DU BLOG IUSTORIA

AI Act : ce que les entreprises tchèques doivent savoir sur l'utilisation de l'intelligence artificielle

> *L'AI Act européen ne concerne pas que les développeurs — les entreprises qui déploient l'IA ont aussi des obligations.*

MGR. GABRIEL KOŽÍK

14/8/2025 · 6 min de lecture

Le règlement (UE) 2024/1689 du Parlement européen et du Conseil — communément appelé AI Act — est entré en vigueur le 1er août 2024. Les obligations s'appliquent de manière progressive : les premières depuis février 2025, d'autres depuis août 2025, et le régime complet prend effet en août 2026. Pourtant, la majorité des entreprises tchèques n'ont pas encore vérifié si ce règlement les concerne.

La raison est simple : on pense généralement que l'AI Act ne réglemente que ceux qui développent l'intelligence artificielle. C'est une erreur. Le règlement couvre également les déployeurs — c'est-à-dire les entreprises qui se contentent d'utiliser des systèmes d'IA dans le cadre de leur activité professionnelle.

Fournisseur et déployeur : une distinction essentielle

L'AI Act distingue deux rôles principaux. Le fournisseur (provider) est l'entité qui développe un système d'IA, ou le fait développer, et le met sur le marché sous son propre nom. Le déployeur (deployer) est l'entité qui utilise un système d'IA dans le cadre de son activité professionnelle.

Si votre entreprise utilise un outil d'IA pour évaluer ses employés, noter ses clients, automatiser des décisions de crédit ou trier des candidatures — vous êtes déployeur. Et vous avez des obligations.

Point essentiel : ces rôles peuvent se chevaucher. Une entreprise qui reprend un modèle open source, l'entraîne sur ses propres données et le déploie en interne peut devenir fournisseur — même si l'intention initiale était simplement d'« utiliser » l'IA.

Classification des risques : où se situe votre système

L'AI Act repose sur un cadre à quatre niveaux de risque.

Les pratiques interdites sont des systèmes d'IA qui ne doivent tout simplement pas exister — la notation sociale des citoyens, les techniques manipulatoires exploitant les vulnérabilités des personnes, l'identification biométrique en temps réel dans les espaces publics (avec des exceptions limitées pour les forces de l'ordre). Ces interdictions s'appliquent depuis février 2025.

Le risque élevé concerne les systèmes d'IA utilisés dans des domaines où une décision erronée a un impact significatif sur une personne. Cela inclut notamment : le recrutement et l'évaluation des employés, l'évaluation de la solvabilité, l'accès à l'éducation, les infrastructures critiques et les dispositifs médicaux. Les systèmes à haut risque sont soumis aux obligations les plus strictes — gestion des risques, documentation, supervision humaine et exigences de transparence.

Le risque limité s'applique aux systèmes qui interagissent avec des personnes (chatbots, générateurs de contenu). L'obligation principale est la transparence — les utilisateurs doivent savoir qu'ils communiquent avec une IA ou que le contenu a été généré par une IA.

Le risque minimal couvre la plupart des applications courantes de l'IA — filtres anti-spam, algorithmes de recommandation dans le commerce en ligne, optimisation logistique. L'AI Act n'impose ici aucune obligation spécifique, mais encourage les codes de conduite volontaires.

Liste de contrôle pratique : que faire maintenant

Fort de notre pratique de conseil, nous recommandons cinq étapes concrètes.

Premièrement : cartographiez les systèmes d'IA dans votre entreprise. La plupart des entreprises ignorent combien d'outils d'IA elles utilisent réellement. Il ne s'agit pas seulement de développements internes — pensez aux outils SaaS, aux services cloud, aux plateformes analytiques. Dressez un inventaire : de quoi s'agit-il, qui le fournit, à quoi cela sert, quelles données sont traitées.

Deuxièmement : classifiez le risque. Pour chaque système de votre inventaire, déterminez dans quelle catégorie il se situe. En cas de doute, partez de la catégorie supérieure — les conséquences d'une sous-estimation dépassent de loin les coûts d'une surestimation.

Troisièmement : désignez une personne responsable. L'AI Act n'exige pas explicitement un « responsable conformité IA », mais quelqu'un dans l'organisation doit avoir une vue d'ensemble des systèmes d'IA utilisés et des obligations qui en découlent. Dans les structures plus petites, ce rôle peut être confié au responsable conformité existant ou au juriste interne.

Quatrièmement : préparez la documentation. Pour les systèmes à haut risque, l'AI Act exige une documentation technique détaillée, des journaux de fonctionnement et des évaluations d'impact sur les droits fondamentaux. Mais même pour les systèmes à risque moindre, il est judicieux de documenter pourquoi et comment l'IA est déployée — ne serait-ce qu'en cas de contrôle ou de litige.

Cinquièmement : mettez en place la supervision humaine. Pour les systèmes à haut risque, une supervision humaine effective doit être garantie — c'est-à-dire la possibilité réelle pour une personne d'intervenir dans le processus décisionnel de l'IA. Les décisions automatisées sans possibilité de révision posent problème non seulement au regard de l'AI Act, mais aussi du RGPD.

Pourquoi l'AI Act est une opportunité

J'entends souvent l'objection : l'AI Act est une charge réglementaire de plus. D'une certaine manière, c'est vrai. Mais considérons l'autre côté de la médaille.

Une entreprise qui a cartographié ses systèmes d'IA, qui comprend leurs risques et qui tient une documentation rigoureuse est une entreprise qui comprend son propre fonctionnement. Dans la pratique, nous constatons que le processus de préparation à l'AI Act révèle des inefficacités, des redondances et des risques dont la direction n'avait pas connaissance.

De plus — et cet argument parle particulièrement aux entreprises tournées vers l'international — la conformité à l'AI Act devient un avantage concurrentiel. Le parallèle avec le RGPD est éclairant : les entreprises qui l'ont pris au sérieux dès le départ ne sont pas en difficulté aujourd'hui. Celles qui ont attendu en subissent encore les conséquences.

L'AI Act suit la même trajectoire. Les obligations arrivent progressivement, mais elles arrivent. Une entreprise qui se prépare maintenant aura une longueur d'avance sur celles qui ne s'en occuperont qu'après le premier contrôle.

L'AI Act n'est pas une réglementation sur l'intelligence artificielle dans un sens abstrait. C'est une réglementation sur la manière dont les entreprises utilisent des technologies qui prennent des décisions concernant des personnes. Cela concerne la plupart des entreprises — elles ne le savent simplement pas encore.

Si vous n'êtes pas certain que l'AI Act s'applique à votre entreprise, ou de quelle manière, contactez-nous. Un audit des systèmes d'IA prend quelques jours, pas des mois — et les conséquences de l'inaction peuvent se révéler incomparablement plus coûteuses. Si les obligations de l'AI Act touchent vos contrats fournisseurs, voyez aussi Cinq clauses contractuelles que personne ne lit — nombre d'obligations se retrouvent dans les clauses de sous-traitance et les contrats de prestation.

Vous utilisez des outils d'IA en entreprise et devez savoir si et comment l'AI Act s'applique ? Dans notre pratique de prévention des risques, nous auditons vos systèmes d'IA et concevons une feuille de route précise jusqu'à août 2026. Écrivez-nous.

AI Act : ce que les entreprises tchèques doivent savoir sur l'utilisation de l'intelligence artificielle

Mgr. Gabriel Kožík · Publié 14/8/2025

https://www.iustoria.cz/fr/blog/ai-act-ce-que-les-entreprises-tcheques-doivent-savoir/