LA PROTECTION DES DONNEES PERSONNELLES

NATHALIE HAAS

AVOCAT AU BARREAU DE MULHOUSE

Pourquoi ?

➔ Protection contre les GAFAM

➔ Pas d'économie numérique sans confiance

➔ Nécessité de protéger la vie privée

Qui est concerné ?

TOUTE ENTITE QUI TRAITE DES DONNEES A CARACTERE PERSONNEL

➔ **Données à caractère personnel :** toute information qui se rapporte à une personne physique qu'elle soit identifiée voire simplement identifiable et ce même de manière indirecte

➔ **Traitement :** opération portant sur des données à caractère personnel quel que soit le procédé utilisé, automatisé ou non

Quel est l’intérêt pour ma structure ?

➔ Les données personnelles que j’ai collectées font partie de l’actif de ma structure

➔ Gage de modernité et de sérieux

➔ Suscite la confiance

➔ Risque important de condamnations

Quels sont les risques ?

1ère étape : mesures correctrices envisagées avant toute sanction

2nde étape : application de la loi du 20 juin 2018 n° 493-2018 modifiant la loi Informatique et Libertés :

- rappel à l'ordre
- injonction de mise en conformité sous astreinte
- retraits de certification…
- amende administrative ne pouvant excéder le montant le plus élevé entre 10.000.000 € OU 2% du CA mondial voire le double dans certaines hypothèses

Risque non théorique

IDEES DIRECTRICES

Accompagner le cycle de vie des données personnelles auxquelles vous avez accès

- ➔ Finalité
- ➔ Minimisation
- ➔ Légalité
- ➔ Information / Consentement
- ➔ Limitation de la conservation

REFLEXES A ADOPTER

1° Formalités RGPD

➔ Registre des traitements à effectuer :

Cartographie, actions à mener avec délais, sous-traitants, salariés, procédures internes de gestion des risques, registre des incidents, législation, étude d'impacts

➔ Nomination d'un Délégué à la Protection des Données le cas échéant

2° Site Internet

Visibilité optimale

Conditions Générales à jour

Formulaire de contact

3° Mettre à jour les contrats

- Recueillir le consentement

- Vérifier les contrats établis avec les sous-traitants (co-responsabilité)

➔ s'assurer qu'ils présentent des garanties nécessaires et suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles pour répondre aux exigences du RGPD

➔ faire signer un avenant

- Modifier les trames des nouveaux contrats de travail et pour les salariés actuels, les informer de leurs droits par un document à remettre avec la prochaine fiche de paye

4° Sécurisation des archives

➔ Optimiser le système d’archivage

➔ Réduire au strict minimum les personnes y ayant accès

➔ Détruire après les périodes de prescription

5° Répondre à toute demande

➔ Création d’une adresse dédiée au RGPD

➔ Délai de réponse d’un mois

6° Cloisonnement des accès

➔ Vis-à-vis de l’extérieur

➔ En interne

➔ Valable également pour les données « papier »

7° Bonnes pratiques informatiques

➔ Politique de mot de passe

➔ Instruments informatiques : smartphone, clé USB, disques durs externes

8° Gérer les failles de sécurité

Dans les 72 heures de la faille de sécurité, le responsable de traitement doit prévenir la CNIL mais aussi l'ensemble des personnes concernées sauf exceptions

Tout retard doit être justifié

Attention au sous-traitant

Merci pour votre attention

Nathalie HAAS
Avocat au Barreau de Mulhouse
57 rue Victor Schoelcher 68200 MULHOUSE
03.89.56.00.47
nathalie.haas.avocat@orange.fr