Certification relative à la protection des données personnelles en Europe

Présentation du corpus des connaissances pour la certification CIPP/E™ (Certified Information Privacy Professional/Europe)

I. Introduction à la protection des données personnelles en Europe

A. Origines et contexte historique du droit en matière de protection des données

1. Fondement de la protection des données personnelles
2. Législation relative aux Droits de l'Homme
3. Premières lois et réglementations
4. La nécessité d'une approche européenne harmonisée
5. Le Traité de Lisbonne
6. Un cadre modernisé

B. Institutions de l'Union européenne

1. Conseil de l'Europe
2. Cour européenne des Droits de l'Homme
3. Parlement européen
4. Commission européenne
5. Conseil européen
6. Cour de justice de l'Union européenne

C. Cadre législatif

1. La convention de 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention du Conseil de l'Europe)
2. La directive européenne relative à la protection des données personnelles (95/46/CE)

3. La directive européenne « vie privée et communications électroniques » (2002/58/CE) (modifiée)
4. La directive européenne relative au commerce électronique (2000/31/CE)
5. Les régimes de la rétention des données personnelles en Europe
6. Le Règlement général sur la protection des données (RGPD) et la législation associée

II. Droit et réglementations en matière de protection des données en Europe

A. Concepts de protection des données personnelles

1. Données personnelles
2. Données personnelles sensibles
3. Données pseudonymisées et anonymisées
4. Traitement
5. Responsable de traitement
6. Sous-traitant
7. Personne concernée

B. Champs d'application matériel et territorial du Règlement général sur la protection des données

1. Établissement dans l'UE
2. Non-établissement dans l'UE

C. Principes relatifs au traitement des données personnelles

1. Loyauté et licéité
2. Limitation de la finalité
3. Proportionnalité
4. Exactitude
5. Limitation de la conservation
6. Intégrité et confidentialité

D. Critères de licéité du traitement

1. Consentement
2. Nécessité contractuelle
3. Obligation légale, intérêts vitaux et intérêt public
4. Intérêts légitimes
5. Catégories particulières de traitement

E. Obligations relatives à la fourniture d'informations

1. Principe de transparence
2. Déclarations de confidentialité
3. Avis hiérarchisés

F. Droits des personnes concernées

1. Accès
2. Rectification
3. Effacement et droit à l'oubli
4. Restriction et opposition
5. Prise de décision automatisée, y compris profilage
6. Portabilité des données
7. Restrictions

G. Sécurité des données personnelles

1. Mesures techniques et organisationnelles appropriées
2. Notification des violations
3. Gestion des fournisseurs

H. Exigences en matière de responsabilité

1. Responsabilités des responsables de traitement et des sous-traitants
2. Protection des données dès la conception et par défaut
3. Documentation et coopération avec les autorités de régulation
4. Analyse d'impact relative à la protection des données
5. Délégués à la protection des données obligatoires

I. Transferts internationaux de données

1. Fondement de l'interdiction
2. Juridictions sûres
3. Safe Harbor et Privacy Shield
4. Contrats types
5. Règles d'entreprise contraignantes (BCR)
6. Codes de conduite et certifications
7. Dérogations

J. Supervision et mise en application

1. Autorités de contrôle et leurs pouvoirs
2. Le Comité européen de protection des données
3. Rôle du Contrôleur européen de la protection des données

K. Conséquences des violations du RGPD

1. Processus et procédures
2. Infractions et amendes
3. Indemnisation des personnes concernées

III. Respect du droit et des réglementations européens en matière de protection des données

A. Relations de travail

1. Base juridique du traitement des données personnelles des salariés
2. Conservation des dossiers du personnel
3. Surveillance du lieu de travail et prévention des pertes de données
4. Comités d'entreprise européens
5. Systèmes internes d'alerte professionnelle (« whistleblowing »)
6. Programmes « bring your own device » (BYOD, apportez votre propre appareil)

B. Activités de surveillance

1. Surveillance par les autorités publiques
2. Interception de communications
3. Télévision en circuit fermé (CCTV)
4. Géolocalisation

C. Marketing direct

1. Télémarketing
2. Marketing direct
3. Ciblage comportemental en ligne

D. Technologies Internet et communications

1. Informatique dans le Cloud
2. Cookies Web
3. SEM (Search Engine Marketing, ou marketing relatif aux moteurs de recherche)
4. Services de réseaux sociaux