Développements réglementaires

Autres évolutions récentes en matière de réglementation

Dernière mise à jour : septembre 2025

Table des matières

1 Autres développements

La loi européenne sur l'IA introduit un cadre fondé sur les risques pour réglementer les systèmes d'intelligence artificielle. Cette législation définit les règles relatives au développement, à la mise sur le marché et à l'utilisation de l'IA dans l'Union européenne, afin de garantir que l'IA est digne de confiance, éthique et respecte les droits fondamentaux.

Status:
- En vigueur depuis le 1er août 2024

1.1 Loi européenne sur l'IA

Applicabilité de dispositions européennes plus strictes en matière de protection des données

La loi européenne sur l'IA, qui est entrée en vigueur le 1er août 2024, introduit un nouveau cadre réglementaire pour régir les systèmes d'intelligence artificielle. Il décrit les règles relatives au développement, à la mise sur le marché et à l'utilisation de l'IA dans l'Union européenne. Les obligations des fournisseurs de modèles d'IA à usage général ont commencé à s'appliquer le 2 août 2025. La majorité des exigences relatives aux systèmes d'IA à haut risque et la pleine applicabilité de nombreuses dispositions d'application entreront en vigueur à compter du 2 août 2026.

La loi européenne sur l'IA s'applique aux fournisseurs et aux utilisateurs de systèmes d'IA opérant au sein de l'UE, ainsi qu'aux fournisseurs et aux utilisateurs en dehors de l'UE si les résultats produits par le système sont destinés à être utilisés dans l'UE. Cette portée extraterritoriale signifie que les entreprises et les organisations, y compris les entreprises suisses, doivent se conformer à la loi sur l'IA de l'UE lorsque leurs systèmes d'IA ont un impact sur les citoyens de l'UE.

Conformité

La loi européenne sur l'IA définit une approche des applications de l'IA fondée sur les risques potentiels qu'elles représentent pour les droits fondamentaux, la sécurité et la vie privée. La loi sur l'IA classe les systèmes d'IA en quatre catégories principales en fonction du niveau de risque qu'ils présentent : risque inacceptable, haut, limité et minimal.

Les systèmes appartenant à la catégorie des risques inacceptables qui représentent des menaces importantes pour la sécurité, les droits ou la démocratie (tels que l'IA pour la notation sociale par les gouvernements) sont interdits. Les systèmes à haut risque utilisés dans des secteurs critiques tels que les soins de santé, l'application de la loi et les transports sont soumis à des exigences strictes, notamment en matière d'évaluation des risques, de gouvernance des données et de surveillance humaine. Ces systèmes devront également être enregistrés dans une base de données européenne des systèmes d'IA à haut risque. Les systèmes d'IA à risque limité, tels que ceux utilisés dans les interactions avec les chatbots, nécessitent des obligations de transparence, tandis que les systèmes d'IA à risque minimal sont largement non réglementés.

La loi sur l'IA introduit plusieurs exigences de conformité, telles que l'obligation d'assurer une surveillance humaine des systèmes d'IA, une documentation précise des données et des processus solides de gestion des risques. Les organisations qui développent ou déploient l'IA devront également procéder à des évaluations de conformité pour les systèmes à haut risque et, dans certains cas, à des auto-évaluations pour les applications à faible risque. Le Conseil européen de l'intelligence artificielle supervisera l'application de la législation et fournira des conseils aux autorités nationales et aux entreprises. Des sanctions importantes sont prévues en cas de non-respect de la loi. Les violations de

la loi sur l'IA, en particulier celles impliquant des systèmes d'IA à haut risque ou interdits, pourraient donner lieu à des amendes allant jusqu'à 7 % du chiffre d'affaires annuel mondial ou EUR 35 millions, le montant le plus élevé étant retenu, ce qui met en évidence les risques financiers importants encourus pour les entreprises qui ne respectent pas les réglementations.

La loi européenne sur l'IA vise à équilibrer l'innovation et la confiance du public en veillant à ce que les systèmes d'IA soient conçus, développés et utilisés de manière à protéger les droits et libertés fondamentaux des individus. Cette réglementation aura probablement de profondes répercussions sur l'innovation en matière d'IA dans toute l'Europe, en particulier pour les entreprises opérant dans des secteurs soumis à une surveillance réglementaire étroite ou à une forte interaction avec les consommateurs. La loi sur l'IA met également l'accent sur la gouvernance de l'IA, appelant à la transparence et à la traçabilité dans la prise de décision en matière d'IA, ce qui nécessitera des efforts techniques et organisationnels importants de la part des entreprises pour assurer la conformité.

Tout comme le RGPD, la loi européenne sur l'IA représente un changement critique dans les approches réglementaires, reconnaissant le pouvoir de transformation de l'IA tout en abordant les risques posés aux individus et à la société dans son ensemble. L'accent mis sur la responsabilité, l'équité et la transparence trouve un écho dans différents secteurs, et les entreprises devront adapter leurs modèles de gouvernance de l'IA en conséquence pour rester en conformité.

Qui est concerné ?

Toute organisation développant ou déployant l'IA au sein de l'Union européenne sera soumise à la loi sur l'IA. Cela inclut les organisations non européennes qui offrent des services ou des produits basés sur l'IA aux résidents de l'UE ou qui opèrent au sein de l'UE. Par exemple, une entreprise technologique suisse qui déploie un logiciel de diagnostic médical basé sur l'IA dans l'UE doit se conformer aux règles de classification à haut risque de la loi sur l'IA.

Ce que vous devez faire

Pour se préparer à la loi européenne sur l'IA, nous recommandons les étapes suivantes :

- Analyser les systèmes d'IA actuellement en service ou en cours de planification et identifier tous les systèmes d'IA à haut risque et à risque limité au sein de vos opérations qui seront soumis à de nouvelles réglementations.
- Veiller à ce que vos processus de développement de l'IA intègrent dès le départ la gestion des risques, les tests et la transparence.
- Examiner vos protocoles de documentation et d'évaluation des risques pour les aligner sur les normes de la loi sur l'IA, en particulier pour les systèmes à haut risque.

Votre expert PwC en protection des données se fera un plaisir de vous aider à évaluer vos systèmes d'IA actuels, de vous guider dans le paysage réglementaire et d'assurer votre conformité à la nouvelle législation sur l'IA.

1.2 La loi européenne sur les données

La loi européenne sur les données vise à créer un cadre harmonisé pour le partage, l'accès et l'utilisation des données entre les entreprises, les consommateurs et les institutions du secteur public dans l'Union européenne. La loi sur les données se concentre sur les données non personnelles, garantissant que l'innovation basée sur les données peut prospérer tout en maintenant l'équité, la concurrence et la souveraineté des données.

Status:
- En vigueur depuis le 12 septembre 2025

Applicabilité des règles de partage des données

La loi européenne sur les données est applicable à compter du 12 septembre 2025. La loi sur les données de l'UE s'appliquera dans toute l'Union européenne, établissant des droits et des obligations pour les entreprises et les organismes publics en ce qui concerne l'accès, le partage et l'utilisation des données non personnelles. La loi sur les données est particulièrement pertinente pour les entreprises qui développent des services en cloud, des produits de l'Internet des objets (IoT) et d'autres technologies à forte intensité de données.

Comme le RGPD et la loi sur l'IA de l'UE, la loi sur les données de l'UE s'étendra au-delà des frontières de l'UE, s'appliquant aux entreprises non européennes qui opèrent dans l'UE ou qui offrent des produits ou des services à des clients basés dans l'UE. Cette application extraterritoriale garantit que toutes les organisations traitant des données basées dans l'UE adhèrent aux mêmes règles.

À l'instar du RGPD et de la loi européenne sur l'IA, les entreprises suisses qui proposent des produits ou des services basés sur des données au marché de l'UE ou qui s'engagent dans des pratiques de partage de données avec des entreprises de l'UE devront s'assurer de leur conformité avec la loi européenne sur les données. Cela permet aux entreprises suisses de rester compétitives et pleinement conformes lorsqu'elles opèrent dans l'économie numérique de l'UE.

Conformité

Pour se conformer à la loi européenne sur les données, les entreprises devront :
S'assurer qu'elles disposent de processus clairs pour le partage des données non personnelles, notamment en ce qui concerne la portabilité des données, les droits d'accès et les conditions de changement de service dans le cloud.
- Développer des accords de partage de données solides qui s'alignent sur les principes énoncés dans la loi sur les données, garantissant un accès équitable aux données par des tiers.
- Assurer la transparence des conditions d'accès aux données et veiller à ce que les utilisateurs, qu'il s'agisse d'entreprises ou de consommateurs, aient le contrôle des données générées par leurs produits ou services.

La loi européenne sur les données impose également des restrictions aux fournisseurs de services en cloud en ce qui concerne la portabilité des données, les obligeant à faciliter les transitions en douceur entre les fournisseurs de services et à empêcher le verrouillage des données.

Qui est concerné ?

La loi européenne sur les données affectera un large éventail d'industries, en particulier celles des secteurs centrés sur les données comme l'IoT, l'informatique en cloud et l'IA. Les entreprises qui collectent, traitent et stockent des données non personnelles seront soumises aux nouvelles règles, tout

comme les institutions du secteur public qui accèdent aux données pour des besoins réglementaires ou sociétaux.

Toute entreprise qui propose des services ou des produits au sein de l'UE, ou qui traite des données générées par des utilisateurs basés dans l'UE, devra se conformer à la loi sur les données. Cette exigence s'étend aux entreprises non européennes (y compris les entreprises suisses) qui proposent des produits ou des services basés sur des données sur le marché européen ou qui s'engagent dans le partage de données avec des entreprises européennes.

Ce que vous devez faire

Pour vous préparer à la loi européenne sur les données, nous vous recommandons de suivre les étapes suivantes :

- Examiner vos pratiques actuelles en matière de partage des données et assurez-vous qu'elles sont conformes aux nouvelles exigences en matière de transparence et d'équité.
- Mettre en place des processus pour la portabilité des données et le passage transparent d'un fournisseur d'informatique dématérialisée à un autre, comme l'exige la loi sur les données.
- Mettre à jour les contrats et les accords de niveau de service avec les tiers afin de refléter les obligations en matière d'accès aux données et d'utilisation de celles-ci.

L'équipe de PwC chargée de la protection des données et de la conformité peut vous aider à évaluer vos stratégies actuelles de partage des données, afin que votre organisation soit prête à relever les défis et à saisir les opportunités qu'offre la loi européenne sur les données.

2 Normes internationales d'audit (ISA)

2.1 ISA 240 (révisée) « Responsabilités de l'auditeur concernant les fraudes lors d'un audit d'états financiers »

La norme révisée est une réponse aux attentes accrues des parties prenantes pour une norme d'audit plus robuste et une plus grande transparence sur le travail de l'auditeur lié à la fraude, à la suite de plusieurs faillites et scandales d'entreprises très médiatisés.

Status:
- s'applique aux audits des états financiers pour des périodes débutant le 15 décembre 2026 ou après cette date.

Les objectifs de la révision étaient les suivants :
- Clarifier les responsabilités des auditeurs : définir plus clairement les responsabilités des auditeurs en matière de fraude dans le cadre d'un audit des états financiers.
- Renforcer la réponse aux risques de fraude : améliorer la cohérence et l'efficacité des réactions des auditeurs face aux risques d'anomalies significatives dues à la fraude, en renforçant et en clarifiant les exigences de la norme ISA 240.
- Promouvoir le scepticisme professionnel : souligner l'importance de maintenir le scepticisme professionnel tout au long de l'audit dans les procédures d'audit liées à la fraude.
- Améliorer la transparence et la communication : améliorer la transparence des procédures liées à la fraude, le cas échéant, notamment en renforçant la communication avec les responsables de la gouvernance et les exigences de reporting de la norme ISA 240 et d'autres normes ISA pertinentes.

2.2 ISA 570 (révisée) « Continuité d'exploitation »

La norme révisée vise à promouvoir des pratiques et des comportements cohérents et comprend donc des exigences portant sur des responsabilités élargies de l'auditeur en matière d'évaluation de l'utilisation par la direction du principe de continuité d'exploitation de la comptabilité, ainsi que de nouveaux ajouts importants au rapport de l'auditeur.

Status:
- s'applique aux audits des états financiers pour des périodes débutant le 15 décembre 2026 ou après cette date.

La norme révisée vise à :
- Promouvoir la cohérence et l'efficacité : encourager des pratiques et des comportements d'audit cohérents ainsi que des réponses efficaces aux risques d'anomalies significatives liés à la continuité de l'exploitation.
- Renforcer l'évaluation par l'auditeur de l'examen de la continuité d'exploitation par la direction : renforcer l'évaluation par l'auditeur de l'examen de la continuité d'exploitation par la direction, en mettant fortement l'accent sur l'exercice du scepticisme professionnel tout au long de l'audit.
- Améliorer la transparence : améliorer la clarté en termes de responsabilités et de travail de l'auditeur liés à la continuité de l'exploitation, y compris des exigences plus strictes en matière de communication et de reporting.