NumSpot
Cloud. Européen. Citoyen.

Le partenaire cloud souverain et de confiance des secteurs stratégiques et sensibles

Garantir les plus hauts standards de sécurité pour assurer la protection de leurs données et celles des citoyens.

Ce qu'il faut retenir de la règlementation DORA

DORA pour "**Digital Operational Resilience Act**", tient compte des risques toujours plus importants de cyberattaques, et matérialise la décision de l'Union Européenne de renforcer la sécurité informatique des entités financières (banques, compagnies d'assurance, entreprises d'investissement). La date d'application est fixée au 17 janvier 2025.

DORA s'adresse aux secteurs financiers de l'Union Européenne pour traiter des risques posés par la profonde transformation numérique des services financiers, l'interconnexion croissante des réseaux et des infrastructures critiques ainsi que par la multiplication de cyberattaques, de plus en plus sophistiquées, à l'encontre des acteurs du secteur.

Le but de **DORA** est de définir des exigences uniformes pour renforcer et harmoniser la gestion des risques liés aux Technologies de l'Information et de la Communication (TIC) et à la sécurité des réseaux et des systèmes d'information au niveau de l'Union Européenne.

« ...Le règlement couvre une série d'entités financières réglementées au niveau de l'Union, à savoir les établissements de crédit, les établissements de paiement, les établissements de monnaie électronique, les entreprises d'investissement, les prestataires de services liés aux crypto-actifs, les dépositaires centraux de titres, les contreparties centrales, les plates-formes de négociation, les référentiels centraux, les gestionnaires de fonds d'investissement alternatifs et les sociétés de gestion, les prestataires de services de communication de données, les entreprises d'assurance et de réassurance, les intermédiaires d'assurance, les intermédiaires de réassurance et les intermédiaires d'assurance auxiliaires, les institutions de retraite professionnelle, les agences de notation de crédit, les contrôleurs légaux des comptes et les cabinets d'audit, les administrateurs d'indices de référence essentiels et les prestataires de services de crowdfunding ».

Quelles sont les exigences à remplir ?

1 Cartographie et essais

Les institutions financières doivent cartographier et tester leurs services, processus et systèmes informatiques critiques afin d'identifier et de gérer les risques opérationnels.

2 Externalisation

Les institutions financières doivent mettre en œuvre des mesures adéquates pour gérer les risques liés à l'externalisation de fonctions ou de services critiques.

3 Signalement des incidents

Les institutions financières doivent signaler les incidents qui ont un impact significatif sur la continuité de leurs services ou qui constituent une menace pour le système financier.

4 Cybersécurité

Les institutions financières doivent adopter des mesures de cybersécurité appropriées et efficaces pour prévenir les cybermenaces et les violations de données.

5 La gestion des risques

Les institutions financières doivent mettre en place un cadre solide de gestion des risques, pleinement intégré à leur stratégie commerciale globale.

6 Gouvernance et bienveillance

Les institutions financières doivent maintenir des lignes de responsabilité claires en matière de résilience opérationnelle, le conseil d'administration étant responsable de la supervision de la résilience opérationnelle de l'institution.

7 Plan de continuité des activités

Les institutions financières doivent élaborer des plans de continuité des activités complets et efficaces afin de garantir la continuité de leurs services essentiels en cas de perturbation.

8 Tests et formation

Les institutions financières doivent régulièrement tester et mettre à jour leurs plans de résilience opérationnelle et former leur personnel, afin d'être prêtes à répondre aux perturbations opérationnelles.

A quelles sanctions potentielles les institutions s'exposent-elles en cas de non-respect ?

1 Amendes administratives

Les institutions financières doivent cartographier et tester leurs services, processus et systèmes informatiques critiques afin d'identifier et de gérer les risques opérationnels.

2 Mesures correctives

Les institutions financières doivent mettre en œuvre des mesures adéquates pour gérer les risques liés à l'externalisation de fonctions ou de services critiques.

3 Réprimandes publiques

Les institutions financières doivent signaler les incidents qui ont un impact significatif sur la continuité de leurs services ou qui constituent une menace pour le système financier.

4 Retrait de l'agrément

Les institutions financières doivent adopter des mesures de cybersécurité appropriées et efficaces pour prévenir les cybermenaces et les violations de données.

5 Indemnisation des dommages

Les institutions financières doivent mettre en place un cadre solide de gestion des risques, pleinement intégré à leur stratégie commerciale globale.

Il est important de noter que **les sanctions exactes en cas de non-respect** peuvent varier en fonction des circonstances spécifiques et de la gravité de l'infraction.

À propos de NumSpot

NumSpot est un acteur du cloud souverain et de confiance. Né de la volonté de 4 entreprises françaises de premier plan des secteurs public et privé (Banque des Territoires, Docaposte, Dassault Systèmes et Bouygues Télécom), NumSpot propose une offre de cloud indépendant, souverain et robuste adossé au IaaS d'OUTSCALE qualifié SecNumCloud. NumSpot est un cloud réversible et transparent, basé principalement sur l'open source et des solutions européennes. L'offre NumSpot s'adresse prioritairement aux secteurs confrontés à une forte sensibilité des données (secteur public, santé, services financiers et assurance, OIV et OSE) en France et en Europe, et à la recherche d'une solution souveraine et de confiance en accord avec les règlementations RGPD et européennes. NumSpot fait ainsi le choix d'œuvrer pour l'intérêt général en proposant un véritable pacte de confiance entre un fournisseur de cloud, ses clients et les citoyens européens.

Suivez-nous @NumSpot @NumSpotCloud