du territoire)

3 BONNES PRATIQUES À DÉPLOYER

- La formation et la **sensibilisation** des collaborateurs de l'entreprise est primordiale en matière de cybersécurité et de protection des données personnelles. Une charte informatique doit être déployée
- La **sécurisation** des accès extérieurs doit être assurée en limitant les connexions à distance et en chiffrant les connexions extérieures
- Les équipements mis à la dispositions des collaborateurs doivent être sécurisés : renforcement des mots de passe, utilisation d'anti-virus et déploiement régulier d'opérations de mise à jour
- **L'installation** de logiciel et d'application **non approuvés** par le support informatique de l'entreprise par les collaborateurs ne doit pas être possible
- La **sauvegarde** des données doit être maintenue et testée régulièrement pour s'assurer de son bon fonctionnement
- Le **registre** des traitements doit être **mis à jour** en cas d'utilisation de nouveaux outils numériques adaptés au télétravail

TROIS QUATORZE
Lyon • +33 (0)6 83 25 34 63 • troispointquatorze.fr
valerie.chazaud@troispointquatorze.fr