DORA · SIGNALEMENT DES INCIDENTS ET RÉSILIENCE

DORA : signaler les incidents. Piloter la résilience.

Guide pratique pour les entités financières : vérifier le champ d’application, articuler les principaux travaux et préparer le signalement des incidents majeurs liés aux TIC.

DORA s’applique depuis le 17 janvier 2025, mais pas à toutes les entreprises.

Vérifiez chaque entité juridique au regard de l’article 2, y compris les exclusions et exigences simplifiées. Un contrat client ne transforme pas automatiquement un prestataire TIC en entité financière soumise à DORA ; des obligations contractuelles et le cadre de surveillance des prestataires tiers critiques de services TIC peuvent s’ajouter.

Cinq domaines de travail liés

Gestion des risques TIC

Organiser les responsabilités, inventaires, protections, détection, réponse et reprise.

Incidents

Enregistrer, classifier et escalader les incidents en interne ; signaler les cas majeurs.

Tests de résilience

Maintenir un programme proportionné couvrant les fonctions critiques et leurs dépendances.

Tiers TIC

Gérer registres, contrats, risques de concentration, suivi et possibilités de sortie.

Apprentissage et partage

Tirer les enseignements des incidents ; les informations sur les cybermenaces peuvent être partagées.

Délais de signalement d’un incident majeur lié aux TIC

4 h / 24 h

Notification initiale

Dès que possible ; dans les 4 h suivant la classification comme majeur et au plus tard 24 h après en avoir eu connaissance.

72 h

Rapport intermédiaire

Au plus tard 72 h après la notification initiale, même sans changement de situation.

1 mois

Rapport final

Au plus tard un mois après le rapport intermédiaire ou sa dernière mise à jour.

Si l’incident est classé majeur plus de 24 heures après que l’entité en a eu connaissance, la notification initiale doit être faite dans les 4 heures suivant cette classification. Transmettez les mises à jour requises sans retard injustifié et vérifiez la procédure de l’autorité compétente et les exceptions applicables.

Évaluer la gravité selon des critères définis

Appliquez les critères et seuils du règlement (UE) 2024/1772 : impact sur les services critiques, durée, clients ou transactions, étendue géographique, perte de données et impact économique. Consignez la classification, sa justification et l’heure.

DU TEXTE À UNE RÉPONSE CLAIRE AUX INCIDENTS

Six étapes pour se préparer

Un processus répété réduit les recherches et les allers-retours lorsque plusieurs équipes et prestataires TIC doivent établir rapidement des faits fiables.

01 · Responsabilité

Désignez pour chaque entité juridique un responsable incident, un suppléant, un contact de direction et un responsable du signalement.

02 · Classification

Évaluez les services critiques touchés, la durée, les clients, transactions, pays, pertes de données et l'impact économique selon les seuils applicables.

03 · Chronologie

Consignez découverte, prise de connaissance, décisions de classification et chaque envoi avec son fuseau horaire.

04 · Réunir les faits

Documentez fonctions et impacts, causes connues, confinement, prestataires et prévisions de reprise.

05 · Rapports de suivi

Préparez le rapport à 72 heures et ses mises à jour. Distinguez clairement estimations et éléments encore à vérifier.

06 · Clôture et retour d'expérience

Finalisez l'analyse des causes, les impacts réels et les mesures correctives ; réinjectez les enseignements dans les tests et le suivi des prestataires.

Informations à garder prêtes pour le premier signalement

ID de l'incident et horodatages · fonction critique ou importante concernée · justification initiale de la classification · pays, clients ou transactions touchés · interruption et impact sur les données · mesures immédiates · principaux prestataires TIC · contact et heure de la prochaine mise à jour. Utilisez les formulaires et le canal de l'autorité compétente.

Deux distinctions importantes

Enregistrez et classez les incidents TIC selon les critères DORA ; les incidents TIC majeurs doivent être signalés à l'autorité. Une cybermenace importante peut faire l'objet d'une notification volontaire au titre de l'article 19. Vérifiez séparément les obligations relatives aux données personnelles, aux contrats et à d'autres secteurs.

Sources officielles · état du droit au 8 octobre 2026

DORA, règlement (UE) 2022/2554 (notamment art. 2, 5-19, 28-30 et 64) · règlement délégué (UE) 2024/1772 (critères de classification) · règlement délégué (UE) 2025/301 (délais) · règlement d'exécution (UE) 2025/302 (formulaires) · EIOPA, aperçu DORA.

Textes officiels: 2022/2554 · 2024/1772 · 2025/301 · 2025/302 · EIOPA

Limites

Support général, pas un conseil juridique, une enquête technique, une évaluation de conformité ou un signalement à une autorité. Vérifiez le champ, la classification, l'autorité, le canal et les exceptions pour l'entité juridique concernée.