

1. Azure AD et le RGPD : Responsabilités

Les entreprises utilisant Azure Active Directory sont considérées comme responsables de traitement. Elles doivent :

- Collecter uniquement les données nécessaires (principe de minimisation),
- Appliquer des politiques d'accès basées sur les rôles (RBAC),
- Sécuriser les données (authentification multifactorielle, chiffrement),
- Respecter les droits des personnes (accès, rectification, suppression, portabilité).

2. Outils Microsoft pour la conformité RGPD

Microsoft fournit plusieurs outils :

- Portail DSR (Data Subject Requests) pour exécuter les droits RGPD,
- Azure Policy : gouvernance et application de politiques (chiffrement, localisation...),
- Compliance Manager : évaluation de conformité et plans d'action,
- Azure Information Protection : classification et protection des données sensibles.

3. Réglementations françaises

a. Hébergement de Données de Santé (HDS) :

Microsoft Azure est certifié HDS, ce qui autorise l'hébergement de données de santé en France.

b. Transferts hors UE :

Les entreprises doivent utiliser des Clauses Contractuelles Types (CCT), des BCR ou

s'assurer d'une décision d'adéquation.

4. Certifications et engagements de Microsoft

Microsoft Azure est certifié selon :

- ISO/IEC 27001 : sécurité de l'information,
- ISO/IEC 27018 : confidentialité des données personnelles,
- SOC 1, SOC 2, SOC 3 : sécurité, intégrité, confidentialité.

5. Recommandations pour les entreprises

- Cartographier les traitements et réaliser des analyses d'impact (PIA),
- Activer l'authentification multifactorielle,
- Utiliser le chiffrement de bout en bout (end-to-end),
- Tenir un registre des traitements,
- Sensibiliser les utilisateurs internes.

Sources :

- <https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-azure>
- <https://learn.microsoft.com/en-us/compliance/regulatory/offering-hds-france>
- <https://learn.microsoft.com/en-us/azure/compliance/>
- <https://learn.microsoft.com/en-us/azure/governance/policy/>
- <https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-overview>
- <https://azure.microsoft.com/en-us/services/information-protection/>
- <https://azure.microsoft.com/en-us/explore/global-infrastructure/data-residency/>

- <https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on>