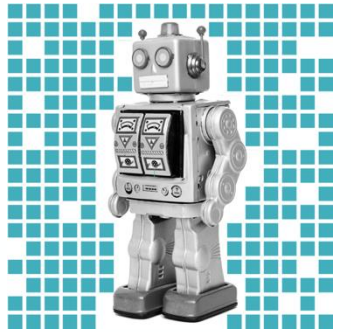
DIGITAL & CREATIVE BUSINESS LAW



DORA : zoom sur les contrats avec les fournisseurs de services IT

Règlement (UE) 2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier

Juin 2025

NEXT avocats www.next-avocats.com
6 rue Bouchardon – 75010 Paris
contact@next-avocats.com 01 75 43 86 23

Entrée en vigueur

Règlement DORA

Règlement (UE) 2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier

17 février 2025

↳ Directive DORA

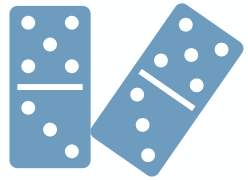
Directive (UE) 2022/2556 du 14 décembre 2022

↳ **Projet de loi**

relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité

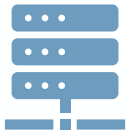
à la promul-gation de la loi

Risques



- Propagation possible d'un cyber incident de l'une des **22000 entités financières** à l'ensemble du système financier européen

Etablissements de crédit	Sociétés de gestion
Etablissements de paiement	Prestataires de services de communication de données
Prestataires de services d'information sur les comptes	Entreprises d'assurance et de réassurance
Etablissements de monnaie électronique	Intermédiaires d'assurance, les intermédiaires de réassurance et les intermédiaires d'assurance à titre accessoire
Entreprises d'investissement	Institutions de retraite professionnelle
Prestataires de services sur crypto-actifs et les émetteurs de jetons	Agences de notation de crédit
Dépositaires centraux de titres	Administrateurs d'indices de référence d'importance critique
Contreparties centrales	Prestataires de services de financement participatif
Plates-formes de négociation	Référentiels des titrisations
Référentiels centraux	
Gestionnaires de fonds d'investissement alternatifs	



Le cadre de gestion du risque lié aux TIC

La politique des services TIC fournis par des prestataires tiers

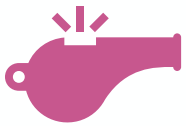
Les contrats avec les prestataires tiers de services TIC

Le cadre de gestion du risque lié aux TIC

La politique des services TIC fournis par des prestataires tiers

Les contrats avec les prestataires tiers de services TIC

Les entités financières doivent adopter :



Fonction de contrôle interne indépendant

Responsabilité de la gestion et de la surveillance

Un cadre de gestion du risque lié aux TIC

- Pour parer aux risques liés aux TIC et garantir un niveau élevé de résilience opérationnelle numérique
- Afin de garantir que tous les actifs informationnels et actifs de TIC sont correctement protégés contre les risques, y compris les dommages et les accès ou utilisations non-autorisés
- En déployant des stratégies, des politiques, des procédures, des protocoles et des outils TIC adéquats

Auditeurs internes

audits

Banque de France / ACPR / AMF

Demandes d'informations sur les risques liés aux TIC et leur cadre de gestion du risque

Le cadre de gestion du risque lié aux TIC

Dans ce cadre, les entités financières doivent mettre en œuvre ces fonctions

- Identification, classification et documentation des fonctions métiers s'appuyant sur des TIC
- Identification des sources de risques liées aux TIC
- Contrôle de la sécurité du fonctionnement des TIC et prévention des incidents
- Détection des incidents
- PCA
- Retour d'expérience post-incident
- Communication en cas d'incident
- Tests de résilience opérationnelle numérique

Le cadre de gestion du risque lié aux TIC

Un cadre de gestion du risque lié aux TIC

Comprenant :

Une stratégie en matière de risques liés aux **prestataires tiers de services TIC**

Comprenant :

Une **politique** relative à l'utilisation des services TIC soutenant des **fonctions critiques ou importantes** qui sont fournis par des **prestataires tiers** de services TIC

Réexamen au moins 1 fois / an

Application sur une base individuelle, consolidée ou sous-consolidée

Le cadre de gestion du risque lié aux TIC

Un cadre de gestion du risque lié aux TIC

Comprenant :

Une stratégie en matière de risques liés aux **prestataires tiers de services TIC**

Comprenant :

Une **politique** relative à l'utilisation des services TIC soutenant des **fonctions critiques ou importantes** qui sont fournis par des **prestataires tiers** de services TIC

Responsabilité incombant à l'organe de direction

Le cadre de gestion du risque lié aux TIC

Les entités financières tiennent et mettent à jour :

un **registre** d'informations en rapport avec tous les accords contractuels portant sur l'utilisation de services TIC fournis par des prestataires tiers de services TIC.

Le registre distingue entre les contrats qui soutiennent des fonctions critiques et les autres

Communication 1 x / an des informations relatives aux nouveaux contrats

Demande de communication

Mise à disposition

Information sur les projets de contrats relatifs à une fonction critique ou importante

Autorités compétentes

Le cadre de gestion du risque lié au TIC

La politique des services TIC fournis par des prestataires tiers

Les contrats avec les prestataires tiers de services TIC

La politique des services TIC tiers

Sont considérés comme des prestataires tiers : les prestataires entièrement ou collectivement détenus par des entités financières (prestataires « intragroupe »)

Sont considérés comme des prestataires tiers tous les sous-traitants de ces prestataires

Comprenant :

Une **politique** relative à l'utilisation des services TIC soutenant des **fonctions critiques ou importantes** qui sont fournis par des **prestataires tiers** de services TIC

La politique des services TIC tiers

La politique de gouvernance des services TIC tiers tient compte :

- Du type de services TIC fournis par les prestataires tiers
- De la situation géographique des prestataires et de leur société mère
- Du lieu à partir duquel les services sont fournis et les données traitées
- De la nature des données traitées par les prestataires tiers
- Du recours à des prestataires tiers qui sont agréés, immatriculés ou soumis à la surveillance ou à la supervision d'une autorité compétente
- De la concentration des services auprès d'un ou d'un petit nombre de prestataires tiers
- De la transférabilité des services
- De l'impact potentiel de perturbations dans la fourniture des services TIC sur la continuité des activités de l'entité financière

La politique des services TIC tiers

La politique met en place un dispositif de gouvernance des services TIC tiers

La politique établit ou fait référence à une **méthode** permettant de déterminer quels services TIC soutiennent des fonctions critiques ou importantes

La politique garantit le maintien des **compétences**, de l'expérience et des connaissances nécessaires à une supervision effective des contrats de services TIC

La politique doit suivre toutes les étapes de chaque phase importante du **cycle de vie des contrats**

La politique doit préciser et énoncer clairement les **responsabilités** internes en matière d'approbation, de gestion, de contrôle et de documentation des contrats sur les services TIC

La politique précise les mesures appropriées de détection, de prévention et de gestion des **conflits d'intérêts** réels ou potentiels découlant du recours à des prestataires tiers de services TIC

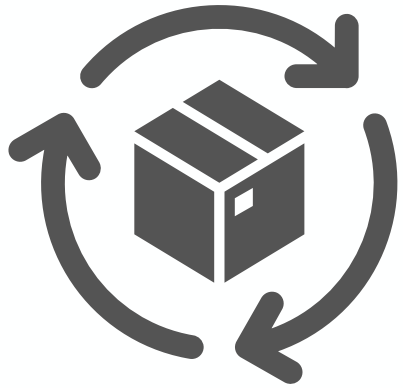
La politique désigne un membre de la **direction générale** en charge du suivi du respect des contrat avec les prestataires tiers.

La politique exige un **audit** indépendant des services TIC

La politique des services TIC tiers

La politique précise les règles, processus et responsabilité à chaque phase du cycle de vie du contrat avec le prestataire tiers :

- Responsabilité de l'organe de direction
- Rôle des contrôles internes
- Planification des contrats
- Mise en œuvre, suivi et gestion des contrats
- Rôle des directions opérationnelles
- Stratégies de sortie et de résiliation



La politique des services TIC tiers

Elle définit un processus de **sélection** des prestataires TIC tiers

Vérification de la réputation, des capacités, de l'expertise, des ressources financières, humaines et techniques, des normes de sécurité, de la structure organisationnelle, de la gestion des risques, des contrôles internes du prestataire

Vérification de la capacité du prestataire à suivre les évolutions technologiques et de mettre en œuvre les pratiques « de pointe » en matière de sécurité

Vérification du recours à des sous-traitants

Vérification si l'hébergement des données hors UE augmente les risques

Vérification que le prestataire agit de manière éthique et socialement responsable, respecte les droits de l'homme et les droits de l'enfant, les principes applicables en matière de protection de l'environnement, et garantit des conditions de travail appropriées.

La politique des services TIC tiers

Elle définit un processus de **sélection** des prestataires TIC tiers

Recours uniquement à des prestataires de services TIC qui respectent des **normes** adéquates en matière de sécurité de l'information.

Lorsque ces accords contractuels portent sur des fonctions critiques ou importantes, les entités financières prennent en considération, avant la conclusion des accords, l'utilisation par les prestataires tiers de services TIC des **normes** les plus actualisées et les plus élevées en matière de sécurité de l'information.

Audit ou évaluations indépendante

Certifications de tiers

La politique des services TIC tiers

La politique requiert, avant la conclusion du contrat, une **évaluation des risques** liés au recours au service d'un prestataire TIC tiers

Risques opérationnels
Risques juridiques
Risques liés aux TIC
Risques réputationnels
Risques liés à la protection de données confidentielles ou à caractère personnel
Risques liés à la disponibilité des données
Risques liés au lieu où les données sont traitées et stockées
Risques liés à la situation géographique du prestataire tiers de services TIC
Risques de concentration de TIC au niveau de l'entité

La politique des services TIC tiers

La politique garantit :

que les incidents liés aux TIC et les incidents opérationnels ou liés à la sécurité des paiements seront notifiés à l'entité financière lorsque cela est approprié

qu'un examen indépendant et des audits indépendants seront effectués pour vérifier le respect des exigences politiques légales et réglementaires.

Le cadre de gestion du risque lié au TIC

La politique des services TIC fournis par des prestataires tiers

Les contrats avec les prestataires tiers de services TIC

Avant la conclusion du contrat

Les entités financières :

- déterminent si l'accord contractuel couvre l'utilisation de services TIC qui soutiennent une fonction critique ou importante
- évaluent si les conditions de surveillance en matière de conclusion de contrats sont remplies
- identifient et évaluent tous les risques pertinents ayant trait à l'accord contractuel, y compris la possibilité que cet accord contractuel contribue à accroître le risque de concentration informatique
- font preuve de toute la diligence requise à l'égard des prestataires tiers de services TIC potentiels et s'assurent, tout au long des processus de sélection et d'évaluation, que les prestataires tiers de services TIC présentent les qualités requises
- identifient et évaluent les conflits d'intérêts susceptibles de découler de l'accord contractuel

La politique des services TIC tiers

La politique prévoit les **engagements contractuels** du prestataire tiers de services TIC en matière de :

CONTROLE	SLA	AUDIT	REVERSIBILITE
Fourniture par le prestataire de rapports périodiques sur les services fournis, sur les incidents, sur la sécurité, sur la continuité d'activité	Chaque contrat précise (i) les mesures et les indicateurs clés de suivi des performances et du respect des exigences de confidentialité, disponibilité, intégrité authenticité des données ; (ii) les mesures en cas de manquement aux SLA, le cas échéant.	Le contrat prévoit des audits (notamment des « pen tests ») par l'entité financière, le prestataire lui-même ou un tiers certificateur	Chaque contrat doit s'accompagner d'un plan de sortie documenté, régulièrement réexaminé et testé
Indicateurs de performance, de contrôle, d'audits, auto-certifications, examens indépendants		L'entité financière ne peut s'appuyer uniquement sur des certifications ou des audits fournis par le prestataire.	
Coopération avec les autorités de contrôle		Accès aux locaux du prestataire	

La formalisation des contrats

Le contrat entre l'entité financière et le prestataire de services TIC doit :

- Être écrit
- Comprendre l'intégralité des droits et obligations entre les parties, y compris les SLA
- Être conclu sur papier ou sous format téléchargeable, durable et accessible.
- Contenir a minima les clauses suivantes

Toute modification doit être convenue par avenant

- Une **description** claire et exhaustive **de tous les services TIC** et fonctions qui seront fournis par le prestataire, indiquant si la sous-traitance d'un service TIC qui soutient une fonction critique ou importante, ou de parties significatives de celle-ci, est autorisée et, le cas échéant, les conditions applicables à cette sous-traitance.
- Les **lieux**, notamment les régions ou les pays, où les services TIC et fonctions visés par le contrat ou la sous-traitance seront fournis et où les données seront traitées, y compris le lieu de stockage, et l'obligation pour le prestataire d'informer au préalable l'entité financière si celui-ci envisage de changer ces lieux.
- Des dispositions sur la **disponibilité**, **l'authenticité**, **l'intégrité** et la **confidentialité** en ce qui concerne la protection des données, y compris les données à caractère personnel.
- Des dispositions sur la **garantie de l'accès, de la récupération et de la restitution**, dans un format facilement accessible, des données à caractère personnel et autres traitées par l'entité financière en cas d'insolvabilité, de résolution, de cessation des activités du prestataire ou de résiliation du contrat.
- Des descriptions des **niveaux de service**, y compris leurs mises à jour et révisions.
- L'obligation pour le prestataire de fournir à l'entité financière, sans frais supplémentaires ou à un coût déterminé ex ante, une **assistance en cas d'incident** lié aux TIC en rapport avec le service TIC fourni à l'entité financière.
- L'obligation pour le prestataire de **coopérer** pleinement **avec les autorités** compétentes et les autorités de résolution de l'entité financière, y compris les personnes nommées par eux.
- Les droits de **résiliation** et les délais de préavis minimaux correspondants pour la résiliation du contrat, conformément aux attentes des autorités compétentes et des autorités de résolution.
- Les conditions de participation du prestataire aux **programmes de sensibilisation à la sécurité** des TIC et aux formations à la résilience opérationnelle numérique élaborés par les entités financières.

- Des descriptions complètes **des niveaux de service**, y compris leurs mises à jour et révisions, assorties d'objectifs de performance quantitatifs et qualitatifs précis dans le cadre des niveaux de service convenus, afin de permettre un suivi efficace par l'entité financière des services TIC, et de prendre, sans retard injustifié, des mesures correctives appropriées lorsque les niveaux de service convenus ne sont pas atteints.

- Les **délais de préavis et les obligations de notification** du prestataire à l'entité financière, y compris la notification de tout développement susceptible d'avoir une incidence significative sur la capacité du prestataire à fournir les services TIC qui soutiennent des fonctions critiques ou importantes de manière efficace conformément aux niveaux de service convenus.

- L'obligation pour le prestataire de mettre en œuvre et de tester des **plans d'urgence** et de mettre en place des mesures, des outils et des **politiques de sécurité des TIC** qui fournissent un niveau approprié de sécurité en vue de la prestation de services par l'entité financière, conformément à son cadre réglementaire.

- L'obligation pour le prestataire de participer et de coopérer pleinement au **test de pénétration** fondé sur la menace effectué par l'entité financière.

- Le droit d'assurer un suivi permanent des performances du prestataire, qui comprend les éléments suivants : (i) les **droits illimités d'accès, d'inspection et d'audit** par l'entité financière ou par une tierce partie désignée, et par l'autorité compétente, et le droit de prendre des copies des documents pertinents sur place s'ils sont essentiels aux activités du prestataire, dont l'exercice effectif n'est pas entravé ou limité par d'autres accords contractuels ou politiques d'exécution ; (ii) le droit de convenir d'autres niveaux d'assurance si les droits d'autres clients sont affectés ; (iii) l'obligation pour le prestataire de **coopérer** pleinement lors des inspections sur place et des audits effectués par les **autorités compétentes,** le superviseur principal, l'entité financière ou une tierce partie désignée ; et (iv) l'obligation de fournir des précisions sur la portée, les procédures à suivre et la fréquence de ces inspections et audits.

- Les **stratégies de sortie**, en particulier la fixation d'une période de transition adéquate obligatoire: (i) au cours de laquelle le prestataire tiers de services TIC continuera à fournir les fonctions ou services TIC concernés en vue de réduire le risque de perturbation au niveau de l'entité financière ou d'assurer sa résolution et sa restructuration efficaces ; (ii) qui permet à l'entité financière de migrer vers un autre prestataire ou de recourir à des solutions en interne adaptées à la complexité du service fourni.

- Le droit de **résilier** le contrat lorsque :

a) le prestataire tiers de services TIC a gravement enfreint les dispositions législatives, réglementaires ou contractuelles applicables ;

b) le suivi des risques liés aux prestataires tiers de services TIC a révélé l'existence de circonstances susceptibles d'altérer l'exécution des fonctions prévues par l'accord contractuel, y compris des changements significatifs qui affectent l'accord ou la situation du prestataire tiers de services TIC ;

c) le prestataire tiers de services TIC présente des faiblesses avérées liées à sa gestion globale du risque lié aux TIC et, en particulier, dans la manière dont il assure la disponibilité, l'authenticité, l'intégrité et la confidentialité des données, qu'il s'agisse de données à caractère personnel ou autrement sensibles, ou de données à caractère non personnel ;

d) l'autorité compétente ne peut plus surveiller efficacement l'entité financière en raison des conditions de l'accord contractuel en question ou des circonstances qui y sont liées.

IT & PLATFORMS

DATA & PRIVACY

IP & ENTERTAIN-MENT

AI & DIGITAL ASSETS

NEXT

RECOGNIZED BY

Best Lawyers®

Information Technology Law
Intellectual Property Law
Media Law
Technology Law
Privacy and
Data Security Law

DÉCIDEURS MAGAZINE

HIGHLY RECOMMENDED

Live Shows
Music Law
Digital Platforms Law
Data Protection Law

2025

LES MEILLEURS CABINETS D'AVOCATS 2025
Le Point
EN COLLABORATION AVEC statista

Droit des Technologies Informatique & Communication

Propriété littéraire & artistique

LEADING FIRM
Legal500
EMEA
2025

IT & internet

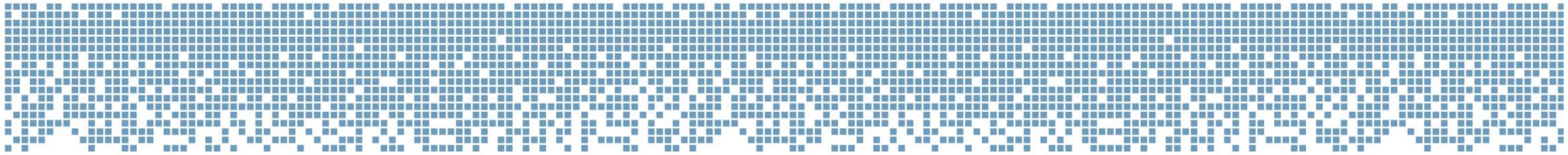
Intellectual Property: Copyright

Media & entertainment Music

Data privacy & protection

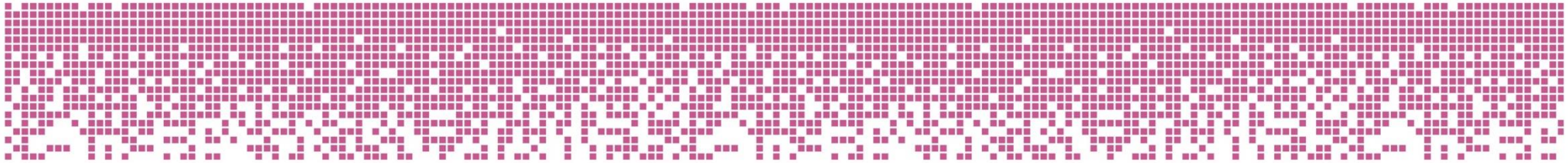
NEXT

INFORMATIQUE INTERNET RESEAUX SOCIAUX PLATEFORMES E-COMMERCE

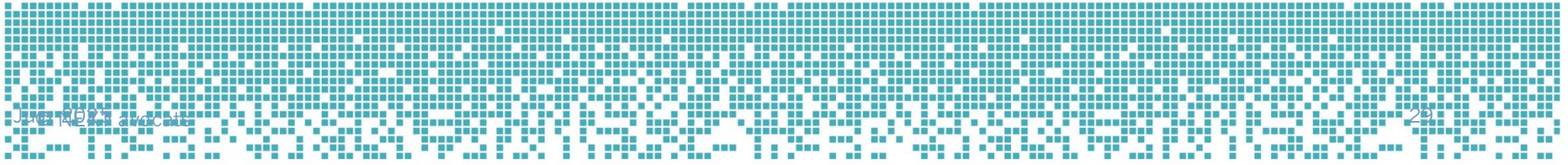


DONNEES PERSONNELLES RGPD DATA PRIVACY CYBERSECURITE

CREATION SPECTACLES DIVERTISSEMENT AUDIOVISUEL DESIGN



INTELLIGENCE ARTIFICIELLE ACTIFS NUMERIQUES TRANSITION DIGITALE



NEXT

L'actualité du droit du numérique
et de la création décryptée.
Suivez-nous :

www.linkedin.com/company/next-avocats/

www.instagram.com/