SÉRIE « COMPRENDRE LE DROIT DE L'IA »

RÉGLEMENTATION DE L'IA EN SUISSE : CADRE RÉGLEMENTAIRE ET OBLIGATIONS DES ENTREPRISES EN 2025

Date: **le 7 octobre 2025**

Auteurs: Me Florian Ducommun; Me Crystal Dubois

Thématique d'expert : Intelligence artificielle ; droit de l'IA ; cadre réglementaire; technologies avancées ; droit de la technologie

L'intelligence artificielle (« **IA** ») est rapidement passée d'un terme général à un instrument créateur de réelles opportunités commerciales. Les organisations de tous les secteurs investissent massivement dans l'IA pour accroître la productivité, stimuler l'innovation et maintenir un avantage concurrentiel, tandis que les individus utilisent des outils d'IA pour amplifier leurs capacités et simplifier leurs flux de travail quotidiens.

Le secteur financier illustre parfaitement cette tendance. Une récente enquête menée par l'Autorité fédérale de surveillance des marchés financiers (FINMA)[1] a révélé que 50 % des 400 banques et autres institutions financières supervisées interrogées utilisent soit l'IA, soit développent des applications, avec en moyenne cinq applications en usage et neuf en cours de développement.

Chez Bonnard Lawson, nous nous sommes spécialisés dans le droit de l'intelligence artificielle au cours des dernières années. Nous participons activement à des groupes de travail d'experts et à des conférences du secteur. Nous conseillons nos clients sur les enjeux de développement et de déploiement de l'IA, les représentons dans les procédures contentieuses, et proposons des formations spécialisées aux conseils d'administration, équipes juridiques et équipes produits des entreprises. Nous intégrons également des outils d'IA dans notre pratique juridique pour maintenir notre avance dans ce domaine en constante évolution.

Tout en poursuivant notre travail et en approfondissant notre expérience, nous lançons cette série d'articles intitulée « Comprendre le droit de l'IA », afin de partager notre savoir et d'aider nos clients dans leurs efforts de conformité réglementaire.

Le présent premier article aborde les **points clés de la réglementation applicable à l'IA en Suisse, que les dirigeants d'entreprise, les équipes produits, les équipes juridiques et autres acteurs doivent prendre en compte lorsqu'ils développent des modèles d'IA, fournissent des systèmes d'IA à des tiers ou déploient de tels systèmes en interne**.

Cet article couvre la portée extraterritoriale du Règlement européen sur l'intelligence artificielle (« **AI Act** »)[2], l'approche réglementaire suisse, la nouvelle communication de la FINMA sur l'IA, les exigences en matière de protection des données, et fournit une checklist pratique de gouvernance pour les organisations.

Les prochains articles de la série « Comprendre le droit de l'IA » exploreront plus en détail la propriété intellectuelle, la responsabilité et d'autres questions critiques du droit de l'IA.

---

[1] Communication de la FINMA sur une enquête du 24 avril 2025, disponible sur : https://www.finma.ch/en/news/2025/04/20250424-mm-umfrage-ki/.

[2] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle.

1. L'AI Act et le champ d'application extraterritorial pour les entreprises suisses

Cet article n'a pas vocation à détailler toutes les dispositions de la réglementation européenne sur l'intelligence artificielle (AI Act), mais il est indispensable que les acteurs suisses gardent à l'esprit que ce texte peut aussi leur être applicable dans certaines hypothèses.

L'AI Act est entré en vigueur le 1er août 2024 et prévoit une application échelonnée. Il instaure un cadre légal harmonisé pour le développement, la mise sur le marché, la mise en service et l'utilisation des systèmes d'IA ainsi que des modèles d'IA à usage général dans l'Union européenne (UE). Il adopte une approche fondée sur le risque, avec une classification des systèmes IA selon les dommages potentiels.

Pour les entreprises suisses, le point le plus déterminant est la **portée extraterritoriale** du Règlement. L'AI Act régule le marché intérieur européen, et s'applique donc même aux entités établies hors de l'UE, si leurs produits ou services d'IA sont utilisés dans l'UE.

Concrètement, l'AI Act s'applique aux **fournisseurs mettant des systèmes d'IA ou des modèles d'IA à usage général sur le marché de l'UE ou en service dans l'UE, qu'ils soient ou non établis dans l'UE**[3]. La notion de « mise sur le marché » désigne la mise à disposition initiale, tandis que la « mise en service » correspond à la première utilisation par l'utilisateur final ou pour un usage interne dans l'UE.

En outre, des fournisseurs ou utilisateurs suisses sont également concernés si **le résultat fourni par leur système d'IA est utilisé dans l'UE**[4]. Autrement dit, même sans distribution directe à des clients UE, un acteur suisse entre dans le champ de l'AI Act si le résultat du système d'IA (prédictions, contenus, recommandations…) est effectivement destinée au marché européen. L'usage fortuit n'est toutefois pas suffisant.

Les articles de notre série « Comprendre le droit de l'IA » reviendront davantage sur le champ d'application, en particulier les exceptions, les catégories d'acteurs ainsi que les autres régulations sur les marchés suisse et européen.

Toutefois, **les acteurs suisses doivent prendre en compte les points suivants :**

- Depuis le 1er février 2025, il est strictement **interdit de fournir des systèmes d'IA présentant un niveau de risque prohibé dans l'UE.**

- Toute entité soumise à l'AI Act doit satisfaire à **l'obligation de la maîtrise de l'IA**, c'est-à-dire s'assurer que ses équipes disposent des compétences nécessaires pour évaluer tant les risques que les opportunités de l'IA.

- Depuis le 1er août 2025, les fournisseurs de modèles d'IA à usage général au sein de l'UE sont tenus de respecter des obligations spécifiques liées à la documentation et à la transparence de leurs modèles d'IA, avec des exigences renforcées pour certains modèles jugés à « haut risque », notamment du point de vue de la sécurité.

2. L'approche suisse en matière de réglementation de l'IA

En Suisse, le Conseil fédéral a récemment clarifié l'approche adoptée en matière de réglementation de l'IA. Trois objectifs principaux ont été identifiés pour la réglementation de l'IA en Suisse :

[3] Article 2, al. 1, let. a, EU AI Act.
[4] Article 2, al. 1, let. c, EU AI Act.

1. **renforcer la position du pays en tant que hub d'innovation** ;

2. **protéger les droits fondamentaux (y compris la liberté économique) ;**

3. **accroître la confiance du public dans l'IA.**

Premièrement, il a été décidé d'opter pour une **approche thématique et sectorielle** plutôt que d'adopter une loi horizontale complète sur l'IA, comme dans l'UE. Cette approche s'explique par le fait que le régime juridique suisse se fonde sur les principes généraux du droit, et adopte une vision générale et neutre d'un point de vue technologique. La réglementation de l'IA doit donc relever du cadre existant, variant selon l'usage de la technologie, plutôt que d'une réglementation unique. Néanmoins, cela ne signifie pas que les lois suisses ne devront pas être adaptées à l'IA, afin de soulever les nouvelles questions et défis juridiques qui sont soulevés par cette technologie.

Deuxièmement, le 27 mars 2025 le Conseil fédéral suisse a ratifié la **Convention sur l'IA du Conseil de l'Europe**[5], appelée Convention-cadre sur l'intelligence artificielle, les droits humains, la démocratie et l'État de droit[6] (la « **Convention IA** »). Cette Convention IA a une portée mondiale. À la date de rédaction de cet article, elle a été ratifiée par 15 signataires, dont les États-Unis. Elle vise à garantir que l'utilisation de l'IA respecte les normes juridiques internationales existantes en matière de droits humains, de la démocratie et de l'état de droit.

La Convention IA définit un **ensemble de principes** que les États doivent suivre dans leur traitement de l'IA. Les dispositions s'appliquent directement aux autorités publiques impliquées dans des activités liées à l'IA, tandis que pour les acteurs privés, cela dépend principalement de la manière dont les États décident d'intégrer les risques et impacts de l'IA dans leur droit existant. Les parties contractantes disposent d'une large latitude pour choisir les mesures législatives, administratives ou autres appropriées pour mettre en œuvre les dispositions.

Le droit suisse semble offrir un niveau de protection suffisant pour certaines dispositions de la Convention iA, telles que l'intégrité des processus démocratiques et le respect de l'État de droit[7], ainsi que l'exigence de consultation publique sur les questions importantes relatives à l'IA[8]. Cependant, quelques ajustements sont encore nécessaires concernant les principes de transparence et supervision[9], d'innovation sûre[10], de recours[11] et de garanties procédurales[12]. De plus, comme l'exige la Convention IA, **de nouvelles bases légales devraient être édictées** pour définir des normes relatives à la gestion des risques et impacts pour les systèmes d'IA[13] ainsi que pour mettre en place des mécanismes efficaces de supervision du respect des obligations de la Convention IA[14].

Toutefois, suivant l'avis d'experts juridiques[15] et de groupes d'intérêt[16], le Conseil fédéral a décidé de **privilégier, dans la mesure du possible, des mesures non contraignantes**. Le Conseil fédéral souhaite en effet que les mesures soient adaptées aux spécificités de chaque secteur. Seuls les droits fondamentaux, tels que la protection des données, doivent faire l'objet d'une réglementation transsectorielle.

Le Département fédéral de justice et police (DFJP), en collaboration avec le Département fédéral de l'environnement, des transports, de l'énergie et des communications (DETEC) et le Département fédéral

[5] https://www.news.admin.ch/en/nsb?id=104110.
[6] https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence.
[7] Article 5, Convention IA.
[8] Article 19, Convention IA.
[9] Article 8, Convention IA.
[10] Article 13, Convention IA.
[11] Article 14, Convention IA.
[12] Article 15, Convention IA.
[13] Article 16, Convention IA.
[14] Article 26, Convention IA.
[15] Comme recommandé dans un ensemble d'articles rédigés par des professeurs d'université et soutenus par la Fondation Mercator : https://www.itsl.uzh.ch/de/Forschung-und-Beratung/Forschungsprojekte/nachvollziehbare-algorithmen.html.
[16] https://www.economiesuisse.ch/fr/articles/comment-la-suisse-peut-devenir-un-site-cle-pour-lia

des affaires étrangères (DFAE), a été chargé de **rédiger un projet de loi incluant mesures légales et non contraignantes, à soumettre à consultation d'ici fin 2026**. Il n'est pas encore clair comment l'administration entend mettre en œuvre la convention sur l'IA.

D'un côté, **une mise en œuvre minimale nécessiterait des ajustements du cadre juridique actuel et l'introduction de nouvelles dispositions concernant la transparence et l'évaluation des risques et impacts**. Par exemple, il pourrait être exigé que les systèmes d'IA utilisés par l'État soient inscrits dans un registre public et que certains acteurs publics et privés soient tenus de réaliser une évaluation des risques et impacts avant d'utiliser un système d'IA. De plus, aucune nouvelle autorité ne serait créée pour superviser le respect de la convention sur l'IA, et les autorités de surveillance existantes assumeraient cette mission dans leur secteur respectif en plus de leurs activités de supervision actuelles.

D'un autre côté, **des mesures plus ambitieuses pourraient être adoptées**, comme imposer des obligations similaires aux acteurs publics et privés et créer de nouveaux droits et obligations en matière de non-discrimination, notamment pour les acteurs privés, auxquels les dispositions actuelles de la convention ne s'appliquent pas directement. Cela prendrait probablement la forme de mesures non contraignantes. De plus, le groupe d'acteurs privés soumis à l'évaluation des risques et impacts pourrait être défini plus largement, un niveau de détail plus élevé pourrait être requis et ces évaluations pourraient devoir être examinées par une autorité publique, augmentant ainsi le niveau de sécurité. Les autorités de surveillance existantes pourraient recevoir des pouvoirs étendus et un bureau de coordination pourrait être créé pour garantir une approche cohérente des questions intersectorielles.

Par ailleurs, **la Convention IA pourrait être mise en œuvre conformément à l'AI Act**, sous forme de réglementation complète des produits. Cela signifie qu'en plus d'ajuster le régime juridique suisse à la Convention IA, une réglementation axée sur les produits applicable aux acteurs publics et privés pourrait être adoptée, en ligne avec les différents niveaux de risque et exigences prévus par l'AI Act. Cela pourrait bénéficier aux fabricants suisses intégrant des composants IA dans leurs produits et leur permettre d'accéder au marché intérieur de l'UE avec moins d'obstacles. Néanmoins, cette approche réglementaire créerait une forte densité de réglementation de l'IA en Suisse, ce qui n'est pas souhaité par l'industrie. Néanmoins, compte tenu de la portée extraterritoriale de l'AI Act, les entreprises suisses pourraient déjà être soumises à ses exigences, et le législateur doit en tenir compte pour adapter le régime juridique suisse afin de faciliter la mise en conformité des entreprises suisses.

Enfin, **en ce qui concerne les produits industriels exportés vers l'UE**, le Conseil fédéral rappelle que 12 des 20 secteurs de produits listés dans l'annexe I de l'ARM CH-UE[17] (accord régissant le commerce des biens industriels entre l'UE et la Suisse) sont affectés par l'AI Act si les produits contiennent des systèmes d'IA[18]. Dans ce cas, les produits de ces 12 catégories, y compris les dispositifs médicaux et machines, seraient classifiés comme systèmes d'IA à haut risque selon l'AI Act s'ils sont soumis à une procédure d'évaluation de la conformité par un organisme tiers conformément à la législation européenne existante. **Aujourd'hui, les réglementations techniques suisses et européennes sont reconnues comme équivalentes. Cependant, ce ne sera plus le cas à partir d'août 2027**, lorsque les exigences de l'AI Act pour les systèmes à haut risque seront entrées en vigueur, s'appliquant aux produits de ces 12 secteurs. À partir de cette date, ces produits devront passer une évaluation de conformité supplémentaire réalisée par un organisme européen, et les entreprises suisses devront se conformer à ces exigences supplémentaires, entraînant travail et coûts accrus.

Compte tenu de ce qui précède, **l'extension de l'ARM CH-UE au secteur de l'IA aiderait à réduire les efforts et coûts liés à la commercialisation de systèmes d'IA suisses vers l'UE**. Par conséquent, le droit suisse devrait prévoir des obligations équivalentes à l'AI Act pour les aspects clés. De grandes incertitudes subsistent quant à la manière dont l'administration gérera cette situation, notamment si une extension du MRA au secteur de l'IA pourrait être prévue dans la version mise à jour du MRA CH-UE, qui devrait entrer en vigueur au plus tôt en 2028.

[17] https://www.seco.admin.ch/seco/en/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/Technische_Handelshemmnisse/Mutual_Recognition_Agreement_MRA0/MRA_Schweiz_EU.html.

[18] Rapport, section 7.2, p. 14 ; Rapport, section 9, p. 17.

L'approche suisse de la réglementation de l'IA reflète le caractère pragmatique national : **promouvoir l'innovation tout en protégeant les droits fondamentaux**. En adoptant une supervision mesurée plutôt que des restrictions lourdes, les autorités suisses visent **à renforcer la position de la Suisse comme hub d'innovation tout en instaurant la confiance du public dans les technologies IA**.

Cependant, il est important de noter que les acteurs suisses ne fonctionnent pas dans un vide réglementaire. Ces entités restent soumises à de nombreux cadres juridiques existants, notamment la Loi fédérale sur la protection des données (LPD), la Loi sur le droit d'auteur (LDA), ainsi qu'aux dispositions générales du droit civil et pénal suisse concernant la responsabilité, et aux réglementations sectorielles spécifiques.

Nous continuerons à suivre l'évolution du cadre réglementaire suisse dans les mois à venir.

3. COMMUNICATION FINMA 08/2024 SUR L'IA

En décembre 2024, la FINMA a publié une communication sur l'usage de l'IA dans les institutions financières[19] (« **Communication IA** »). Cette Communication IA représente la première mesure non légale sectorielle, régulant l'utilisation de l'IA par les institutions financières supervisées. Elle s'appuie sur ses directives existantes et sur sa supervision de la gestion des risques dans ces institutions, abordant des exigences spécifiques pour l'usage de l'IA.

La Communication IA ne fait pas de distinction entre les différentes technologies ou méthodes d'implémentation de l'IA. Elle **couvre l'intégralité de l'utilisation de l'IA dans ces institutions**, qu'il s'agisse d'applications propriétaires développées en interne, de systèmes personnalisés ou d'applications développées par des tiers, ou de systèmes d'IA tiers accessibles via API, services par abonnement, voire plateformes gratuites. Cette portée large assure une supervision cohérente, quel que soit le mode d'intégration de l'IA.

La Communication IA établit un ensemble structuré de mesures que les institutions financières doivent mettre en œuvre pour atténuer les risques liés au déploiement de l'IA. Les activités de supervision de la FINMA ont identifié plusieurs catégories de risques clés :

- vulnérabilités opérationnelles liées au manque de robustesse, précision, explicabilité ou biais inhérents aux systèmes d'IA ;
- expositions accrues en cybersécurité et informatique ;
- préoccupations en matière de protection des données.

La FINMA reconnaît également les défis émergents liés à la dépendance accrue aux tiers et aux conséquences légales et réputationnelles potentielles de l'implémentation de l'IA.

Pour répondre à ces risques, **la Communication IA recommande :**

1) **Gouvernance de l'IA :** mise en place d'un **cadre solide de gouvernance de l'IA définissant clairement les rôles et responsabilités** pour le développement, la mise en œuvre, le suivi et l'utilisation de l'IA, couvrant les solutions internes et externalisées. Selon une enquête récente de la FINMA[20], seulement la moitié des répondants utilisant l'IA ont développé une stratégie IA, montrant un potentiel d'amélioration important.

2) **Inventaire et classification des risques :** tenir un inventaire centralisé de toutes les applications IA, avec classification des risques et mesures d'atténuation documentées.

[19] https://www.eda.admin.ch/eda/en/fdfa/fdfa/aktuell/newsuebersicht/2023/europa.html ; Rapport, section 7.2, p. 14 ; Rapport, section 9, p. 17.
[20] https://www.finma.ch/en/news/2024/12/20241218-mm-finma-am-08-24/.

3) **Exigences de qualité des données :** établir des exigences explicites dans le cadre de gouvernance interne pour garantir **l'intégrité des données** (complétude, exactitude, cohérence) et protéger l'accès et la disponibilité. Ceci est crucial, car des données compromises entraînent des sorties IA biaisées ou peu fiables, notamment pour les systèmes exploitant directement les données institutionnelles (applications analytiques, systèmes RAG, agents conversationnels internes).

4) **Tests et surveillance continue** : la FINMA exige que les institutions financières mettent en place des protocoles de test programmés et une surveillance continue des applications IA. Cela inclut, par exemple, la validation statistique, les tests adversariaux, les audits de biais, le suivi des performances et la vérification de la qualité des données afin de garantir que les systèmes fonctionnent de manière fiable tout en permettant l'identification rapide des risques. Les institutions financières peuvent également demander un examen indépendant du processus de développement des modèles par du personnel qualifié afin de réduire les risques liés aux modèles.

5) **Documentation :** la FINMA exige que les institutions financières maintiennent une **documentation complète conformément au principe de transparence**. Les entités supervisées doivent **documenter l'objectif de l'application IA, la sélection et préparation des données, les critères de sélection du modèle d'IA sous-jacent, les métriques de performance, les hypothèses sous-jacentes, les limitations opérationnelles, les protocoles de test, les mécanismes de contrôle et les solutions de repli**. Lors des évaluations, la FINMA examinera si les institutions ont correctement documenté les sources de données et les procédures de vérification de qualité, comment elles assurent la robustesse, fiabilité et traçabilité de l'application, et si la catégorisation des risques est appropriée.

6) **Explicabilité :** la Communication IA impose aux institutions financières de **pouvoir expliquer les décisions générées par l'IA à tous les acteurs concernés, y compris investisseurs, clients, employés, FINMA et auditeurs externes**. Les entités supervisées doivent donc assurer une transparence suffisante dans leurs systèmes IA pour expliquer la logique et le processus derrière toute décision automatisée. Cette exigence établit une responsabilité en garantissant que les institutions financières peuvent clairement démontrer comment leurs applications IA produisent des résultats ou recommandations spécifiques.

4. LES EXIGENCES SUISSES EN MATIÈRE DE PROTECTION DES DONNÉES

Le Préposé Fédéral à la Protection des Données et à la Transparence (PFPDT) a confirmé que la Loi fédérale sur la protection des données (LPD), en vigueur depuis le 1er septembre 2023, s'applique directement aux systèmes IA traitant des données personnelles[21]. Les organisations déployant de l'IA doivent donc garantir la conformité aux principes suisses de protection des données en parallèle avec toute réglementation spécifique à l'IA.

Tous les principes de la LPD s'appliquent au traitement de données personnelles dans des systèmes d'IA : minimisation des données, limitation de la finalité, exactitude, durée de conservation limitée, sécurité. Les organisations doivent fournir des informations complètes sur la collecte de données personnelles, y compris les finalités, les durées de conservation et les destinataires des données. Par exemple, les entreprises déployant des systèmes IA doivent informer clairement les utilisateurs que leurs données sont traitées pour des finalités spécifiques (amélioration du service, personnalisation), préciser la durée de conservation et identifier tout fournisseur de services IA tiers impliqué.

[21] https://www.finma.ch/en/news/2025/04/20250424-mm-umfrage-ki/.

La LPD établit des **obligations spécifiques pour les décisions automatisées**[22]. Lorsque les systèmes IA produisent des décisions qui produisent un effet juridique sur les personnes concernées, les organisations doivent :

- notifier les individus sur les processus de décision automatisée ;
- permettre une intervention humaine pour révision de la décision ;
- permettre aux personnes concernées d'exprimer leur point de vue et de contester la décision.

Le consentement explicite est obligatoire pour le profilage à haut risque réalisé par des entités privées et pour tout profilage effectué par des autorités fédérales. Peuvent être considérés comme tels des systèmes d'IA pour *scoring* de crédit bancaire, le tri automatisé de candidatures, le calcul de primes d'assurance, ou encore l'analyse comportementale pour de la publicité ciblée.

La LPD exige également la réalisation **d'analyses d'impact sur la protection des données (AIPD)** pour tout traitement IA susceptible d'entraîner des risques élevés pour les droits et libertés des individus[23]. Cela concerne notamment le profilage à haut risque et le traitement à grande échelle de données sensibles. Les organisations doivent consulter le PFPDT lorsque des risques résiduels importants persistent après les mesures d'atténuation. Les AIPD sont typiquement nécessaires dans les cas suivants : systèmes de surveillance des employés à grande échelle, algorithmes de police prédictive, outils de diagnostic médical IA traitant des données de santé.

Les transferts internationaux de données personnelles nécessitent des niveaux de protection adéquats ou des garanties appropriées, telles que des clauses contractuelles types et des évaluations d'impact sur le transfert.

La LPD impose aux responsables du traitement et aux sous-traitants de mettre en œuvre des **mesures techniques et organisationnelles adaptées pour assurer la sécurité des données personnelles**[24]. Pour les systèmes IA, cela comprend :

- le chiffrement des données personnelles lors du traitement et du stockage ;
- les contrôles d'accès et mécanismes d'authentification ;
- des évaluations de sécurité régulières des modèles IA et infrastructures ;
- des protocoles sécurisés de transmission des données ;
- la protection contre l'accès, l'altération ou la destruction non autorisés.

Enfin, au-delà de la protection des données personnelles, les systèmes IA traitent souvent des informations commerciales confidentielles, nécessitant des mesures supplémentaires :

- **Protection des secrets commerciaux :** clauses contractuelles de confidentialité avec les fournisseurs IA et mesures techniques pour prévenir toute divulgation non autorisée ;
- **Secret professionnel :** conformité aux obligations sectorielles (juridique, médical, financier) ;
- **Informations commerciales confidentielles :** classification des données et contrôles d'accès pour les informations propriétaires ;
- **Garanties contractuelles :** inclure des dispositions de confidentialité et de protection des données dans les contrats de services IA ;
- **Isolement technique :** séparer, lorsque possible, le traitement des données confidentielles des autres opérations IA.

[22] https://www.edoeb.admin.ch/en/09112023-current-data-protection-legislation-is-directly-applicable-to-ai ; https://www.edoeb.admin.ch/en/update-current-legislation-directly-applicable-ai.
[23] Article 21, LPD (Loi fédérale sur la protection des données, RS 235.1).
[24] Article 22, LPD.

5. Conclusion

Le paysage réglementaire suisse sur l'IA requiert une **attention immédiate des dirigeants et des équipes juridiques**. Bien qu'une législation complète sur l'IA soit encore en développement, les lois existantes sur la protection des données, la guidance FINMA et la portée extraterritoriale de l'EU AI Act créent des obligations de conformité immédiates pour les organisations suisses.

La clé d'une gouvernance IA réussie réside dans la **compréhension des obligations réglementaires spécifiques selon le rôle de chaque acteur dans l'écosystème IA, et la mise en œuvre de cadres robustes adaptables aux exigences évolutives**. Les organisations qui anticipent ces obligations assureront non seulement la conformité, mais également un **avantage concurrentiel** dans une économie guidée par l'IA.

Le moment d'agir est maintenant. Évaluez vos applications IA, mettez en place les mesures de protection nécessaires et établissez des structures de gouvernance protégeant votre organisation et les individus dont vous traitez les données.

6. Checklist pratique

Applicabilité de l'AI Act :

- ✓ Mettez-vous des systèmes IA ou des modèles d'IA à usage général sur le marché de l'UE ?
- ✓ Mettez-vous des systèmes IA en service dans l'UE ?
- ✓ Les résultats de vos systèmes IA sont-ils destinés à être utilisées dans l'UE ?
- ✓ Vos produits contenant de l'IA relèvent-ils des 12 secteurs MRA affectés par l'AI Act ?
- ✓ Avez-vous identifié si vos systèmes IA sont prohibés, à haut risque ou à risque limité selon l'AI Act ?

Votre rôle dans le développement et le déploiement IA :

- ✓ Êtes-vous fournisseur (développement/fabrication de systèmes IA ou de modèles d'IA à usage général) ?
- ✓ Êtes-vous déployeur (utilisation de systèmes IA dans vos opérations) ?
- ✓ Utilisez-vous des services IA tiers (API, IA cloud) ?
- ✓ Opérez-vous dans le secteur financier soumis à la supervision FINMA ?
- ✓ Avez-vous classé toutes les applications IA par niveau de risque et cas d'usage ?

Obligations légales suisses :

- ✓ Avez-vous réalisé des DPIA pour les traitements à haut risque de données personnelles ?
- ✓ Fournissez-vous une information adéquate sur les décisions automatisées aux personnes concernées ?
- ✓ Avez-vous mis en place le droit à une intervention humaine sur les décisions IA ?
- ✓ Des mesures de sécurité adaptées sont-elles en place pour les données personnelles et confidentielles ?
- ✓ Avez-vous mis en place des garanties pour les transferts internationaux de données personnelles ?
- ✓ Respectez-vous les réglementations sectorielles (Communication IA FINMA pour les institutions financières) ?

Gouvernance interne IA :

- ✓ Avez-vous mis en place un cadre de gouvernance IA avec des rôles et responsabilités clairs ?
- ✓ Maintenez-vous un inventaire centralisé de toutes les applications IA avec classification des risques ?
- ✓ Les exigences de qualité des données pour les systèmes IA sont-elles définies et appliquées ?
- ✓ Avez-vous mis en œuvre des protocoles de test et une surveillance continue des applications IA ?
- ✓ Une documentation complète est-elle tenue pour tous les systèmes IA ?
- ✓ Disposez-vous de processus d'explicabilité pour les décisions générées par l'IA ?

Documentation externe et conformité :

- ✓ Avez-vous mis à jour les politiques de confidentialité pour couvrir les activités de traitement IA ?
- ✓ Des contrats appropriés sont-ils en place avec les fournisseurs IA, incluant des clauses de confidentialité ?
- ✓ Disposez-vous de clauses contractuelles types pour les transferts internationaux de données IA ?
- ✓ Avez-vous préparé des procédures de notification en cas de violation liée à l'IA ?
- ✓ La documentation technique est-elle prête pour inspections réglementaires ?
- ✓ Avez-vous mis en place des procédures pour répondre aux demandes des personnes concernées concernant le traitement IA ?

Restez informés : nous vous invitons à suivre notre série « Comprendre le droit de l'IA » et à vous abonner à notre newsletter.

Notre étude s'engage à fournir des solutions juridiques sur mesure pour votre organisation, notamment des services de conseil personnalisés, des formations spécialisées, des évaluations réglementaires et un accompagnement complet pour la rédaction de contrats et la révision de documents.

Pour discuter de vos besoins juridiques spécifiques, veuillez nous contacter directement par courriel ou par téléphone.

***

Vos Contacts

Florian Ducommun

Associé

Profile

fd@bonnard-lawson.com

+41 (0)21 348 11 88

Crystal Dubois

Collaboratrice Senior

Profile

cd@bonnard-lawson.com

+41 (0)21 348 11 88