Souveraineté numérique : checklist pour les acteurs des transactions

Dans le cadre d'opérations de capital-investissement, de fusions-acquisitions, d'immobilier ou de financement, vos informations les plus sensibles ainsi que vos échanges liés aux transactions sont hébergés sur des plateformes de data room.
La souveraineté numérique désigne la question de savoir qui détient, en dernier ressort, le contrôle de ces données — et quelles législations peuvent contraindre votre fournisseur à les communiquer. L'une des lois extraterritoriales les plus importantes dans ce contexte est le CLOUD Act américain.

Qu'est-ce que le CLOUD Act américain ?

- Le Clarifying Lawful Overseas Use of Data Act (CLOUD Act) est une loi fédérale américaine promulguée en 2018.
- Il permet aux autorités américaines d'exiger des fournisseurs américains de services de communications électroniques et de cloud qu'ils communiquent des données, quel que soit leur lieu de stockage dans le monde.
- Il s'applique non seulement aux données américaines, mais à toute donnée « en possession, sous la garde ou sous le contrôle » d'un fournisseur relevant de la juridiction américaine.
- En juin 2025, Microsoft France a confirmé devant le Sénat français qu'elle pourrait, en dernier ressort, être contrainte de transmettre des données stockées en France sur la base d'une décision de justice américaine — ce qui souligne que la juridiction suit le fournisseur, et non uniquement l'emplacement des serveurs.

Qui est concerné ?

1. Les fournisseurs dont le siège est situé aux États-Unis et qui détiennent ou hébergent des données, y compris dans des centres de données européens.
2. Les fournisseurs non américains contrôlés par une société mère ou une holding américaine et relevant, à ce titre, du droit américain.

La plateforme européenne pour des transactions véritablement souveraines

- Drooms est détenue et contrôlée à 100 % par des intérêts européens, avec des sièges sociaux en Allemagne et en Suisse.
- L'ensemble des données clients est hébergé sur des serveurs géoredondants situés en Europe.
- La plateforme ainsi que les fonctionnalités d'intelligence artificielle sont développées en interne en Europe.
- L'entreprise est soumise exclusivement au droit européen et n'est pas concernée par le CLOUD Act américain.

Plus d'informations sur notre sécurité | Contact commercial

Checklist de souveraineté numérique pour votre prochaine data room

Utilisez cette liste de contrôle dans vos appels d'offres, vos processus d'achat et vos évaluations internes des risques avant de choisir une plateforme de transaction.

A. Entreprise et juridiction

- [ ] L'entreprise a-t-elle son siège social en Europe ?
- [ ] L'entreprise est-elle entièrement détenue et contrôlée par des intérêts européens, sans société mère ni investisseurs majoritaires non européens ?
- [ ] L'entreprise, ou toute entité mère, n'est-elle pas soumise à la loi américaine CLOUD Act ?

B. Infrastructure et localisation des données

- [ ] Vos données seront-elles stockées et traitées exclusivement en Europe ?
- [ ] Tous les sous-traitants (le cas échéant) chargés du stockage ou du traitement de vos données sont-ils situés en Europe ?
- [ ] L'ensemble du service client, qui peut avoir accès aux données, est-il assuré depuis l'Europe ?

C. Technologie et IA

- [ ] La technologie de base de la plateforme (y compris les fonctionnalités d'IA) est-elle développée en interne ?
- [ ] Les fonctionnalités de communication intégrées sont-elles régies uniquement par les juridictions européennes ?
- [ ] Le fournisseur précise-t-il clairement où les services d'analyse par IA sont exécutés (cloud et région) ?
- [ ] Vos données en temps réel sont-elles exclues par défaut de l'entraînement de l'IA de la plateforme ?
- [ ] Aucune de vos données n'est-elle transmise à des modèles d'IA publics ?

D. Demandes émanant d'autorités étrangères

- [ ] L'entreprise dispose-t-elle d'un processus documenté pour traiter les demandes émanant de gouvernements ou d'autorités chargées de l'application de la loi situés en dehors de l'Europe ?
- [ ] Le fournisseur peut-il expliquer clairement comment il réagirait à une injonction américaine de partager vos données ?
- [ ] Le fournisseur peut-il confirmer qu'il n'a jamais divulgué de données de clients hébergées en Europe à des autorités non européennes ?

E. Gouvernance, certifications et contrats

- [ ] Le fournisseur est-il certifié selon des normes de sécurité reconnues telles que ISO 27001 / 27018 ?
- [ ] Toutes les activités de la salle de données sont-elles consignées, et les journaux peuvent-ils être exportés à des fins d'audit ou de procédure judiciaire ?
- [ ] La plateforme offre-t-elle des contrôles détaillés sur les autorisations d'accès, jusqu'au niveau des documents et des utilisateurs ?