ÉDITION SUISSE – GOUVERNANCE IA

POLITIQUE-CADRE d'utilisation responsable de l'intelligence artificielle

Pour [NOM JURIDIQUE COMPLET DE L'ÉTUDE]

POSITIONNEMENT

Un cadre de gouvernance orienté conformité, fondé sur le secret professionnel, la protection des données, la supervision humaine et la traçabilité. Son adoption ne constitue ni une certification ni une garantie absolue de conformité.

VERSION DE PUBLICATION

Version 1.1 · 11 novembre 2026

Droit et sources vérifiés au 11 novembre 2026

AVERTISSEMENT ESSENTIEL & STATUT DU DOCUMENT

AVERTISSEMENT DE PUBLICATION — À CONSERVER DANS LA VERSION PUBLIÉE

La présente politique-cadre fournit une structure de gouvernance pour l'usage responsable de l'IA dans la pratique juridique suisse. Elle doit être adaptée à [NOM JURIDIQUE COMPLET DE L'ÉTUDE], à ses mandats, outils, fournisseurs, contrats, configurations, cantons d'activité et activités internationales. Sa publication ou son adoption ne constitue ni un avis juridique, ni une certification, ni une garantie de conformité avec la LPD, le RGPD, le règlement de l'UE sur l'IA, DORA, les exigences FINMA ou toute autre règle. La conformité dépend des faits, des mesures opérationnelles et de leur preuve. Une validation par un conseil suisse qualifié est requise avant adoption ou publication, puis après toute modification importante du droit, des systèmes ou des activités.

Ce modèle AWSMTECH est destiné à être adapté, adopté et mis en œuvre par l'Étude. Avant publication, chaque champ entre crochets doit être remplacé, toute option non pertinente supprimée et le texte aligné sur les contrats, configurations, registres, analyses d'impact, procédures d'incident et formations effectivement en place. Les délais internes, paramètres de sécurité et listes d'outils approuvés doivent rester dans des documents opérationnels distincts, non publics.

Principes de lecture

- **« doit » / « interdit » :** exigence minimale du modèle, à rendre obligatoire dans la politique interne de l'étude.
- **« selon le droit applicable » :** la règle dépend notamment de la LPD, du RGPD, du droit professionnel, du droit cantonal, du droit du travail ou d'un régime sectoriel.
- « Étude » : [NOM JURIDIQUE COMPLET DE L'ÉTUDE], [FORME JURIDIQUE], ayant son siège à [NPA, LOCALITÉ, CANTON], qui adopte la présente politique et demeure soumise aux règles professionnelles et cantonales applicables.
- « Responsable IA » : [NOM OU FONCTION DU RESPONSABLE IA / COMITÉ IA], chargé de coordonner les approbations, le registre et les contrôles, sans décharger les associés et avocats de leurs propres devoirs.

SOMMAIRE

1. Objet, objectifs et portée 3
2. Définitions opérationnelles 3
3. Cadre juridique de référence 4
4. Responsabilités 4
5. Registre et approbation 5
6. Classification des usages 5
7. Usages permis et interdits 6
8. Secret professionnel 6
9. Client, instructions et consentement 7
10. Protection des données 7
11. Décisions automatisées 8
12. Analyse d'impact 8
13. Sous-traitants et contrats 9
14. Transferts à l'étranger 9
15. Sécurité et agents autonomes 10
16. Vérification et qualité 10
17. Propriété intellectuelle 11
18. Emploi et surveillance 11
19. LBA et activités financières 11
20. Incidents et violations 11
21. Conservation et traçabilité 12
22. Formation et contrôle 12
23. Règlement UE, DORA et FINMA 13
24. Entrée en vigueur 13
Annexe A. Lettre de mission 15
Annexe B. Approbation 15
Annexe C. Matrice d'incident 16
Annexe D. Références 16
Note de publication AWSMTECH 17

PARTIE I – FONDEMENTS & CHAMP D'APPLICATION

1. OBJET, OBJECTIFS & PORTÉE

La présente politique établit les règles minimales applicables à la sélection, à la configuration et à l'utilisation de systèmes d'intelligence artificielle dans la pratique du droit et l'administration d'une étude suisse. Elle poursuit cinq objectifs : protéger le secret professionnel et la confidentialité; préserver les droits des personnes; assurer la qualité du travail juridique; maintenir une responsabilité humaine identifiable; et démontrer, par des preuves vérifiables, une gouvernance proportionnée aux risques.

Elle s'applique aux associés, avocates et avocats, stagiaires, juristes, collaboratrices et collaborateurs, personnel administratif, temporaires, prestataires et toute autre personne utilisant un système d'IA pour le compte de l'Étude. Elle couvre les outils achetés séparément, les fonctions d'IA intégrées à des logiciels existants, les interfaces de programmation, les modèles locaux, les extensions de navigateur, les outils personnels et les agents capables d'exécuter des actions.

RÈGLE DE PRIORITÉ

En cas de conflit, la loi, le secret professionnel, les instructions du client, les ordres d'une autorité ou d'un tribunal, ainsi que les règles professionnelles et cantonales applicables prévalent sur cette politique.

2. DÉFINITIONS OPÉRATIONNELLES

Terme	Définition de travail
Système d'IA	Système fondé sur une machine qui, selon des objectifs explicites ou implicites, produit des prédictions, contenus, recommandations, décisions ou actions influençant un environnement physique ou virtuel.
IA générative	Système produisant notamment du texte, du code, des images, du son, de la vidéo, des résumés ou des analyses à partir d'instructions et de données d'entrée.
Outil approuvé	Système inscrit au registre de l'Étude, autorisé pour un ou plusieurs cas d'usage, classes de données, groupes d'utilisateurs et configurations déterminés.
Donnée protégée	Information couverte par le secret professionnel, une obligation de confidentialité, la protection des données, un secret d'affaires, une mesure de protection, une instruction client ou une restriction procédurale.
Donnée personnelle sensible	Catégorie visée par la LPD, notamment les données de santé, génétiques ou biométriques identifiantes, opinions religieuses, philosophiques, politiques ou syndicales, sphère intime ou origine raciale/ethnique, mesures d'aide sociale, poursuites ou sanctions administratives et pénales.
Décision individuelle automatisée	Décision reposant exclusivement sur un traitement automatisé et produisant des effets juridiques ou affectant la personne de manière significative, selon le test du droit applicable.
Incident IA	Événement portant ou susceptible de porter atteinte à la confidentialité, à la sécurité, aux droits, à la qualité juridique, à l'intégrité d'une procédure ou à une obligation contractuelle en lien avec l'IA.

3. CADRE JURIDIQUE DE RÉFÉRENCE

La gouvernance doit être déterminée au cas par cas. Au 11 novembre 2026, l'utilisation de l'IA en Suisse est notamment encadrée par le droit existant, y compris le droit professionnel, le droit pénal, la protection des données, le droit des contrats, le droit du travail, la propriété intellectuelle, la concurrence, la non-discrimination et les règles de procédure. Les travaux fédéraux relatifs à la Convention du Conseil de l'Europe sur l'IA doivent être suivis dans un registre juridique contrôlé.

- **Secret professionnel** : art. 321 du Code pénal suisse, art. 13 LLCA, règles cantonales et obligations contractuelles.
- **Protection des données** : LPD et OPDo; RGPD lorsqu'il s'applique au traitement concerné.
- **Travail** : art. 328b CO, art. 26 OLT 3, protection de la personnalité, proportionnalité et éventuels droits de participation.
- **Activités réglementées** : LBA lorsque les activités de l'Étude entrent dans son champ; exigences FINMA, OAR, DORA ou contractuelles uniquement si elles sont effectivement applicables.
- **Union Européenne** : règlement sur l'IA et autres règles de l'UE uniquement après une analyse documentée du rôle, du territoire, du système et du calendrier applicable.

PARTIE II – GOUVERNANCE & AUTORISATION

4. RESPONSABILITÉS & INDÉPENDANCE PROFESSIONNELLE

L'IA assiste; elle ne porte ni mandat, ni responsabilité professionnelle, ni pouvoir de décision final. La personne qui utilise, valide, communique ou dépose un résultat reste responsable de son travail et doit disposer de la compétence, du temps, de l'accès aux sources et de l'autorité nécessaires pour l'examiner.

Rôle	Responsabilités minimales
Organe dirigeant / associés	Adopter la politique, allouer les ressources, définir l'appétence au risque, désigner les responsables et approuver les exceptions à risque élevé.
Responsable IA / comité IA	Tenir le registre, coordonner les évaluations, vérifier les contrôles, surveiller les changements et organiser la formation.
Responsable protection des données	Conseiller sur la LPD/RGPD, les AIPD, les transferts, l'information des personnes et les incidents.
Associé responsable du mandat	Appliquer les instructions client, déterminer l'autorité contractuelle et professionnelle, valider les usages sensibles et la communication externe.
Sécurité / informatique	Configurer les accès, la journalisation, le chiffrement, la gestion des clés, les sauvegardes, l'intégration et la réponse technique.
Utilisatrice ou utilisateur	Employer uniquement les outils et cas d'usage autorisés, minimiser les données, vérifier les résultats et signaler tout incident ou fonctionnalité inconnue.

NON DÉLÉGATION

Un contrat fournisseur, une certification de sécurité, un hébergement en Suisse ou un avis automatisé ne remplace jamais l'analyse juridique et professionnelle de l'Étude.

5. REGISTRE DES SYSTÈMES D'IA & PROCÉDURE D'APPROBATION

Aucun système ne peut traiter des informations liées à un mandat avant son inscription au registre et l'autorisation du cas d'usage correspondant. L'approbation est limitée à la version, aux finalités, aux données, aux utilisateurs, aux intégrations et aux paramètres évalués.

5.1 Contenu minimal du registre

- fournisseur, produit, version ou famille de modèle, propriétaire interne et utilisateurs autorisés;
- finalité, cas d'usage, données d'entrée, sorties, personnes affectées et niveau de risque;
- rôle juridique de l'Étude et du fournisseur, lieux de traitement, sous-traitants et accès à distance;
- base contractuelle, évaluation du secret professionnel, justification de protection des données et restrictions client;
- rétention, entraînement, journalisation, sécurité, intégrations, clés, connecteurs et actions autonomes;
- AIPD ou autre analyse requise, tests, approbateur, date d'approbation, conditions, exceptions et date de réexamen;
- qualification au regard du règlement de l'UE sur l'IA, du RGPD, de la LBA, de FINMA ou de DORA, le cas échéant.

5.2 Déclencheurs de réévaluation

Une nouvelle évaluation est requise en cas de changement matériel de modèle, fournisseur, finalité, données, lieu de traitement, sous-traitant, conditions, politique d'entraînement, intégration, niveau d'autonomie, population affectée, incident, vulnérabilité ou droit applicable. L'absence de réponse du fournisseur bloque l'usage de données protégées.

6. CLASSIFICATION DES USAGES

Classe	Décision	Exemples / conditions
INTERDIRE	Arrêt immédiat; accès retiré.	Violation du secret; outil personnel non évalué; entraînement incontrôlé; action externe autonome non approuvée; usage discriminatoire ou trompeur.
SUSPENDRE	Aucune donnée protégée; examen rapide.	Fonction d'IA nouvellement activée, changement contractuel, sous-traitant inconnu, rétention ou localisation non confirmée.
AUTORISER SOUS CONDITIONS	Contrôles, périmètre et durée documentés.	Valeur démontrée, mais restrictions de données, revue renforcée, environnement isolé ou autorisation client nécessaires.
AUTORISER	Usage approuvé et surveillé.	Contrat, secret, sécurité, protection des données, tests et supervision humaine jugés adéquats pour le périmètre défini.

7. USAGES PERMIS, RESTREINTS & INTERDITS

7.1 Usages généralement admissibles - uniquement avec un outil approuvé

- dictée et transcription; première ébauche de textes; résumés; traduction; recherche assistée; extraction de clauses, dates ou entités; préparation de chronologies; automatisation administrative; formation sur données fictives;
- analyse de documents et préparation de dossiers lorsque les données, le contrat fournisseur et les contrôles de confidentialité correspondent exactement au périmètre approuvé;
- génération de code, scripts ou formules après revue de sécurité, tests et contrôle des licences.

7.2 Usages soumis à autorisation renforcée

- données couvertes par le secret professionnel ou données personnelles sensibles;
- recrutement, gestion du personnel, conflits, admission d'un client, évaluation de risque, fraude, LBA, sanctions ou accès à un service;
- agents capables d'envoyer, publier, conclure, payer, supprimer, déplacer, modifier des droits ou agir dans un système tiers;
- génération ou modification d'images, de voix ou de vidéos de personnes identifiables;
- usages susceptibles d'être classés à haut risque ou soumis à transparence par le règlement de l'UE sur l'IA.

7.3 Interdictions minimales

- introduire des données liées à un mandat dans un outil grand public, personnel ou non approuvé;
- contourner les paramètres de sécurité, les restrictions client, les contrôles d'accès ou la journalisation;
- laisser un système rendre seul un avis juridique, engager l'Étude, communiquer avec un client, une partie, un tribunal ou une autorité, ou accomplir un acte procédural;
- utiliser une citation, un fait, un calcul, une traduction déterminante ou une analyse sans vérification indépendante;
- dissimuler un usage d'IA lorsqu'une obligation d'information ou une instruction impose la transparence;
- procéder à une notation sociale, une manipulation interdite, une discrimination illicite, une surveillance générale, une inférence d'émotions ou un profilage de personnalité du personnel;
- fabriquer, altérer ou présenter comme authentique un élément de preuve, un enregistrement, une image, une signature, une voix ou une identité;
- utiliser l'IA pour déterminer seule l'identité, l'ayant droit économique, le classement LBA, la levée d'une alerte ou l'opportunité d'une communication.

PARTIE III – SECRET PROFESSIONNEL, CLIENTS & DONNÉES

8. SECRET PROFESSIONNEL & EXTERNALISATION

CONDITION PRÉALABLE IMPÉRATIVE

Aucune information protégée par le secret professionnel ne peut être rendue accessible à un fournisseur d'IA, hébergeur, support, opérateur de modèle ou sous-traitant avant une analyse écrite au regard de l'art. 321 CP, de l'art. 13 LLCA et des règles cantonales applicables.

L'analyse doit déterminer si l'accès est compatible avec le statut d'auxiliaire et les obligations de secret, ou si une autorisation spécifique du client est nécessaire. Elle couvre les personnes pouvant accéder au texte en clair, les accès de support, les opérateurs étrangers, les demandes d'autorités,

l'entraînement, l'évaluation humaine, les journaux, les embeddings, les caches, les sauvegardes et les suppressions.

Une convention de traitement, une clause de confidentialité, un abonnement entreprise, une certification ISO ou un centre de données suisse ne suffisent pas, à eux seuls. L'Étude doit pouvoir contrôler le périmètre, les accès, la chaîne de sous-traitance, les changements, la restitution et la suppression. Si le secret ne peut être préservé avec un degré de confiance documenté, l'usage est interdit.

8.1 Règles de minimisation

- n'utiliser que les extraits strictement nécessaires; préférer les environnements isolés et les traitements locaux approuvés;
- retirer les identifiants et détails contextuels lorsqu'ils ne sont pas nécessaires; vérifier qu'une réidentification raisonnable n'est pas possible;
- traiter les données pseudonymisées comme des données personnelles; une simple suppression du nom ne constitue pas une anonymisation;
- ne pas importer l'intégralité d'un dossier lorsque la finalité peut être atteinte avec un corpus réduit.

9. AUTORITÉ DU CLIENT, INSTRUCTIONS & CONSENTEMENT

Avant tout usage touchant un mandat, l'associé responsable distingue et documente quatre questions indépendantes :

1. la justification du traitement au regard de la LPD, du RGPD ou d'un autre régime;
2. l'autorité contractuelle donnée par la lettre de mission et les instructions du client;
3. la licéité de l'accès d'un prestataire à une information couverte par le secret professionnel;
4. les restrictions propres au client concernant les outils, fournisseurs, pays, types de données ou usages.

Le consentement n'est pas une base universelle et ne corrige pas un dispositif disproportionné, insuffisamment sécurisé ou incompatible avec le secret professionnel. Lorsqu'il est utilisé, il doit être valable pour la finalité concernée, suffisamment informé et documenté; les conséquences d'un retrait doivent être gérées conformément au droit et aux obligations professionnelles.

9.1 Information et choix du client

L'Étude informe le client lorsque la nature, l'importance, les instructions, le contrat, le droit applicable ou les attentes légitimes le requièrent. L'information porte de manière proportionnée sur la catégorie d'usage, les données concernées, les garanties, la supervision humaine, les limites et les possibilités de restriction. Une opposition est enregistrée au niveau du dossier et techniquement répercutée.

9.2 Honoraires et transparence

L'IA ne justifie ni une facturation fictive ni l'attribution à une personne d'un travail qu'elle n'a pas accompli. L'Étude applique ses règles d'honoraires, les accords du mandat et les exigences professionnelles, et décrit l'assistance d'IA lorsqu'elle est matériellement pertinente pour la facturation ou demandée par le client.

10. PROTECTION DES DONNÉES DÈS LA CONCEPTION

Tout usage d'IA traitant des données personnelles respecte la licéité, la bonne foi, la transparence, la proportionnalité, la finalité, l'exactitude, la sécurité, la protection des données dès la conception et par défaut, ainsi que les obligations d'information et de documentation du régime applicable.

10.1 Information des personnes

L'information décrit de façon intelligible le responsable du traitement, les finalités, les catégories de destinataires et, lorsque cela est requis, les transferts à l'étranger. Pour un traitement fondé sur l'IA, l'Étude documente et communique, au niveau approprié, la finalité, le fonctionnement pertinent, les principales sources de données, les réutilisations et les voies permettant d'exercer les droits. Les demandes relatives à la protection des données et à l'exercice des droits sont adressées à [CONTACT PUBLIC — E-MAIL, URL OU ADRESSE POSTALE].

10.2 Droits

Les personnes peuvent exercer les droits que leur confère le droit applicable au traitement concerné. Selon les circonstances, ceux-ci peuvent inclure l'accès, la rectification, l'effacement ou la destruction, la remise ou la transmission des données, l'opposition, la limitation et l'examen humain d'une décision individuelle automatisée. Leur étendue, leurs conditions et leurs exceptions ne sont pas identiques sous la LPD, le RGPD et les autres régimes.

10.3 Données exactes et biais

Les données d'entrée et les résultats utilisés pour une personne, une décision ou un conseil sont évalués quant à leur pertinence, exactitude, représentativité, actualité et risque de biais. Les erreurs signalées sont corrigées à la source lorsque cela est possible; les limites connues sont communiquées aux personnes qui s'appuient sur le système.

11. DÉCISIONS INDIVIDUELLES AUTOMATISÉES

Avant tout cas d'usage susceptible d'influencer l'admission d'un client, un conflit, un recrutement, l'emploi, la fraude, un service, un accès, une tarification ou une mesure défavorable, le responsable du cas d'usage établit :

- s'il existe une décision concernant une personne et non une simple analyse préparatoire;
- si la décision repose exclusivement sur un traitement automatisé;
- si elle produit des effets juridiques ou affecte significativement la personne;
- quelle information doit être fournie et à quel moment;
- si la personne peut exprimer son point de vue et obtenir l'examen de la décision par une personne physique;
- si une exception légale existe et si ses conditions sont remplies;
- si le RGPD ou le règlement de l'UE sur l'IA ajoute des obligations.

PRINCIPE INTERNE

Sauf obligation légale contraire dûment documentée, l'Étude ne confie pas à l'IA une décision finale défavorable concernant une personne. La revue humaine doit être réelle : le réviseur doit comprendre les facteurs pertinents, pouvoir contester le résultat et disposer de l'autorité nécessaire pour le modifier.

12. ANALYSE D'IMPACT & GESTION DES RISQUES ÉLEVÉS

Une évaluation préliminaire est réalisée dès la planification. Une analyse d'impact relative à la protection des données (AIPD) est menée lorsqu'un traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux, notamment selon la nature, l'étendue, les circonstances, la finalité, l'usage de nouvelles technologies, le profilage, les décisions automatisées, le traitement à grande échelle de données sensibles ou la surveillance systématique.

12.1 Procédure obligatoire

1. décrire le système, la finalité, les données, les flux, les personnes, les fournisseurs et les alternatives moins intrusives;
2. noter séparément la probabilité et la gravité des risques, y compris le secret professionnel, les droits fondamentaux, la discrimination et l'accès étranger;
3. définir les mesures techniques, organisationnelles, contractuelles et humaines;
4. évaluer le risque résiduel et obtenir l'approbation du responsable du traitement et des fonctions compétentes;
5. si un risque résiduel élevé demeure, consulter le PFPDT ou, lorsque les conditions légales sont réunies, le conseiller à la protection des données;
6. réexaminer l'analyse après tout changement matériel ou incident.

L'avis du PFPDT ou du conseiller ne doit pas être présenté comme une certification du système. Un usage contraire aux principes de la protection des données, au secret professionnel ou à une autre règle demeure interdit, même si une AIPD a été réalisée.

PARTIE IV – FOURNISSEURS, TRANSFERTS & SÉCURITÉ

13. SOUS-TRAITANTS, CONTRATS & DILIGENCE FOURNISSEUR

Avant l'approbation, l'Étude vérifie la capacité juridique, technique et organisationnelle du fournisseur. Lorsque celui-ci agit comme sous-traitant, le contrat doit satisfaire aux exigences de l'art. 9 LPD et, si applicable, de l'art. 28 RGPD, sans se contenter de l'étiquette « DPA ».

13.1 Clauses et preuves minimales

- traitement uniquement sur instruction et pour les finalités autorisées; aucune utilisation propre non approuvée;
- confidentialité et secret des personnes autorisées à accéder aux données; mesures de sécurité vérifiables;
- interdiction ou encadrement exprès de l'entraînement, du réglage, de l'évaluation humaine, de l'apprentissage par retour et de la création d'embeddings;
- liste, lieux, fonctions et mécanisme de contrôle des sous-traitants; information préalable des changements;
- rétention, effacement, restitution, sauvegardes, journaux, demandes d'autorités et fin du contrat;
- assistance pour les droits, AIPD, incidents, enquêtes, audits, litiges et obligations professionnelles;
- notification sans délai contractuel incompatible avec les obligations de l'Étude; coopération et conservation des preuves;
- droits d'audit ou assurance indépendante proportionnée; gestion des vulnérabilités, continuité, réversibilité et sortie;
- droits sur les données, les sorties, les configurations et les contenus; mécanisme de contestation;
- obligation d'alerter l'Étude si une instruction paraît contraire au droit.

13.2 Diligence continue

L'Étude surveille les conditions, avis de sécurité, changements de modèle, sous-traitants, incidents connus, performances, biais, certifications et capacités de suppression. Les déclarations marketing sont corroborées par des documents, tests ou garanties contractuelles proportionnés.

14. COMMUNICATIONS DE DONNÉES À L'ÉTRANGER

L'Étude cartographie le lieu réel du traitement et de l'accès : centre de données, support, supervision humaine, télémétrie, journaux, détection d'abus, embeddings, caches, sauvegardes, reprise après sinistre et sous-traitants. Une région d'hébergement annoncée ne prouve pas, à elle seule, l'absence d'accès depuis l'étranger.

- vérifier si l'État destinataire figure dans la liste suisse des États assurant un niveau de protection adéquat;
- à défaut, documenter une garantie reconnue, notamment des clauses contractuelles appropriées, et les mesures complémentaires nécessaires;
- effectuer une analyse du transfert lorsque le droit ou le risque l'exige, y compris l'accès d'autorités et les voies de recours;
- privilégier le chiffrement avec maîtrise adéquate des clés, la minimisation, la pseudonymisation et la séparation des données;
- encadrer les transferts ultérieurs; suspendre ou mettre fin au traitement si la protection ne peut être maintenue;
- utiliser les dérogations légales de manière exceptionnelle, étroite et documentée.

> **DOUBLE CONTRÔLE**
>
> Une communication à l'étranger peut être compatible avec la LPD tout en restant incompatible avec le secret professionnel ou les instructions du client. Les deux analyses sont obligatoires.

15. SÉCURITÉ TECHNIQUE & AGENTS AUTONOMES

Les mesures sont proportionnées à la sensibilité, au volume, à la durée, au contexte et à l'autonomie du système. Elles couvrent au minimum l'identité, les accès, le chiffrement, les secrets, les journaux, la segmentation, les sauvegardes, la continuité, la suppression, les vulnérabilités, les environnements de test et les intégrations.

15.1 Exigences particulières pour les agents

- privilège minimal, identités techniques séparées, droits temporaires et périmètre de données limité;
- environnement isolé, liste d'actions autorisées, plafonds, validation humaine avant toute action externe ou irréversible;
- protection contre l'injection d'instructions, les contenus non fiables, l'exfiltration, l'escalade de privilèges et les boucles d'action;
- journal complet des instructions, outils appelés, données consultées, actions, erreurs et validations;
- tests adverses, scénarios d'échec, mécanisme d'arrêt, révocation immédiate des accès, retour arrière et procédure de reprise;
- interdiction par défaut d'envoyer un message, déposer un acte, engager une dépense, signer, conclure, publier, modifier des droits ou supprimer des données sans approbation humaine explicite.

PARTIE V – QUALITÉ JURIDIQUE & USAGES SPÉCIAUX

16. SUPERVISION HUMAINE, VÉRIFICATION & QUALITÉ

L'intensité du contrôle augmente avec le risque. La revue ne consiste pas à relire passivement un texte plausible : elle doit permettre de reconstruire le raisonnement, de vérifier les sources primaires et de détecter omissions, biais, informations obsolètes, erreurs de compétence, conflits et hallucinations.

16.1 Exigences pour le travail juridique

- vérifier chaque autorité, citation, date, compétence, disposition, calcul et fait matériel dans une source fiable et actuelle;
- contrôler les traductions déterminantes et la terminologie de la juridiction concernée;
- examiner la stratégie, les exceptions, les délais, les conflits, les risques et les conséquences pour le client;
- ne jamais déposer ou transmettre une production d'IA sans validation d'un professionnel qualifié;
- documenter la revue lorsque le risque, le mandat, la procédure ou l'assurance qualité le requiert;
- corriger les sources et modèles internes lorsqu'une erreur récurrente est identifiée.

16.2 Tribunaux, autorités et preuve

L'Étude respecte les règles de procédure, les ordres du tribunal et les devoirs de loyauté. Aucun contenu généré ou modifié ne doit être présenté comme un document authentique ou une preuve d'origine humaine. La provenance, les métadonnées et la chaîne de conservation sont préservées lorsque l'authenticité est pertinente.

17. PROPRIÉTÉ INTELLECTUELLE, PERSONNALITÉ & CONTENUS SYNTHÉTIQUES

- vérifier les licences des données d'entrée, modèles, bases, sorties, images, code et contenus de tiers;
- ne pas demander de reproduire un contenu protégé au-delà de ce que le droit et les licences permettent;
- examiner les risques de similitude substantielle, marque, concurrence déloyale, secret d'affaires et droit de la personnalité;
- indiquer clairement les images, voix ou vidéos synthétiques lorsque le droit, le contexte ou le risque de tromperie l'exige;
- obtenir les autorisations nécessaires avant d'utiliser l'image, la voix ou l'identité d'une personne;
- conserver les informations de provenance utiles et ne pas supprimer les marquages ou métadonnées obligatoires.

18. EMPLOI, SURVEILLANCE & RESSOURCES HUMAINES

Les traitements concernant le personnel respectent l'art. 328b CO, l'art. 26 OLT 3, la protection de la personnalité, la nécessité, la proportionnalité, la transparence, la sécurité et les droits de participation ou de consultation applicables. Un rapport de subordination augmente le risque et limite la portée d'un consentement prétendument libre.

INTERDICTION PAR DÉFAUT

Sont interdits : notation automatisée de performance, inférence d'émotions ou de sentiments, profilage de personnalité à partir des communications, surveillance continue de productivité, classement opaque et recommandation automatisée de mesure disciplinaire ou de licenciement. Une exception ne peut être envisagée qu'après une analyse écrite de droit du travail, de protection des données et de non-discrimination, avec mesures strictes et décision humaine.

19. LBA, SANCTIONS & ACTIVITÉS FINANCIÈRES

Lorsque l'Étude exerce une activité entrant dans le champ de la LBA ou est soumise à un règlement d'OAR, elle documente les obligations applicables et la répartition des responsabilités. L'IA peut assister la collecte, la comparaison et le tri, mais une personne qualifiée vérifie les sources, résout les correspondances contradictoires et conserve la motivation.

- aucune détermination autonome de l'identité du cocontractant ou de l'ayant droit économique;
- aucune validation autonome d'un contrôle sanctions ou PEP, d'une classification de risque ou d'une alerte;
- aucune décision autonome de communiquer ou de ne pas communiquer un soupçon;
- aucune destruction automatisée de preuve ou de dossier soumis à conservation;
- tests documentés de faux positifs, faux négatifs, biais et actualité des listes.

PARTIE VI · INCIDENTS, PREUVES & RÉGIMES CONDITIONNELS

20. INCIDENTS IA & VIOLATIONS DE LA SÉCURITÉ DES DONNÉES

Toute personne signale immédiatement, par [CANAL INTERNE DE SIGNALEMENT DES INCIDENTS IA], tout envoi non autorisé, toute sortie erronée ayant un impact matériel, toute fuite, tout accès indu, toute action autonome, tout comportement discriminatoire, toute compromission, tout changement préoccupant concernant un fournisseur ou toute violation de la présente politique. La crainte d'une sanction ne doit retarder aucun signalement effectué de bonne foi.

20.1 Réponse coordonnée

1. **Contenir** : arrêter ou isoler le système, révoquer les accès et empêcher la propagation de l'incident;
2. **Préserver** : conserver, de manière proportionnée, les journaux, les instructions (prompts), les sorties, les versions, les décisions et les preuves;
3. **Qualifier** : déterminer les données, les secrets, les personnes, les mandats, les fournisseurs, les pays et les actions concernés, ainsi que les conséquences de l'incident;
4. **Corriger** : procéder à la suppression ou à la sécurisation, demander l'effacement au fournisseur, rectifier les résultats et protéger les procédures;
5. **Décider** : statuer sur les notifications, l'information, les mesures concernant les clients, le tribunal, l'assureur, les autorités et le personnel, ainsi que sur la communication;
6. **Apprendre** : analyser les causes, définir les actions correctives et mettre à jour le registre, les tests, les AIPD, les contrats et la formation.

20.2 Notifications

Sous le régime de la LPD, l'Étude annonce au PFPDT, dans les meilleurs délais, toute violation de la sécurité des données vraisemblablement susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux. Elle informe la personne concernée lorsque cette information est nécessaire à sa protection ou que le PFPDT le demande, sous réserve des limites légales. La LPD ne prévoit pas de délai général de 72 heures en Suisse.

Le délai de 72 heures prévu par le RGPD ne s'applique que lorsque l'art. 33 RGPD régit la violation concernée. L'Étude se prononce séparément sur l'information du client, des personnes, des tribunaux, des autorités, des organes professionnels, des assureurs et des partenaires contractuels. Elle veille à préserver le secret professionnel et documente également toute décision de ne pas notifier.

21. CONSERVATION, TRAÇABILITÉ & DOSSIER DU MANDAT

L'Étude détermine, pour chaque catégorie d'usage, si les instructions, les sorties, les validations, les journaux ou les évaluations doivent être versés au dossier du mandat. La conservation repose sur la finalité, les obligations de preuve, les instructions, les litiges prévisibles, le secret et la protection des données. Aucune règle unique n'impose de conserver chaque prompt ni de tout supprimer automatiquement.

- conserver la version du système ainsi que les sources nécessaires à la compréhension d'un résultat matériel;
- éviter toute duplication non nécessaire de données protégées dans les journaux ou les historiques;
- appliquer des durées de conservation et des blocages de suppression documentés;
- préserver la confidentialité, les droits d'accès ainsi que la chaîne de conservation;
- prévoir la restitution, l'exportation et la suppression vérifiable des données lors de la fin de l'utilisation d'un outil.

22. FORMATION, CONTRÔLE & AMÉLIORATION CONTINUE

L'accès aux systèmes d'IA est subordonné à une formation adaptée au rôle, au risque et aux fonctions disponibles. L'Étude vérifie périodiquement la compréhension et l'efficacité des contrôles, plutôt que de se fonder sur une simple attestation de présence.

- formation initiale avant tout accès aux données protégées; actualisation de la formation après tout changement matériel;
- exercices pratiques portant sur le secret, la minimisation, les hallucinations, les biais, les incidents et les agents;
- tests de qualité et de sécurité reposant sur des scénarios représentatifs;
- contrôles de l'usage proportionnés, respectueux du droit du travail et ne s'apparentant pas à une surveillance comportementale générale;
- voie d'escalade accessible et protection des signalements effectués de bonne foi;
- révision de la politique au moins une fois par an, ainsi qu'en cas d'incident ou de changement du droit, de fournisseur ou de système.

23. RÈGLEMENT DE L'UE SUR L'IA, DORA & EXIGENCES FINMA

23.1 Règlement de l'UE sur l'IA

L'Étude n'affirme pas être soumise ou conforme au règlement de l'UE sur l'IA sans analyse. Le registre identifie le rôle éventuel de fournisseur, déployeur, importateur ou distributeur; le lieu d'établissement; le marché et les personnes affectées; la portée territoriale; les pratiques interdites; la littératie en IA; les obligations de transparence; la classification à haut risque; les responsabilités relatives aux modèles d'IA à usage général; et les dates d'application, y compris les modifications et mesures transitoires.

Les dates d'application ne sont pas figées dans les engagements publics de l'Étude. Elles sont tenues dans un registre juridique contrôlé et vérifiées avant tout lancement ou changement matériel.

23.2 DORA et FINMA

DORA vise principalement les entités financières de l'Union européenne et leur gestion des risques liés aux TIC. Les exigences FINMA s'appliquent aux destinataires et activités qu'elles désignent. Une étude d'avocats n'est pas automatiquement soumise à ces régimes du seul fait qu'elle conseille un client financier.

Une couche de contrôle spécifique est toutefois activée lorsque l'Étude est elle-même réglementée, fournit un service qualifié d'externalisation ou de service TIC, s'engage contractuellement envers une entité réglementée, ou traite un mandat dont les exigences sont répercutées. Elle couvre alors la classification du service, la chaîne de sous-traitance, les droits d'audit et d'accès, la localisation, les incidents, la continuité, les tests, la sortie et les informations exigées par le client ou l'autorité.

24. ENTRÉE EN VIGUEUR, EXCEPTIONS & RÉVISION

Toute exception doit être formulée par écrit, limitée, proportionnée, assortie de mesures compensatoires, approuvée par les fonctions compétentes et inscrite au registre. Aucune exception ne peut autoriser une violation du secret professionnel, d'une loi, d'une décision d'autorité ou d'une instruction contraignante du client.

L'Étude adopte une version datée de la politique, en désigne le propriétaire, conserve l'historique des modifications et communique les règles pertinentes aux personnes concernées. La politique est révisée au moins une fois par an et sans délai inutile après tout changement matériel du droit, de fournisseur, de système, de risque ou d'organisation.

24.1 Fiche d'adoption et contacts — à compléter avant publication

Champ à compléter	Valeur propre à l'Étude
Nom juridique complet et forme	[NOM JURIDIQUE COMPLET DE L'ÉTUDE] — [FORME JURIDIQUE]
Siège et coordonnées	[ADRESSE] — [NPA, LOCALITÉ, CANTON, SUISSE]
Périmètre professionnel	[CANTON(S), ORDRE(S) OU AUTORITÉ(S) PROFESSIONNELLE(S)]
Organe d'approbation	[ASSOCIÉS / CONSEIL D'ADMINISTRATION / AUTRE ORGANE]
Propriétaire de la politique	[NOM ET FONCTION]
Responsable IA / comité IA	[NOM, FONCTION ET CONTACT INTERNE]

Champ à compléter	Valeur propre à l'Étude
Contact protection des données	[NOM OU FONCTION — E-MAIL — URL OU ADRESSE POSTALE]
Signalement des incidents IA	[E-MAIL / TÉLÉPHONE / PORTAIL INTERNE]
Cycle documentaire	Version [X.Y] — adoptée le [JJ MOIS AAAA] — en vigueur le [JJ MOIS AAAA] — prochaine révision au plus tard le [JJ MOIS AAAA]

Instruction de finalisation : remplacer tous les champs entre crochets, supprimer les variantes inutiles et s'assurer qu'aucun espace réservé ne subsiste dans la version publiée.

ANNEXES – OUTILS D'ADOPTION

ANNEXE A - CLAUSE DE LETTRE DE MISSION (MODÈLE À ADAPTER)

USAGE PRUDENT

La présente clause ne constitue ni un consentement universel ni une autorisation de divulguer des informations couvertes par le secret professionnel. Elle doit être adaptée au mandat, aux outils utilisés et aux règles professionnelles applicables.

« L'Étude peut recourir à des outils d'intelligence artificielle approuvés pour l'assister dans certaines tâches, notamment la recherche, l'analyse, la synthèse, la traduction ou la préparation de projets. Ces outils n'exercent aucun mandat et leurs résultats sont soumis à un contrôle humain adapté au risque. L'Étude demeure responsable de ses prestations.

Avant de traiter des informations relatives au mandat, l'Étude évalue les aspects liés au secret professionnel, à la protection des données et à la sécurité, ainsi que les fournisseurs et sous-traitants, les lieux de traitement et les conditions d'utilisation. Elle limite les données à ce qui est nécessaire et n'autorise pas l'utilisation d'informations protégées pour entraîner des modèles partagés, sauf si une base juridique, une autorisation et des garanties spécifiques sont documentées.

Lorsque le droit, la nature du mandat ou vos instructions l'exigent, l'Étude vous informe de l'usage envisagé et recueille les instructions ou autorisations nécessaires. Vous pouvez lui communiquer des restrictions particulières; l'Étude vous indiquera si celles-ci ont une incidence sur les modalités, les délais ou le coût d'exécution du mandat. »

ANNEXE B - DÉCISION D'APPROBATION D'UN SYSTÈME D'IA

Domaine	Questions de décision
Cas d'usage	Finalité précise? Bénéfice attendu? Solution moins intrusive? Utilisateurs? Personnes concernées? Action autonome?
Secret professionnel	Accès possible au texte en clair? Statut d'auxiliaire? Personnel et assistance technique? Droit étranger? Autorisation du client? Règles cantonales?
Données	Catégories de données, sensibilité, volume, minimisation, pseudonymisation, conservation, droits des personnes, décision automatisée et AIPD?
Fournisseur	Traitement uniquement sur instruction? Entraînement? Sous-traitants? Audit? Incidents? Suppression? Réversibilité? Stabilité financière?
Transferts	Pays concernés, accès à distance, adéquation de la protection, clauses, analyse du transfert, chiffrement et gestion des clés, transferts ultérieurs?
Sécurité	Identités, authentification multifacteur (MFA), rôles, segmentation, journaux, secrets, intégrations, vulnérabilités, sauvegardes, arrêt et retour arrière?
Qualité	Sources, tests, taux d'erreur, biais, limites, contrôle humain, documentation et critères de suspension?
Régimes	LPD, RGPD, règlement de l'UE sur l'IA, LBA/OAR, FINMA, DORA, contrats clients, règles de procédure et propriété intellectuelle?

Domaine	Questions de décision
Décision	Interdire / suspendre / autoriser sous conditions / autoriser; personne chargée de l'approbation, date, limites, exceptions, preuve et réexamen.

ANNEXE C – MATRICE DE DÉCISION EN CAS D'INCIDENT

Question	Décision à documenter
Secret professionnel	Mandat concerné, informations en cause, destinataire, récupération ou suppression, client, tribunal ou autorité à informer, mesures de protection.
LPD	Violation de la sécurité des données? Risque vraisemblablement élevé? Annonce au PFPDT dans les meilleurs délais? Information des personnes nécessaire à leur protection ou demandée par le PFPDT?
RGPD	RGPD applicable? Risque pour les droits et libertés? Notification à l'autorité dans les 72 heures si l'art. 33 est applicable? Information des personnes en cas de risque élevé, sous réserve des exceptions?
Contrats / secteurs	Délais et destinataires prévus par les contrats; assureur; OAR; exigences FINMA/DORA ou du client réglementé; conservation des preuves.
Qualité / procédure	Un résultat erroné a-t-il été utilisé? Correction, retrait, information, délai de procédure, déclaration au tribunal et préservation de la preuve.
Remédiation	Cause, portée, blocage, mesures correctives, tests, mise à jour de l'AIPD, du registre, du contrat et de la formation, et décision de remise en service.

ANNEXE D – RÉFÉRENCES OFFICIELLES PRINCIPALES

Sélection non exhaustive. Les textes consolidés, les règles cantonales et les obligations propres à chaque mandat doivent être vérifiés au moment de l'usage. Liens consultés ou vérifiés pour cette édition le 11 novembre 2026.

Source	Lien officiel
Loi fédérale sur la protection des données (LPD), RS 235.1	Ouvrir la source
Ordonnance sur la protection des données (OPDo), RS 235.11	Ouvrir la source
PFPDT – IA et protection des données	Ouvrir la source
PFPDT – Aide-mémoire AIPD, art. 22 et 23 LPD	Ouvrir la source
Code pénal suisse, art. 321, RS 311.0	Ouvrir la source
Loi sur la libre circulation des avocats (LLCA), art. 13, RS 935.61	Ouvrir la source
Code des obligations, notamment art. 328b, RS 220	Ouvrir la source
Ordonnance 3 relative à la loi sur le travail, art. 26, RS 822.113	Ouvrir la source
FINMA – Organismes d'autorégulation et obligations LBA	Ouvrir la source

Source	Lien officiel
Office fédéral de la justice - Intelligence artificielle	Ouvrir la source
Règlement (UE) 2024/1689 sur l'intelligence artificielle, texte officiel	Ouvrir la source
Règlement (UE) 2026/1744 modifiant le règlement sur l'IA	Ouvrir la source
Règlement (UE) 2016/679 (RGPD)	Ouvrir la source
Règlement (UE) 2022/2554 (DORA)	Ouvrir la source

NOTE DE PUBLICATION AWSMTECH

AVERTISSEMENT FINAL DE PUBLICATION

La présente politique-cadre ne peut servir de base à une publication qu'après le remplacement intégral des champs entre crochets et la validation de son adéquation aux faits propres à l'Étude. Elle ne constitue ni un avis juridique, ni une certification, ni une garantie de conformité. Son adoption ne dispense pas [NOM JURIDIQUE COMPLET DE L'ÉTUDE] de vérifier et de démontrer, pour chaque usage, la licéité, le respect du secret professionnel, la sécurité, les contrats, les paramètres, la supervision humaine et les règles cantonales ou sectorielles applicables. **Une revue par un conseil suisse qualifié est requise avant toute publication et lors de toute modification importante.**

Pour une adoption par une étude, AWSMTECH recommande de conserver séparément : le registre des systèmes d'IA; la liste des outils et cas d'usage approuvés; les analyses de secret professionnel; les AIPD et analyses de transfert; les évaluations fournisseur; les configurations techniques; les tests; les exceptions; les formations; et le dossier des incidents.

Technologie responsable. Pratique juridique maîtrisée.

Politique-cadre FR-CH | Version 1.1 | 11 novembre 2026