

iapp



CORPUS DE CONNAISSANCES POUR LA CERTIFICATION CIPP/E

VERSION 1.3.2

DATE DE PRISE D'EFFET : 02/09/2024

Certification en matière de protection des données personnelles en Europe

Présentation du corpus de connaissances du Certified Information Privacy Professional/Europe (CIPP/E™)



I. Introduction à la protection des données en Europe

A. Origine et contexte historique de la réglementation relative à la protection des données

1. Fondement de la protection des données personnelles
2. Législation relative aux droits de l'Homme
3. Premières lois et réglementations
 - a. Lignes directrices de l'OCDE et du Conseil de l'Europe
 - b. Convention 108
4. La nécessité d'une approche européenne harmonisée
5. Le traité de Lisbonne
6. Convention 108+
7. Brexit

B. Institutions de l'Union européenne

1. Cour européenne des droits de l'homme
2. Parlement européen
3. Commission européenne
4. Conseil européen
5. 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 personnelles (Convention du Conseil de l'Europe)
2. La directive de l'UE relative à la protection des données personnelles (95/46/CE)
3. La directive européenne sur les données personnelles et les communications électroniques (2002/58/CE) (directive e-Privacy) (modifiée)
4. La directive européenne relative au commerce électronique (2000/31/CE)
5. Les régimes européens relatifs à la conservation des données
6. Le Règlement général sur la protection des données (RGPD) (UE) 2016/679 et la législation connexe
 - a. Lien avec d'autres textes juridiques (directive sur les services de paiement 2, règlement sur la gouvernance des données, Règlement (UE) 2018/1725, le Data Act de l'UE, etc.)
7. Directive NIS (2016) / Directive NIS 2 (2022)
8. Législation sur l'intelligence artificielle de l'UE (2021)

II. **Règlementations relatives à la protection des données en Europe**

A. Concepts relatifs à la protection des données

1. Données personnelles
2. Données personnelles sensibles
 - a. Catégories particulières de données personnelles
3. Données anonymes et pseudonymisées
4. Traitement
5. Responsable du traitement
6. Sous-traitant
 - a. Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD
7. Personne concernée

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

1. Établissement dans l'UE
2. Non-établissement dans l'UE
 - a. Lignes directrices 3/2018 relatives au champ d'application territorial du RGPD (article 3)

C. Principes relatifs au traitement des données

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, intérêt public
4. Intérêts légitimes
5. Catégories particulières de traitement

E. Obligations relatives à l'information des personnes concernées

1. Principe de transparence
2. Notices d'information relatives aux données à caractère personnel
3. Notices d'information hiérarchisées

F. Droits des personnes concernées

1. Accès
 - a. Lignes directrices 01/2022 sur les droits des personnes concernées – Droit d'accès
2. Rectification
3. Effacement et droit à l'oubli
 - a. Lignes directrices 5/2019 sur les critères du droit à l'oubli au titre du RGPD dans le cas des moteurs de recherche
4. Limitation et objection
5. Consentement, y compris le droit au retrait
6. Prise de décision automatisée, y compris le profilage
7. Portabilité des données
8. Limitations
 - a. Lignes directrices 10/2020 sur les limitations au titre de l'article 23 du RGPD

G. Sécurité des données personnelles

1. Mesures techniques et organisationnelles appropriées
 - a. Mécanismes de protection (chiffrement, contrôles d'accès, etc.)
2. La notification d'une violation
 - a. Exigences relatives au signalement des risques
 - b. Lignes directrices 1/2021 sur les exemples concernant la notification de violations de données à caractère personnel
 - c. Lignes directrices 9/2022 sur la notification de violations de données à caractère personnel dans le cadre du RGPD
3. Gestion des fournisseurs
4. Partage des données

H. Exigences en matière d'accountability

1. Responsabilités des responsables du traitement et des sous-traitants
 - a. Responsables conjoints
2. Protection des données dès la conception et par défaut
3. Documentation et coopération avec les régulateurs
4. Analyse d'impact relative à la protection des données (AIPD)
 - a. Critères établis pour leur conduite
5. Délégués à la protection des données obligatoires
6. Audit des programmes de protection des données personnelles

I. Transferts internationaux de données

1. Motifs d'interdiction
 - a. Lignes directrices 5/2021 sur l'interaction entre l'article 3 et le chapitre V du RGPD
2. Juridictions appropriées
3. Safe Harbour, Privacy Shield et le cadre UE-États-Unis pour la protection des données personnelles
 - a. Décisions Schrems, conséquences
4. Clauses contractuelles types (CCT)
5. Règles d'entreprise contraignantes (BCRs)
6. Codes de conduite et certifications
 - a. Lignes directrices 04/2021 sur les codes de conduite en tant qu'outils pour les transferts

7. Dérogations
 - a. Lignes directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679
 8. Évaluations de l'impact du transfert (TIAs)
 - a. Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données personnelles de l'UE
- J. Supervision et contrôle de l'application
1. Les autorités de contrôle et leurs pouvoirs
 - a. Lignes directrices 8/2022 concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant
 2. Le Comité européen de la protection des données
 3. Rôle du Contrôleur européen de la protection des données (CEPD)
- K. Conséquences des violations du RGPD
1. Procédures
 2. Infractions et amendes
 3. Recours collectifs
 4. Dédommagement des personnes concernées

III. Respect de la réglementation européenne relative à la protection des données

- A. Relations de travail
1. Base juridique du traitement des données des employés
 2. Stockage des dossiers du personnel
 3. Surveillance sur le lieu de travail et prévention des pertes de données
 4. Comités d'entreprise localisés dans l'UE
 5. Dispositifs d'alerte
 6. Programmes BYOD (Apportez votre équipement personnel de communication)
 7. Risques liés aux données relatives aux employés (par exemple, via les réseaux sociaux et les systèmes d'IA)
- B. Activités de surveillance
1. Surveillance par les autorités publiques
 2. Interception de communications
 3. Système de vidéosurveillance
 - a. Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo
 4. Géolocalisation
 5. Biométrie/reconnaissance faciale
 - a. Lignes directrices 05/2022 sur l'utilisation de la technologie de reconnaissance faciale dans le domaine répressif
- C. Démarchage commercial
1. Démarchage téléphonique
 2. Démarchage commercial
 3. Publicité ciblée en ligne
 - a. Lignes directrices 8/2020 sur le ciblage des utilisateurs de médias sociaux

D. Technologie et communications Internet

1. Cloud Computing
2. Cookies Internet
3. Marketing par moteur de recherche
4. Plateformes de médias sociaux
 - a. Designs trompeurs
 - i. Lignes directrices 3/2022 sur les dark patterns dans les interfaces des plateformes de médias sociaux
5. Intelligence artificielle (IA)
 - a. Machine learning
 - b. Problèmes éthiques