Attribuer une responsabilité ne garantit pas les moyens de l'exercer

Forward Deployed Engineers et continuité réglementaire : lire les offres, les conditions et le droit avant de présumer

Plusieurs grands acteurs ont fortement investi, au printemps et à l'été 2026, dans le déploiement embarqué de l'IA en entreprise : AWS a annoncé un investissement d'un milliard de dollars dans une organisation de *Forward Deployed Engineering*, Microsoft a lancé Frontier Company, activité opérationnelle de quelque 6 000 experts adossée à un engagement de 2,5 milliards, et OpenAI a constitué une société de déploiement financée à plus de 4 milliards par des investisseurs tiers. Les trois montants ne mesurent pas la même chose ; ils indiquent une direction, pas une norme de marché. Le modèle est connu : les ingénieurs du fournisseur construisent dans l'environnement du client, livrent en quelques semaines, puis repartent. Reste l'après. Qui tient alors les obligations réglementaires attachées au système, et avec quels moyens ?

La thèse est étroite. Un contrat FDE peut attribuer clairement au client des responsabilités d'exploitation et de conformité sans décrire, dans le même document, les informations, accès et assistance utiles à leur exercice. *La répartition des obligations et la remise des moyens se vérifient donc séparément, système par système*, en tenant compte du rôle juridique réel de chaque acteur. Le domaine de validité est celui des systèmes construits sur mesure et susceptibles de relever du régime haut risque du règlement (UE) 2024/1689. Trois matériaux sont mobilisés, et aucun ne conclut à la place des autres : des offres d'emploi, des conditions contractuelles publiques, le droit.

1. Ce que les offres rendent visible

Vingt-deux offres publiques de management FDE ont été codées, consultées le 13 novembre 2026 : quatorze chez des hyperscalers et laboratoires (Google Cloud, Microsoft, AWS, OpenAI, Anthropic, Scale AI, Cohere, Snorkel, Handshake), huit chez des plateformes ou éditeurs d'applications d'IA. L'inventaire, les liens et le codebook figurent en annexe A. Selon ce codebook, qui ne retient comme réglementaire qu'une mention nommant une obligation ou un référentiel externe, deux offres sur vingt-deux mentionnent explicitement un référentiel de conformité ; aucune ne cite l'AI Act ; aucune des sept offres d'hyperscalers ne contient de mention de ce type. Les vingt-deux parlent en revanche d'adoption, de croissance ou de vitesse.

Les deux occurrences sont instructives. Chez Scale AI, la conformité (SOC 2, RGPD, HIPAA) apparaît comme une limite à respecter dans le périmètre de sécurité et de conformité du client ; chez Parloa, elle prend la forme d'une expérience attendue du

RGPD et de la norme ISO 27001. Dans les deux cas, il s'agit de protection des données et de sécurité de l'information, non d'une réglementation propre aux systèmes d'IA. Ailleurs, les termes de gouvernance qui figurent dans les offres relèvent de la sécurité, de la souveraineté des données ou de l'IA responsable. Selon le codebook retenu, les mentions de conformité réglementaire explicite restent donc rares dans le corpus ; cela décrit le vocabulaire des offres, non la place de la conformité dans l'organisation réelle.

Le résultat mesure une visibilité, pas une organisation. Une offre indique ce que l'employeur choisit de mettre au premier plan pour recruter ; elle ne dit rien des objectifs internes, des artefacts livrés ni des équipes qui, sous d'autres intitulés, portent la conformité. Le corpus est restreint, non aléatoire et majoritairement américain ; il a été codé deux fois par le même codeur, mais ni par un second codeur ni contre un groupe de contrôle portant sur les offres de conformité des mêmes entreprises, qui permettrait de mesurer la visibilité de ces fonctions. La chaîne qui irait de « peu de mentions » à « le client hérite d'une dette » compte quatre maillons ; le corpus n'en documente qu'un. Ne pas savoir n'autorise pas à présumer ; cela oblige à lire les contrats.

2. Run technique, surveillance du fournisseur, surveillance du déployeur

Le même corpus nuance une idée reçue : les attentes de production, d'évaluation ou de fiabilité sont explicites dans dix-neuf offres sur vingt-deux. Ce que les offres rendent visible du côté de l'exploitation est d'une autre nature que ce qu'elles laissent peu visible du côté réglementaire.

Pour les systèmes à haut risque, et à compter du 2 décembre 2027 pour ceux de l'annexe III ou du 2 août 2028 pour ceux de l'annexe I, le règlement impose deux surveillances qui ne se recouvrent pas. L'article 72 oblige le fournisseur à mettre en place un système de surveillance après commercialisation, fondé sur un plan intégré à la documentation technique. L'article 26 oblige le déployeur à utiliser le système selon la notice, à en surveiller le fonctionnement et, le cas échéant, à en informer le fournisseur conformément à l'article 72 ; il l'oblige aussi à conserver les journaux générés automatiquement par le système, dans la mesure où ils sont sous son contrôle, pendant au moins six mois, sauf disposition contraire du droit applicable, notamment en matière de protection des données. Superviser un système pour qu'il fonctionne et pouvoir établir qu'il demeure conforme sont deux activités distinctes, portées par des acteurs distincts. *Run technique n'est pas run réglementaire.*

3. Lire des conditions FDE : un cas borné

AWS publie les conditions de son offre FDE, en version de *preview* mise à jour le 12 novembre 2026. Le document est public, précis et daté. Il a trois bornes. C'est un seul fournisseur. Ce sont des conditions de *preview*. Elles renvoient à un ensemble plus large : l'AWS Customer Agreement ou un autre accord applicable, une lettre de sprint qui déclenche l'engagement, un plan de sécurité pour l'accès à la production, des avenants sur les données réglementées et sur les données de santé, des politiques d'usage. Ce qui suit décrit les conditions FDE consultées, non l'ensemble contractuel.

Ces conditions circonscrivent d'abord les usages autorisés. Elles excluent les environnements dangereux et les systèmes critiques ; elles ne sont pas conçues pour des dispositifs médicaux finis et n'autorisent pas les solutions, seules, pour la décision clinique ; l'accès à des données de santé protégées suppose un avenant signé. Le cas ne dit donc rien de la manière dont on contracte un FDE pour un système à haut risque en santé ou en infrastructure critique. Il montre comment un fournisseur gère son propre risque : en délimitant ce qu'il autorise.

À l'intérieur de ce périmètre, la répartition est explicite. Le client décide du déploiement, exploite et maintient ; il répond des activités et des modifications dans son environnement de production, y compris celles exécutées par AWS sur ses instructions ; il gère accès, journaux et registres ; il veille à la conformité de l'usage aux lois applicables, l'AI Act étant cité nommément. Le règlement absent des offres figure donc dans le contrat, du côté des obligations du client. On n'en tirera pas davantage.

Les moyens remis sont réels. Le client détient le contenu développé et livré pendant le sprint (documents, logiciels, modèles, prompts) et reçoit une licence perpétuelle sur la propriété intellectuelle préexistante d'AWS qui y serait incluse ; ses ingénieurs travaillent aux côtés des FDE pendant des sprints de quarante-cinq jours. Les conditions consultées ne décrivent pas, en revanche, de transfert de compétences ni de support après l'engagement ; elles prévoient la révocation des accès de production d'AWS en fin de travaux et excluent tout conseil juridique ou de conformité.

Conclure à un manque de moyens serait un glissement : l'absence d'une promesse dans ce document ne prouve ni son absence ailleurs, ni l'absence de compétences chez le client. Ce que le cas établit est plus étroit. La répartition et la propriété se lisent dans ces conditions ; la suffisance des moyens pour un système donné ne s'y lit pas. Détenir le code et les prompts ne dit pas si l'on détient la documentation technique, les évaluations, les journaux et l'assistance qu'exigent les obligations applicables. *Attribuer une responsabilité et fournir les moyens de l'exercer sont deux points de vérification distincts.*

4. Qui est fournisseur ? Des faits, pas une clause

Le règlement définit le fournisseur comme la personne qui développe un système d'IA ou le fait développer et le met sur le marché ou en service sous son propre nom ou sa propre marque (article 3, point 3). L'article 25 vise ensuite trois situations où un déployeur ou un tiers devient fournisseur d'un système à haut risque : apposition de son nom ou de sa marque sur un système à haut risque déjà mis sur le marché ; modification substantielle d'un tel système, à condition qu'il demeure à haut risque ; changement de destination d'un système qui, de ce fait, entre dans la catégorie haut risque. Dans ces cas, le fournisseur initial cesse d'être considéré comme fournisseur de ce système aux fins du règlement ; l'article 25(2) prévoit qu'il coopère alors étroitement avec le nouveau fournisseur et met à sa disposition les informations, l'accès technique et l'assistance raisonnablement attendus, sauf s'il a clairement indiqué que son système ne devait pas être transformé en système à haut risque. La question des moyens se pose donc aussi au moment où le rôle de fournisseur change de mains.

Un système bâti sur mesure par une équipe FDE peut donc faire du client un fournisseur ; il ne le fait pas nécessairement. Les faits décisifs sont identifiables : qui développe ou fait développer le système, qui le met en service et sous quel nom, pour quelle destination, avec quelles modifications. Les conditions AWS apportent un indice, puisqu'elles interdisent de commercialiser les solutions sous la marque d'AWS ; elles ne tranchent pas la qualification et ne déchargent aucun opérateur de ses obligations légales. *Une clause répartit des engagements. Elle ne qualifie pas un fournisseur.*

5. Le régime transitoire : ce qui est clarifié, ce qui ne l'est pas

Depuis le règlement (UE) 2026/1744, en vigueur le 27 juillet 2026, l'article 111 précise le sort des systèmes à haut risque déjà sur le marché. Une part est clarifiée : ces systèmes ne sont concernés qu'en cas de changement significatif de conception à partir de la date d'application ; lorsqu'une première unité a été légalement mise sur le marché avant cette date, d'autres unités du même type et du même modèle peuvent continuer à l'être tant que la conception reste inchangée. Deux régimes particuliers s'y ajoutent : mise en conformité au plus tard le 2 août 2030 pour les systèmes destinés aux autorités publiques, régime propre pour les composants de certains grands systèmes d'information européens.

Une part reste incertaine, et elle est plus étroite qu'on ne le dit parfois : non pas l'existence d'un cadre, que le règlement modificatif a précisé, mais l'application pratique de la notion de changement significatif de conception à une nouvelle version de modèle, à des prompts modifiés ou à une architecture remaniée. Sur ce point précis, aucune doctrine

établie n'a été identifiée à ce jour [SOURCE À DOCUMENTER]. Une évolution de modèle ne déclenche donc pas automatiquement les obligations. Mais un système livré par itérations, dépendant de composants dont les versions évoluent, pose une question pratique que le calendrier ne règle pas : qui évalue la portée de chaque changement, selon quels critères, avec quelles informations ?

6. Ce que l'acheteur devrait vérifier

Trois vérifications, système par système. Sur la répartition : les conditions et les documents qu'elles incorporent, en commençant par le périmètre d'usage autorisé. Sur les moyens : ce qui est remis, puis ce qui est suffisant au regard du rôle effectivement tenu (voir ci-dessous), y compris le transfert de compétences, le support après le sprint et la procédure de documentation des changements. Sur le rôle : la qualification au regard des faits, indépendamment du contrat. Le risque d'une responsabilité sans moyens suffisants est à évaluer dans chaque engagement ; il n'est pas une conséquence démontrée du modèle FDE.

Ce qu'il faut posséder dépend du rôle, et les obligations d'un acteur ne créent pas, à elles seules, un droit général d'accès aux documents d'un autre. Pour un système à haut risque, la documentation technique est établie et conservée par le fournisseur (articles 11 et 18) ; elle intègre notamment les éléments de gestion des risques et d'essais, et un déployeur n'a pas, du seul fait de son rôle, un droit à en obtenir l'intégralité. Ce que le fournisseur doit remettre au déployeur, c'est une notice d'utilisation (article 13). Les journaux sont générés automatiquement par le système, dont la conception relève du fournisseur (article 12) ; chacun conserve ceux qui sont sous son contrôle (articles 19 et 26). Lorsque le client est lui-même fournisseur, il doit établir la documentation technique et a besoin, pour cela, d'éléments qu'il ne produit pas seul.

C'est là qu'interviennent les obligations de coopération. Outre l'article 25(2) évoqué plus haut, l'article 25, paragraphe 4, impose au fournisseur d'un système à haut risque et au tiers qui fournit un système d'IA, un modèle d'IA, des outils, services, composants ou processus utilisés ou intégrés dans ce système de préciser par accord écrit les informations, capacités, accès techniques et autre assistance nécessaires pour permettre au fournisseur de respecter ses obligations. L'exception vise les tiers qui rendent publiquement accessibles, sous licence libre et ouverte, des outils, services, processus ou composants autres que des modèles d'IA à usage général. Le support après le sprint et le transfert de compétences ne sont donc pas des obligations générales autonomes, dues dans tout contrat FDE. Mais une assistance postérieure au sprint peut relever de cet accord écrit lorsqu'elle est nécessaire pour permettre au fournisseur du système de satisfaire à ses obligations. Au-delà de ce qui est nécessaire en ce sens, elle relève de la bonne pratique d'achat.

Limites

Le corpus mesure une visibilité dans vingt-deux offres, dont treize sans date affichée, sans second codeur ni groupe de contrôle. Le cas contractuel est unique, en *preview*, et exclut plusieurs usages critiques et cliniques. Les accords propres aux clients, lettres de sprint comprises, n'ont pas été consultés. La notion de changement significatif de conception appliquée aux modèles d'IA reste sans doctrine établie. Les voies de sanction et de réparation, résumées en annexe B, dépendent de conditions et de calendriers propres que ce texte ne développe pas.

Conclusion

Le modèle FDE n'est ni une menace pour la conformité ni une solution à son problème. Il déplace la question vers un document que les offres n'éclairent pas : le contrat, lu ligne à ligne, puis confronté au droit et aux faits du système. Une répartition peut être parfaitement explicite sans que les moyens de l'exercer soient décrits au même endroit. Ce n'est pas un défaut propre à un fournisseur ; c'est une propriété de toute répartition.

L'annonce montre ce qu'on met en avant. Le contrat organise ce que les parties se doivent. Le droit qualifie, au cas par cas, qui répond de quoi.

Annexe A. Méthode du corpus

Sélection. Offres de management FDE (Manager, Senior Manager, Head, Director, Multidisciplinary Manager FDE) visibles en 2026 sur des pages carrières ou des agrégateurs ; consultées le 13 novembre 2026. Quatre offres exclues (page vide, poste pourvu, page inaccessible, texte non codable).

Inventaire. Les 22 offres figurent dans corpus.csv, qui accompagne l'article : entreprise, intitulé, segment, URL, date affichée, dates de consultation (13 novembre 2026) et de recodage (14 novembre 2026), codage par catégorie, extraits codés. Les extraits, de dix mots au plus, sont regroupés par offre dans fiches-corpus-2026-11-14.md. Dates : sept offres affichent une date absolue (de juin à septembre 2026, dont une date de mise à jour), deux une date relative, treize aucune. L'archivage public des pages n'a pas pu être réalisé depuis l'environnement de travail [SOURCE À DOCUMENTER].

Codebook. Unité : segment de phrase exprimant une attente du poste. Quatre catégories fixées avant lecture : conformité réglementaire (obligation ou référentiel externe nommé, par exemple SOC 2, RGPD, HIPAA, AI Act, réglementation sectorielle) ; gouvernance technique (sécurité, souveraineté et gouvernance des données, IA responsable, garde-fous) ; run et stabilité (production, évaluation, monitoring, fiabilité) ; commercial et vitesse (adoption, croissance, expansion, revenu, time-to-value, vitesse). Exclusions :

mentions légales RH et énoncés de mission. Exemples de codage : « dans le respect des limites de sécurité et de conformité du client (SOC 2, GDPR, HIPAA) » codé conformité réglementaire ; « secure governance » codé gouvernance technique. La règle tend à sous-estimer la catégorie réglementaire.

Procédure. Extraction automatique des occurrences puis revue manuelle par un seul codeur, en deux passes à un jour d'intervalle. Concordance entre les passes : 86 décisions identiques sur 88 (22 offres, 4 catégories). Les deux divergences sont documentées dans corpus.csv : une mention de conformité manquée au premier passage (Parloa), une mention d'habilitation de sécurité écartée au second (AWS). Le second passage fait foi. Double codage par un second codeur non réalisé. Cas limite consigné : une offre (Anthropic) mentionne des questions de propriété intellectuelle et de contrat, non codées comme conformité réglementaire.

Résultats par offre. Conformité réglementaire explicite : 1 sur 14 hyperscalers et laboratoires, 1 sur 8 plateformes. Gouvernance technique : 7 et 1. Run et stabilité : 14 et 5. Commercial et vitesse : 14 et 8. Les nombres d'occurrences dépendent du codebook et de la longueur des annonces ; ils ne sont pas utilisés dans le texte.

Annexe B. Voies juridiques possibles, sous conditions

Surveillance du marché (règlement (UE) 2024/1689, article 79) : pour un système présentant un risque, mesures d'abord correctives ; la restriction, le retrait ou le rappel font partie des mesures possibles. *Amendes* (article 99) : plafonds, notamment 15 millions d'euros ou 3 % du chiffre d'affaires mondial pour la plupart des obligations des opérateurs, avec critères d'appréciation et règles propres aux PME. *Responsabilité du fait des produits défectueux* (directive (UE) 2024/2853) : régime prévu pour les produits, logiciels et systèmes d'IA compris, mis sur le marché ou en service à partir du 9 décembre 2026, sous réserve de la transposition nationale ; responsabilité sans faute, mais preuve du dommage, du défaut et du lien de causalité, sous réserve des présomptions ; le fabricant peut être le développeur ou le fabricant d'un composant. *Actions représentatives* : directive (UE) 2020/1828, dont l'annexe I inclut le règlement sur l'IA à la suite de l'article 110 du règlement (UE) 2024/1689 ; atteintes aux intérêts collectifs des consommateurs. *Action de groupe en France* (loi n° 2025-391 du 30 avril 2025, article 16) : demandeurs habilités, personnes en situation similaire, manquement commun. Les acteurs visés et les conditions d'engagement varient selon le régime : l'opérateur concerné (fournisseur, déployeur ou autre) au titre de l'AI Act, sur le fondement de ses propres obligations ; le fabricant au titre de la responsabilité du fait des produits, sur la preuve d'un défaut, d'un dommage et d'un lien de causalité, sans qu'un manquement réglementaire soit requis ; le professionnel concerné dans une action collective, selon le fondement invoqué.

Sources principales.

Règlement (UE) 2024/1689 et règlement (UE) 2026/1744 (EUR-Lex) ; AWS, *FDE Preview Terms* (aws.amazon.com/legal/fde_terms, version du 12 novembre 2026) ; annonces d'AWS (aboutamazon.com, 30 juin 2026), de Microsoft (blogs.microsoft.com, 2 juillet 2026) et d'OpenAI (mai 2026, URL de l'annonce primaire [SOURCE À DOCUMENTER]) ; directive (UE) 2024/2853 ; loi n° 2025-391 du 30 avril 2025.