plan EU



LIVRE BLANC · OCTOBRE 2026

La dépendance numérique est un risque d'entreprise

Pourquoi chaque organisation européenne doit savoir où se trouvent ses logiciels, ses données et ses paiements, et a besoin d'un plan de sortie pour les services dont elle ne peut pas se passer.

SYNTHÈSE

En bref

Pour la messagerie, les documents, la comptabilité, les paiements et l'hébergement, les organisations européennes reposent largement sur des services de fournisseurs non européens. Cela fonctionne généralement très bien, jusqu'au moment où une décision prise hors d'Europe entraîne la restriction, la coupure ou l'intenabilité juridique d'un service.

POINTS CLÉS

- **Le risque n'est pas technique mais juridique et politique.** Les lois, les sanctions et les règles d'exportation du pays du fournisseur peuvent déterminer si votre service continue de fonctionner.
- **La plupart des dépendances sont invisibles.** Elles se trouvent chez vos prestataires et leurs sous-traitants, pas seulement dans votre propre informatique.
- **La réglementation l'exige déjà.** DORA impose aux établissements financiers des stratégies de sortie ; NIS2 et le RGPD exigent une visibilité sur la chaîne ; le Data Act facilite le changement de service cloud.
- **Changer n'est pas toujours nécessaire, être préparé l'est.** Un plan de sortie pour chaque service critique fait la différence entre une semaine difficile et des semaines d'arrêt.

Ce livre blanc décrit où se situent ces dépendances, quels mécanismes en font un risque, ce que demande la réglementation et comment passer en cinq étapes de la prise de conscience à un plan de sortie opérationnel.

Pour qui ? Administrateurs, dirigeants et responsables de la conformité et de l'informatique d'organisations européennes de tous secteurs, avec une attention particulière pour les établissements financiers soumis à DORA.

1 La dépendance silencieuse

Demandez à n'importe quelle organisation quels logiciels elle utilise, et la réponse vient vite : une suite bureautique, un logiciel comptable, un CRM, un prestataire de paiement. Demandez ensuite où tournent ces services, à quel droit le fournisseur est soumis et ce qui se passe si le service n'est plus disponible demain, et le silence s'installe.

C'est compréhensible. Les services cloud sont populaires justement parce qu'on n'a pas à y penser. Mais il en résulte qu'en peu de temps, le fonctionnement quotidien de nombreuses organisations européennes dépend d'un petit nombre de fournisseurs hors d'Europe, sans que personne ne l'ait choisi consciemment.

> **Le problème n'est pas d'utiliser des services non européens. Le problème, c'est de ne pas savoir quoi faire s'ils disparaissent.**

Un exemple qui a marqué

En 2025, il a été largement rapporté que le procureur de la Cour pénale internationale à La Haye, après des sanctions américaines contre la Cour, n'avait plus accès à sa messagerie chez un fournisseur américain. Les récits divergent sur les circonstances exactes. Mais pour beaucoup d'organisations, le principe est soudain devenu concret : la décision d'un gouvernement étranger peut, par l'intermédiaire d'un fournisseur, toucher directement une organisation européenne, même si celle-ci n'a rien fait de mal.

La même chose peut arriver pour des raisons moins spectaculaires : une hausse de prix qui rend un service inabordable, un produit abandonné, un compte bloqué par un contrôle automatisé, ou un fournisseur racheté.

2 Trois mécanismes derrière le risque

La dépendance à un fournisseur non européen devient un risque par trois voies. Elles sont indépendantes de la qualité ou des bonnes intentions du fournisseur.

01

Compétence juridique

Un fournisseur est soumis au droit du pays où il est établi. Le CLOUD Act américain (2018) permet par exemple aux autorités américaines de demander des données à des fournisseurs américains, même si ces données sont stockées en Europe. Cela peut entrer en conflit avec le RGPD.

02

Sanctions et règles d'exportation

Les États peuvent obliger des entreprises à cesser de fournir des services à certaines personnes, organisations ou pays. Le fournisseur n'a alors pas le choix. Pour vous, cela peut signifier la perte d'un service, ou un client ou une contrepartie qui n'est plus joignable.

03

Contrôle technique

Pour les services cloud et les appareils connectés, le fournisseur détient les clés techniques. Mises à jour, contrôles de licence ou désactivation de fonctions peuvent se faire à distance, avec ou sans mauvaise intention.

Pas seulement les États-Unis

Le débat porte souvent sur les géants technologiques américains, parce qu'ils servent la plus grande partie du marché. Mais il en va de même pour des fournisseurs d'autres pays. Un exemple clair : les véhicules connectés, les bornes de recharge, les onduleurs et autres équipements dont le logiciel peut être mis à jour ou désactivé à distance. En janvier 2025, les États-Unis ont adopté des règles qui excluent les logiciels chinois et russes des véhicules connectés à partir de l'année-modèle 2027, précisément pour cette raison. Pour les entreprises européennes disposant de flottes, d'activités logistiques ou d'installations énergétiques, la question est directe : qui peut commander vos équipements à distance ?

Pourquoi maintenant ?

Ces risques ont toujours existé, mais trois évolutions les rendent plus pressants : les rapports géopolitiques sont devenus moins prévisibles, de plus en plus de processus métier tournent exclusivement dans le cloud, et la réglementation européenne attend désormais des organisations qu'elles maîtrisent ces risques de manière démontrable.

3 La chaîne cachée

Les plus grandes dépendances ne se trouvent souvent pas dans votre propre informatique, mais chez vos prestataires. Votre cabinet comptable, votre prestataire de paie, votre infogérant ou votre auditeur utilise lui aussi des logiciels et un hébergement, et ces choix vous échappent.

Exemple : la chaîne financière

Un gestionnaire de fonds confie souvent l'administration de ses fonds à un administrateur spécialisé, travaille avec un dépositaire ou un trustee et avec un prestataire de conformité externe. Chacun de ces acteurs fonctionne sur ses propres systèmes : un logiciel d'administration, une plateforme documentaire, une messagerie, un hébergeur. Le gestionnaire reste responsable en dernier ressort, mais n'a souvent aucune visibilité sur les éléments situés hors d'Europe.

MAILLON	QUESTION TYPE QUI RESTE SANS RÉPONSE
Votre organisation	Quels services utilisons-nous, et lesquels sont critiques ?
Prestataire direct	Sur quels logiciels et quel hébergement repose le service qu'il nous fournit ?
Sous-traitants (sous-traitants ultérieurs)	Où se trouvent les données et à quel droit ces acteurs sont-ils soumis ?
Contrat	Qu'a-t-on convenu sur la résiliation, le transfert des données et la sortie ?

La réponse à ces questions existe généralement, dans les accords de traitement, les listes de sous-traitants ultérieurs et les clauses contractuelles, mais elle est dispersée et longue à rassembler. C'est précisément là que les choses se gâtent en pratique.

Conseil. Demandez à vos principaux prestataires leur liste à jour de sous-traitants ultérieurs, avec le pays d'établissement et la localisation des données. Selon le RGPD, un sous-traitant ne peut pas recruter de sous-traitant ultérieur sans votre autorisation et doit vous informer à l'avance de tout changement.

4 Ce que demande la réglementation

Les règles européennes n'obligent personne à n'utiliser que des fournisseurs européens. Elles exigent en revanche que les organisations connaissent leurs dépendances, maîtrisent les risques et puissent changer de fournisseur si nécessaire.

TEXTE	POUR QUI	CE QUI COMPTE
DORA Règlement (UE) 2022/2554, applicable depuis le 17 janvier 2025	Banques, assureurs, entreprises d'investissement, gestionnaires de fonds agréés et autres entités financières (seuls les gestionnaires de FIA simplement enregistrés sont exclus)	Registre de tous les contrats de services TIC ; évaluation des risques avant contractualisation ; stratégies de sortie obligatoires pour les services TIC soutenant des fonctions critiques ou importantes ; attention au risque de concentration.
NIS2 Directive (UE) 2022/2555	Entités essentielles et importantes, notamment dans l'énergie, les transports, la santé, l'infrastructure numérique et l'administration	Obligation de sécuriser la chaîne d'approvisionnement, y compris l'évaluation des fournisseurs et prestataires.
RGPD Règlement (UE) 2016/679	Toute organisation qui traite des données personnelles	Transferts hors de l'EEE uniquement avec des garanties appropriées ; depuis l'arrêt Schrems II (2020), il faut évaluer au cas par cas si le droit du pays destinataire compromet ces garanties.
Data Act Règlement (UE) 2023/2854, applicable depuis le 12 septembre 2025	Clients et fournisseurs de services cloud	Droit de changer de fournisseur ; les frais de changement diminuent progressivement et disparaissent à partir de janvier 2027. Un plan de sortie devient ainsi plus réaliste en pratique.

Attention. Ce tableau est une présentation simplifiée et ne constitue pas un conseil juridique. Les obligations exactes qui s'appliquent à votre organisation dépendent de votre secteur, de votre taille et de vos agréments. Pour chaque texte, vous pouvez vérifier sur les pages législation s'il vous concerne.

5 De la prise de conscience au plan de sortie

Plan EU suit une démarche fixe en cinq étapes. Vous pouvez réaliser les premières vous-même avec le scan ; pour l'approfondissement et le plan de sortie, nous vous accompagnons.

1

Domaine

À partir de votre nom de domaine, nous identifions les services visibles publiquement, comme les fournisseurs de messagerie et d'hébergement.

2

Secteur

Votre secteur détermine la réglementation et les dépendances types qui sont pertinentes.

3

Questions par domaine

De courtes questions à choix multiple par domaine : bureautique, comptabilité, paiements, hébergement, communication, prestataires.

4

Rapport

Pour chaque réponse, une position sur l'échelle de risque de Plan EU, avec explication et alternatives européennes.

5

Plan de sortie et conseil

Un plan pas à pas pour chaque service non européen. Si vous le souhaitez, nous examinons les contrats, recueillons les réponses des fournisseurs et accompagnons le changement.

L'échelle de risque

● Souverain	◐ Maîtrisable	○ Vulnérable	■ Critique
Fournisseur européen, données et gestion au sein de l'UE.	Non européen, mais pas critique pour l'activité ou facile à remplacer.	Non européen et important pour l'activité.	Non européen, critique pour l'activité et difficile à remplacer.

Le scan ne conserve aucune donnée qui ne soit nécessaire au rapport. Nous évaluons des situations, pas des fournisseurs : le rapport décrit de manière factuelle où un service est établi et ce que cela signifie pour vous. Plus de détails dans notre méthodologie.

6 Ce que contient un bon plan de sortie

Un plan de sortie n'est pas un plan de déménagement. C'est une préparation qui vous permet de changer quand c'est nécessaire, de façon planifiée ou sous pression. Pour chaque service classé vulnérable ou critique, consignez au minimum :

- **Fonction et responsable.** Quel processus métier dépend du service et qui en est responsable ?
- **Données.** Quelles données s'y trouvent, dans quel format pouvez-vous les exporter, et à quelle fréquence le faites-vous ?
- **Alternative.** Au moins une alternative européenne, avec une estimation approximative du coût et du délai.
- **Contrat.** Délai de préavis, accords sur le transfert des données, assistance à la sortie et vos droits au titre du Data Act.
- **Scénario d'urgence.** Que faites-vous dans les 48 premières heures si le service disparaît soudainement ?
- **Dépendances.** Quels autres systèmes ou interfaces s'arrêtent aussi ?
- **Revue.** Quand le plan est-il revu et testé ?

Pour des dizaines de services courants, un tel plan est déjà prêt dans nos plans de sortie.

Cinq choses à faire ce mois-ci

1. Dressez la liste des dix services sans lesquels votre organisation s'arrête en une journée.
2. Notez pour chaque service le pays d'établissement du fournisseur et la localisation des données.
3. Demandez à vos principaux prestataires leur liste de sous-traitants ultérieurs.
4. Vérifiez que vous pouvez réellement exporter vos données essentielles dans un format exploitable.
5. Faites le scan sur plan-eu.eu pour un premier aperçu.

Sources

- Règlement (UE) 2022/2554 sur la résilience opérationnelle numérique du secteur financier (DORA), en particulier l'article 28.
- Directive (UE) 2022/2555 (NIS2), en particulier l'article 21 sur la sécurité de la chaîne d'approvisionnement.
- Règlement (UE) 2016/679 (RGPD), chapitre V ; CJUE, 16 juillet 2020, C-311/18 (Schrems II).
- Règlement (UE) 2023/2854 (Data Act), chapitre VI sur le changement de service de traitement de données.
- Clarifying Lawful Overseas Use of Data Act (CLOUD Act), États-Unis, 2018.

plan EU

PLAN-EU.EU

À propos de Plan EU

Plan EU aide les organisations européennes à cartographier leurs dépendances numériques et à établir un plan de sortie opérationnel. Avec un scan en ligne, un rapport clair et des conseils sur mesure, du second avis DORA à l'accompagnement du passage vers une alternative européenne.

plan-eu.eu

info@plan-eu.eu

Plan EU est une initiative de Luce Holding B.V. Ce livre blanc a été rédigé avec soin sur la base d'informations publiques disponibles en octobre 2026 et a une vocation d'information générale. Il ne crée aucun droit et ne constitue pas un conseil juridique, fiscal ou en investissement. Plan EU n'est pas une institution de l'Union européenne.