Qualis Formation

RGPD – DPO

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

DURÉE
- 2 jours

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.**
Nous vous proposons un décryptage du **statut**, du **processus** de **désignation du DPO** et **des règles juridiques**.

OBJECTIFS

- Acquérir les connaissances juridiques liées au RGPD.
- Identifier les cas de désignation obligatoire d'un DPO.
- Identifier le rôle et les actions menées par le DPO.
- Mesurer les obligations de sécurité à appliquer.
- Connaître le périmètre de 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 enjeux quant à la désignation d'un DPO :
  - > Améliorer la qualité de la base de données
  - > Garantir la e-reputation
  - > Garantir le respect des droits des personnes concernées
  - > Améliorer la sécurité et la confidentialité des données
  - > Définir un point de contact
- 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 / DEFINITION DU 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.

RGPD – DPO - *(suite)*

- 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.

II / MAITRISER LE NOUVEAU CADRE JURIDIQUE GENERAL

L'ESPRIT DU RÈGLEMENT

- Licéité du traitement :
  - > Données personnelles, sensibles, perçues comme sensibles.
  - > 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 – DPO *- (suite)*

III / CONSÉQUENCES DU RGPD SUR LA PRATIQUE

- Les mesures à mettre en place en anticipation des risques :
  - > Adhérer à des codes de bonnes conduites.
  - > Pseudonymisation des données.
  - > Restreindre l'accès aux données.
  - > Contractualisation de la relation RT/ST.
  - > Le registre de traitement.
  - > Formalisation d'un référentiel de sécurité.
  - > Déclenchement régulier et analyse des tests d'intrusion.
  - > Sensibilisation du personnel aux enjeux de sécurité & confidentialité.
  - > Souscription à une assurance en cybersécurité.
- Responsabilité & sous-traitant
  - > Définition du sous-traitant.
  - > Définition du traitement et de ses modalités par le RT
  - > Devoirs et obligations du sous-traitant
  - > Responsabilité en cas de violation
  - > La sous-sous traitance & responsabilité

MODALITÉS PÉDAGOGIQUES

- Etudes de cas pratiques et Quiz, Pratiques et opérationnels

Pour aller plus loin ...
Formation complémentaire sur « comment conduire une EIVP »