

Data Act et AI Act: obligations, risques et opportunités

L'objectif de cette formation est de comprendre les obligations clés du Data Act et de l'AI Act, d'identifier les risques juridiques, financiers et réputationnels liés à ces réglementations, de repérer les opportunités stratégiques pour l'innovation et la gouvernance des données, ainsi que de définir les premières étapes d'un plan de mise en conformité..

Pré-requis : Notions générales en protection des données, notions en gouvernance IT (facultatif).



- Modalité :**
- Distanciel en classe virtuelle
 - E-learning : à venir
 - Présentiel

Communauté: community.reconvert.net

Durée totale : 7 H (1 jour)

Synthèse et plan d'action : 45 min

Points transversaux : gouvernance des données, sécurité, clauses contractuelles, formation interne.

Check-list de conformité : priorisation des actions court, moyen et long terme.

Questions/réponses et échanges sur les stratégies d'anticipation.

PLAN DETAILLE

Introduction : 15 mn

Contexte européen : explosion des données, montée en puissance de l'IA, besoin de régulation.

Articulation entre RGPD, Data Act et AI Act.

Calendrier d'application et sanctions prévues.

Data Act – Approfondissement : 3 h

Objectifs du règlement : faciliter l'accès et le partage des données entre acteurs privés, utilisateurs et secteur public.
Champ d'application : données générées par des produits ou services, B2B, B2C et B2G.

Droits et obligations :

- Droits des utilisateurs sur les données produites.
- Clauses contractuelles types et obligations de transparence.
- Partage avec les autorités publiques en cas d'urgence.
- Portabilité et changement de fournisseur cloud (interopérabilité).

Impacts opérationnels : modèles économiques, sécurité, gouvernance des données.

Atelier pratique : analyse d'un scénario de partage de données et rédaction de points clés pour un contrat.

AI Act – Approfondissement : 3h

Objectifs : encadrer la conception, la mise sur le marché et l'utilisation des systèmes d'IA.

Classification des systèmes :

- Risque inacceptable (interdiction).
- Risque élevé (obligations renforcées).
- Risque limité et minimal (transparence).

Obligations pour les systèmes à risque élevé :

- Gestion des données d'entraînement et de validation.
- Documentation technique et traçabilité.
- Évaluation de conformité et surveillance post-déploiement.

Responsabilités des acteurs : fournisseurs, importateurs, distributeurs, utilisateurs.

Atelier stratégique : évaluer un cas d'usage IA, déterminer le niveau de risque et définir les mesures de conformité.