Plan de formation RGPD

Phase 1 : Compréhension des principes du RGPD

I. Généralités et contexte juridique

1. Définition du RGPD

2. Objectifs du RGPD

3. Champ d'application du RGPD

4. Sanctions liées à la non-conformité

5. Traitement des données à caractère personnel (DCP)

Qu'est-ce qu'une DCP ?

Cas particulier des données dites 'sensibles'

Traitement des DCP

- Qu'est-ce qu'un traitement de DCP ?
- Obligations à respecter pour le traitement des DCP
- Définition des finalités du traitement
- Définition des finalités du traitement - la durée de conservation
- Contrôle de la qualité des DCP
- Notifier le traitement dans le registre des traitements
- Information, obtention du consentement des personnes
- Assurer l'exercice des droits de la personne concernée
- Assurer la sécurité et encadrer le transfert hors UE

II. Désignation d’un Délégué à la protection des données

6. Quand un DPO est-il obligatoire ?

7. Grande échelle : notion très subjective. 4 facteurs sont retenus

8. Quelques exemples de traitements à grande échelle

9. Quelques exemples de traitements ne constituant pas un traitement à grande échelle

10. La notion de suivi régulier et systématique des personnes concernées s’articule autour de deux critères cumulatifs

Le suivi régulier

Le suivi systématique

Quelques exemples de traitements opérant un suivi régulier et systématique des personnes

11. Désignation d’un DPO

12. Qualités et compétences requises pour le DPO

13. Les missions du DPO

Phase 2 : Mise en place opérationnelle du RGPD

III. Les 5 étapes de la mise en place

Cartographier les traitements de DCP

- Le Registre des traitements
- Exemple de registre des traitements renseigné

Apprécier les risques engendrés par chaque traitement

- Identifier les impacts potentiels sur les droits et libertés des personnes
- Identifier les sources de risque et les menaces réalisables
- Estimer la gravité et la vraisemblance des risques
- Déterminer les mesures existantes ou prévues pour traiter les risques

Mettre en œuvre les mesures prévues

- Cf. Chapitre : La sécurité des DCP

Documenter la conformité

- Documents sur les traitements des DCP
- L'information des personnes (Cf chapitre suivant)
- Les contrats qui définissent les rôles et responsabilités des acteurs

Réaliser des audits de sécurité périodiques

IV. Information préalable des personnes - Consentement explicite

Principe

Informer les personnes

Obtenir le consentement

Exemples d'informations et de consentements

- Politique de confidentialité
- Formulaire de collecte d'emails
- Cas des emailings / NewsLetters / Formulaires de contact
- Dossier « papier » (Dossiers d'inscription / Dossiers de candidature, …)
- Gestion des cookies

V. La sécurité des DCP

Utilisateurs : Sensibilisation / Authentification / Habilitations

- Rédiger une charte informatique et lui donner une force contraignante
- Sensibiliser régulièrement les utilisateurs travaillant avec des DCP
- Authentification des utilisateurs
- Gérer les habilitations

Matériel : Sécurisation des postes de travail / Serveurs / Réseaux

Logiciels : Sécurisation des Sites Web / Applications / Sauvegardes

Sous-traitants & autres organismes : Sécurisation des échanges

Locaux : Protection des locaux (Archives, salles informatiques, …)

VI. Le PIA

Qu'est-ce qu'un PIA ?

Qu'est-ce qu'un « risque sur la vie privée » ?

Quand le mettre en œuvre ?

Quand un PIA n'est-il pas obligatoire ?

Qui intervient dans la réalisation d'un PIA ?

Quand transmettre un PIA à la CNIL ?

Le montant des sanctions en cas de non-conformité

Comment mener un PIA

VII. Notifier une violation de DCP à la CNIL

Qu'est-ce qu'une violation de DCP ?

Comment déclarer une violation de données ?

Quand déclarer une violation de DCP ?

Comment déclarer une violation de données ?

Que va faire la CNIL ?