

# Clauses contractuelles DORA

## Check-list à exiger d'un prestataire IT - applications Symfony

Le règlement DORA (UE) 2022/2554 déplace une partie de la responsabilité sur la relation contractuelle avec les prestataires informatiques. Voici les clauses essentielles à vérifier ou à exiger. Chaque engagement écrit doit correspondre à une capacité technique réelle et démontrable.

### 1. Droit d'audit et d'accès à l'information

Pouvoir auditer les pratiques de sécurité et obtenir les preuves (logs, rapports de tests, journaux d'incident).

### 2. SLA mesurables et pénalités

Niveaux de service chiffrés (disponibilité, temps de rétablissement), instrumentés et assortis de pénalités.

### 3. Notification et coopération en cas d'incident

Obligation d'alerter sans délai, de coopérer et de respecter les délais de notification DORA.

### 4. Stratégie de sortie et réversibilité

Plan de sortie documenté : période de transition, assistance, restitution sans dépendance irréversible.

### 5. Restitution du code et des données

Export dans des formats ouverts et exploitables, conteneurisation et infrastructure as code.

### 6. Encadrement de la sous-traitance

Transparence et contrôle sur la chaîne de prestataires en aval (sous-traitants critiques).

### 7. Localisation des données et traitements

Localisation connue et maîtrisée des données et des environnements de traitement.

### 8. Sécurité et conformité

Chiffrement des données sensibles, gestion des accès, MFA, conformité RGPD des journaux.

### 9. Tests de résilience et continuité

Sauvegardes testées (RTO/RPO), continuité éprouvée, participation aux tests de résilience.

### 10. Traçabilité et intégrité du code

Signature des commits et des artefacts, pipeline CI/CD reproductible et auditable.