CONFORMITÉ RGPD – QUESTIONNAIRE D'ÉVALUATION PRÉLIMINAIRE

- ☐ L'Autorité pour la Protection des Données recommande que tous les responsables du traitement et sous-traitants maintiennent un registre de leurs activités de traitement de données personnelles et ce, même si l'Article 30 du RGPD ne les y oblige pas.
- ☐ **En pratique** cela signifie que vous devez avoir une bonne idée des flux de données à l'intérieur de votre entreprise. Posez-vous les questions suivantes : – à quelles fins des informations personnelles sont-elles collectées, utilisées, sauvegardées? Avec qui et comment seront-elles partagées? Si plusieurs raisons le justifient, chacune d'elles doit être analysée séparément.
- ☐ **SURVOL DU TRAITEMENT - ANALYSE DE L'INFORMATION RETENUE?**
  - **Pourquoi** des données personnelles sont-elles traitées ? (par.ex. gestion de la main d'oeuvre, obligations légales, prestation de biens ou de services, marketing direct, profilage ...)?
  - De **qui** sont traitées les données personnelles ? (par.ex. employés, clients, contacts d'affaires, fournisseurs, enfants ou mineurs...**Quelle** est la source des données : l'individu lui-même, un tiers...?
  - **Quelles** données personnelles sont traitées? (par.ex. détails personnels – nom, adresse, courriel, adresse IP, téléphone, date de naissance, détails financiers – compte en banque, cartes de crédit, références fiscales, détails concernant l'emploi; catégories spéciales (par.ex. santé, biométrie, dossier judiciaire)?
  - **Quand** sont traitées les données personnelles ? (et y compris, quand sont-elles obtenues, divulguées, sauvegardées, supprimées, collectées? Partagées avec qui et pourquoi? Sauvegardées jusqu'à quand?)
  - **Où** sont traitées les données personnelles ? (par.ex. Fichiers électroniques – sont-ils gérés en interne ou par un fournisseur de services externe? Les serveurs sont-ils situés dans l'EEE, aux États-Unis ou ailleurs? Services infonuagiques – où sont les serveurs? Fichiers non informatisés – où se trouvent-ils?).
- ☐ **PROCESSUS EN PLACE**
  - Avez-vous offert de former vos employés en protection de données privées? Qui se charge de la protection des données chez vous? Avez-vous élaboré des politiques concernant la protection des données à la fois en interne (employés) et en externe (clients et fournisseurs)? Quand ces politiques ont-elles été révisées? Quelles politiques de protection des données et relatives aux fichiers témoins apparaissent sur votre site web?
- ☐ **TIERCES PARTIES**
  - Êtes-vous un responsable du traitement des données? Utilisez-vous des sous-traitants? Avez-vous sous la main des copies des contrats? Ont-ils été révisés à la lumière du RGPD par rapport à la sécurité, l'intégrité et la confidentialité?

☐ **TRANSPARENCE**

- Avez-vous actualisé l'information destinée aux personnes concernées quant au traitement permis des données et ce, dans un langage clair et en tenant compte des informations requises par les articles 13 et 14 RGPD?

☐ **ÉVALUATION DES RISQUES**

- Existe-t-il un processus en place pour régulièrement tester et évaluer votre système de gestion des données, par rapport à leur sécurité et protection contre des attaques internes ou externes?

☐ **ÉTAT DE PRÉPARATION**

- Existe-t-il un processus interne pour évaluer et enregistrer (et éventuellement divulguer) les incidents relatifs aux données?

☐ **INTERNATIONAL**

- Si vous effectuez la transmission de données à l'extérieur de l'EEE, avez-vous vérifié le fondement juridique qui vous permet de le faire?