Qualis Formation

RGPD & SOUS-TRAITANTS

Le règlement de protection des personnes physiques à l'égard du traitement des données à caractère personnel, plus communément appelé « RGPD », applicable au 25 mai 2018, encadre la collecte, le traitement et la conservation des données à caractère personnel, prenant en compte **l'évolution des technologies digitales et les pratiques du marché.**
La protection du patrimoine informationnel de l'entreprise et la mise en conformité **des contrats de sous-traitance** est fondamentale pour toutes les entités amenées à traiter des données à caractère personnel.
Nous vous proposons un décryptage des **règles juridiques** avec un **guide** des bonnes pratiques en matière de sous-traitance concernant le traitement des données.

PUBLIC CONCERNÉ
- Direction Générale et Direction de la Communication
- Juristes
- CIL-DPO
- DSI (Direction des systèmes d'information)

DURÉE
- 1 jour

OBJECTIFS

- Acquérir les connaissances juridiques liées au RGPD.
- Identifier les actions à mener en vue de la mise en conformité des contrats de sous-traitance dans la collecte et/ou le traitement de données.
- Mesurer les obligations de sécurité à appliquer.
- Connaître le périmètre de responsabilité dont les cas de co-responsabilité.

INTRODUCTION

- Le régime antérieur Loi informatique et libertés n°78-17 du 6 janvier 1978, modifiée.
- Application directe du texte réglementaire au sein de l'ensemble des Etats membres de l'UE au 25 mai 2018.
- Objectifs du règlement :
  - > Renforcer les droits des personnes.
  - > Responsabiliser les acteurs traitant des données (responsable de traitement et sous-traitant).
- Les sanctions :
  - > Sanctions pénales, pénalités financières de 2% du CA mondial ou 10 millions d'euros à 4% du CA mondial ou 20 millions d'euros.

PROGRAMME

I / MAÎTRISER LE NOUVEAU CADRE JURIDIQUE GÉNÉRAL

L'ESPRIT DU RÈGLEMENT :
- Licéité du traitement.
  - > Données personnelles, sensibles, perçues comme sensible.
  - > Security by default.
  - > Cartographie des données.
- Privacy by design.
- Le Consentement.
  - > Les incontournables en cas de faille de sécurité.
  - > Cartographie des risques.
- Etude d'impact préalable.

Minimisation des données

RGPD & SOUS-TRAITANTS *- (suite)*

LE DATA PROTECTION OFFICER
A/ LES RÈGLES DE DESIGNATION

- La nomination obligatoire d'un DPO :
  - > Traitement effectué par une autorité ou un organisme public.
  - > Si RT ou ST procèdent à un suivi régulier et systématique à grande échelle des personnes.
  - > RT ou ST procèdent à un traitement à grande échelle de catégories particulières de données.
- La nomination facultative d'un DPO:
  - > Article 37 RGPD.
  - > Exigences similaires à la désignation obligatoire.
- Comment designer un DPO?
  - > Faire acter la nomination par l'organisme.
  - > Formaliser nomination dans une lettre de mission.
  - > Informer les instances représentatives du personnel.
  - > Informer l'autorité de contrôle.
  - > Publication des coordonnées du DPO.

B/ LE PROFIL DU DPO

- Type de profil:
  - > Interne: Salarié désigné.
  - > Externe: le contrat de service.
  - > Mutualisé : dans quel cas?
- Capacité:
  - > Les attentes en matière de savoir.
- Statut DPO:
  - > Independence fonctionnelle.
  - > Responsabilité/Irresponsabilité.
  - > Compatibilité de ses fonctions.
  - > Secret professionnel.

C/ MISSIONS DU DPO

- Les ressources du DPO.
- Les actions incontournables à mener:
  - > Conseil & information.
  - > Contrôle.
  - > Formation.
  - > Coopération.
  - > AUDIT PIA.
  - > Point de contact.
  - > Reporting & analyse de risque.
  - > De la Tenue du Registre de Traitement selon la taille des entités.
- Les actions facultatives :
  - > Notification.
  - > La tenue du registre de traitement pour les sociétés de - de 250 salariés.

RGPD & SOUS-TRAITANTS *- (suite)*

II/ LE SOUS-TRAITANT

- Définitions :
  - > Article 4-8 RGPD.
  - > Loi de 1975 sur la sous-traitance.
- Critères de sélection d'un prestataire :
  - > Le programme de sécurité fondé sur des normes reconnues (ISO, référentiel ANSI, SOC).
  - > Le mécanisme de gestion des risques à la résilience du SI face aux menaces.
  - > Le process de sécurité au sein de la SI.
  - > La politique de sécurité des données.
  - > L'obligation de sensibilisation des équipes à la sécurité des données.
  - > La Certification.
- Sécuriser le contrat de sous-traitance :
  - > Les annexes opérationnelles.
  - > Le répertoire des fournisseurs.
- Evaluer le risque lié au sous-traitement des données :
  - > Clause données personnelles.
  - > Mentions obligatoires dans le contrat de sous-traitance.
- Responsabilité :
  - > Le responsable de traitement et le ST peuvent être contrôlés par la CNIL.
  - > Responsabilité in solidum.
  - > Le cas de la co-responsabilité.
  - > Action récursoire.
  - > Possible exonération de responsabilité.
  - > Amendes administratives & sanctions pénales.

III / CONSÉQUENCES SUR LA PRATIQUE

- Les mesures à mettre en place en anticipation des risques.
- Contrôles.

MODALITÉS PÉDAGOGIQUES

- Etudes de cas pratiques et Quiz, Pratiques et opérationnels.