Les rendez-vous experts

Contrats IT

ÉPISODE #8 : Contrats cloud : quelles clauses sensibles (portabilité, réversibilité, continuité, suspension, tarification…) ?

Dans un contrat cloud, le fournisseur est structurellement en position de force : le client n'acquiert aucun bien tangible, seulement un droit d'accès temporaire à un service et à une infrastructure que le fournisseur maîtrise entièrement, y compris les données du client, qui y résident presque toujours exclusivement. Le contrat ne formalise donc pas un achat mais construit une promesse de service. Plusieurs clauses portent cette charge.

Clause de niveau de service (SLA) : le droit d'accès n'est rien sans garantie de continuité

Disponibilité. Le SLA doit définir le taux de disponibilité, sa méthode de calcul et ses exclusions (maintenance, force majeure, tiers). L'enjeu principal porte sur les conséquences d'un manquement : les service credits sont-ils une sanction réelle ou un mécanisme cosmétique ? Il faut se méfier des clauses qui en font le recours exclusif du client (sole and exclusive remedy), et prévoir un droit de résiliation en cas de manquements répétés, rarement offert par les modèles standards.

Support. Le client ne peut résoudre lui-même aucun incident, faute d'accès à la couche technique. La clause doit fixer des niveaux de criticité (P1, P2, P3), des plages de support adaptées, et distinguer clairement temps de prise en charge et temps de résolution. Une question est également fréquemment éludée lors des négociations : qu'advient-il en cas de non-respect par le fournisseur de ses engagements de support ?

Clause de suspension : la négation même de l'accès au service cloud

Le fournisseur détient la faculté, en un instant, de couper les accès du client au service. Il faut encadrer strictement les cas d'ouverture (impayé, faille de sécurité, etc.), imposer préavis et notification, et

exiger une suspension proportionnée plutôt qu'une coupure généralisée, pour éviter qu'elle ne devienne une résiliation de fait ou un moyen de pression.

Clauses d'évolution des services et des tarifs, ou la rançon d'un modèle par nature évolutif

Le service évolue en continu sans que le client n'en maîtrise le calendrier : la clause de description des services doit encadrer la faculté pour le fournisseur de faire évoluer les services, en ne permettant de telles modifications que sous réserve de ne pas dégrader le périmètre fonctionnel, et en offrant un droit de résiliation dans le cas contraire.

De même, l'évolution tarifaire, généralement prévue contractuellement, et fréquemment automatique et basée sur un index, doit être plafonnée, annoncée avec un préavis suffisant, et ouvrir un droit de résiliation sans pénalité en cas de hausse substantielle.

Clause de propriété des données et droit d'usage du fournisseur : l'ère de l'IA impose une vigilance accrue

La propriété des données ne pose généralement pas de débat et fait consensus d'un contrat cloud à l'autre : le client reste propriétaire de ses propres données. La vraie question, elle, porte sur l'usage que le fournisseur s'en réserve au-delà de la stricte exécution du service. L'essor des fonctionnalités d'IA dans les offres cloud donne à cette question une acuité particulière : le fournisseur traite-t-il les données du client uniquement pour exécuter le contrat, ou la clause d'usage lui permet-elle également de les exploiter pour développer ses propres technologies, voire entraîner ses modèles d'intelligence artificielle ?

Clause de protection des données et clause de sécurité : l'autre face de la mainmise

En cloud, l'éditeur agit généralement comme sous-traitant au titre du RGPD, dont l'article 28 impose de prévoir un socle d'obligations (instructions documentées, assistance, sort des données en fin de contrat, etc.). Assurer la sécurité des données en est une composante essentielle, la clause associée doit donc prévoir des engagements fermes : maintien de certifications (ISO 27001, SOC 2, HDS), chiffrement, authentification, gestion des accès, notification des incidents. Un renvoi à une politique du fournisseur est possible, sous réserve de prévoir que les mesures qui y sont décrites ne pourront être revues qu'à la hausse durant l'exécution du contrat.

Clause d'audit : désormais, c'est l'éditeur qui a des comptes à rendre

L'article 28 du RGPD impose au sous-traitant de permettre les audits du responsable de traitement. Contrairement au modèle *on-premise*, où l'audit sert surtout le fournisseur pour vérifier la licence, le besoin se déplace côté client, qui doit pouvoir vérifier la sécurité et la protection de ses données. La clause doit préciser périmètre, méthode, déclenchement et conséquences des écarts, idéalement dans un protocole dédié (notre **épisode 7** y était par ailleurs consacré).

Clause de réversibilité et clause de portabilité : préparer la sortie avant d'y être contraint

À négocier en amont de la signature, cette clause comprend trois volets : la portabilité (format et contenu de la restitution : données brutes, métadonnées, configurations, historiques) ; l'organisation de la migration (durée, maintien du service et assistance, tarification éventuelle) ; et l'effacement des données après restitution (délais, sort des copies résiduelles, certificat de destruction).

Cette exigence est aussi réglementaire : le RGPD impose au sous-traitant de supprimer ou restituer les données personnelles en fin de contrat, au choix du responsable de traitement. Le Data Act (chapitre VI) étend cette logique à toutes les données : suppression des obstacles au changement de fournisseur, préavis maximal de deux mois pour l'initiation de la migration, délai de transition de principe de 30 jours calendaires (pouvant être remplacé, en cas d'impossibilité technique dûment justifiée et notifiée dans les 14 jours ouvrés, par une période alternative allant jusqu'à sept mois), et suppression totale des frais de changement de fournisseur à compter du 12 janvier 2027.

Voir nos précédents épisodes

ÉPISODE #1 : Pourquoi les contrats IT ne sont pas des contrats comme les autres

ÉPISODE #2 : Contrats IA – Rien ne change, mais tout est différent

ÉPISODE #3 : Les effets des réglementations cyber (DORA et NIS2) sur les contrats IT

ÉPISODE #4 : Conformité légale des contrats IT : quelle liberté contractuelle ?

ÉPISODE #5 : Comment préparer ses contrats au Data Act ?

ÉPISODE #6 : Contrats IA : comment sécuriser la propriété des outputs ?

ÉPISODE #7 : La clause d'audit dans les contrats IT : simple clause de style ou véritable obligation ?

A propos de l'auteur – Paul Sierzputowski, Avocat

Paul Sierzputowski est spécialisé en droit en droit de la propriété intellectuelle, du numérique et des données personnelles.

Il est titulaire d'un Master 2 Common Law et Droit comparé de l'Université Paris Descartes.

Paul a assuré les fonctions de juriste durant six ans, à Paris puis à Boston, au sein de l'entreprise Mirakl, licorne française leader mondial de la fourniture de solutions cloud de places de marché.

Il est avocat au Barreau de Paris depuis 2022 et a rejoint Racine en 2025.

A propos de l'équipe IP IT & Data de Racine

Racine dispose d'une équipe de 11 avocats accompagnant groupes internationaux, grandes entreprises, ETI, acteurs du numérique et start-up dans leurs projets de transformation digitale et sur leurs problématiques liées au droit de la propriété intellectuelle.

Ainsi, l'équipe intervient principalement dans 3 domaines de compétences :

- L'IT : informatique, télécommunications, sécurité des systèmes d'information, intelligence artificielle. L'équipe dispose d'une expertise reconnue dans l'accompagnement des projets informatiques et numériques.
- Data Protection : protection des données à caractère personnel et le déploiement du RGPD, contrôle et contentieux devant l'autorité de contrôle.
- L'IP : protection et valorisation du patrimoine immatériel et contentieux associés.

Paul Sierzputowski
Avocat
psierzputowski@racine.eu
Tel. : +33 (0)1 44 82 43 00
www.racine.eu