Les rendez-vous experts

Contrats IT

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

La clause d'audit dans les contrats IT est passée d'une bonne pratique optionnelle à une obligation en grande partie imposée par les réglementations. Mais l'avoir écrite ne suffit pas : encore faut-il savoir si elle sera appliquée, par qui, comment, et avec quelles conséquences. C'est là que la plupart des contrats pèchent.

De la faculté à l'obligation

Il y a quelques années encore, la clause d'audit dans un contrat IT relevait de la bonne volonté contractuelle. Certains praticiens la négociaient systématiquement ; la plupart des contrats n'en contenaient pas, faute d'obligation ou de pression suffisante pour l'imposer. Aujourd'hui, la situation a radicalement changé. Cette clause, qui confère à l'une des parties le droit de vérifier que son cocontractant respecte ses obligations contractuelles (niveaux de service, exigences de sécurité, traitement de données personnelles), s'impose désormais dans les contrats IT autant sous l'effet d'impératifs réglementaires que d'un besoin de transparence dans une relation où l'une des parties confie des actifs critiques à une autre.

Le RGPD en a fait une obligation non négociable : l'article 28 impose que le sous-traitant permette et contribue aux audits du responsable de traitement. Les annexes relatives à la protection des données prévoient généralement un droit d'audit encadré (préavis minimal, nombre d'audits par période, périmètre). Il est cependant recommandé de prévoir une exception en cas de violation de données ou de manquement grave. C'est précisément dans ces situations que le contrôle est urgent et que les restrictions classiques risquent de devenir un obstacle à la gestion de crise.

DORA impose de son côté aux entités financières et à leurs prestataires de services TIC des droits d'audit renforcés. NIS2, bien que toujours en attente de sa transposition française, renforce les obligations de contrôle à l'égard des entités importantes et essentielles. La clause d'audit n'est donc plus négociable sur le principe : la marge de manœuvre porte sur ses modalités d'exercice.

Rédiger une clause d'audit c'est bien, l'appliquer c'est mieux

Le choix de déclencher ou de ne pas déclencher un audit soulève les questions les plus importantes.

Ne pas exercer son droit d'audit n'est pas sans conséquence. D'abord, sur le plan de la responsabilité propre du client : lorsque l'audit est imposé par une réglementation (DORA et RGPD notamment) ou exigé par son assureur cyber, ne pas le réaliser peut constituer un manquement à ses propres obligations, susceptible d'engager sa responsabilité en cas d'incident. Ensuite, sur le plan de la relation contractuelle : un prestataire avisé peut se prévaloir de l'absence d'audit pour limiter sa propre responsabilité, au motif qu'il n'a pas pu être contrôlé et que les manquements éventuels n'ont donc pas été détectés ni formalisés en temps utile. La clause d'audit non exercée devient ainsi un argument au service du prestataire plutôt que du client.

La mise en œuvre : de la clause au protocole d'audit

C'est au stade de sa mise en œuvre que la clause d'audit révèle le plus souvent ses limites. Les clauses d'audit dans les contrats IT sont fréquemment rédigées de manière trop sommaire. On y lit que « le client dispose d'un droit d'audit », sans que quoi que ce soit ne soit précisé sur la méthode, le périmètre, le déclenchement ou les conséquences. En pratique, cela revient à donner au prestataire toute latitude pour résister à un audit, en soulevant des questions de forme ou de méthode que la clause ne tranche pas. La pratique a développé une réponse à ce problème : l'accord d'audit préalable, parfois appelé accord de méthode d'audit ou protocole d'audit. Ce document, annexé au contrat principal ou négocié en amont d'un audit, définit les modalités d'exercice du droit : périmètre, métriques, locaux et documentation concernés, procédure de déclenchement, obligations des parties, règles de confidentialité.

Ce protocole doit répondre à plusieurs exigences fondamentales. L'identité de l'auditeur se tranche en amont, tiers indépendant des deux parties ou directement l'une d'entre elles selon le contexte. Le principe de non-perturbation des activités doit être posé : accès organisés en dehors des heures critiques, durée maximale définie, nombre de personnes habilitées encadré. La fréquence doit être proportionnée et la répartition des coûts doit être prévue. Et surtout, ce protocole doit préciser ce que l'on cherche à vérifier, avec quelle méthode, et quelle est l'incidence d'un écart constaté. Sans cela, l'audit peut se conclure sur un constat sans suite, ce qui revient à en neutraliser l'utilité.

La question du rapport d'audit mérite également d'être anticipée. L'accord d'audit peut prévoir que le projet de rapport soit communiqué à la partie auditée avant toute diffusion ou utilisation, avec un délai suffisant pour formuler des observations ou des corrections. Cette étape réduit les risques d'inexactitude ou de mauvaise interprétation et renforce l'opposabilité du rapport, la partie auditée pouvant difficilement contester une méthodologie sur laquelle elle a été mise en mesure de s'exprimer.

La clause d'audit n'est donc plus un simple accessoire du contrat IT. Mais la présence de cette clause dans le contrat n'est qu'une première étape : encore faut-il l'avoir rédigée avec suffisamment de précision pour qu'elle soit réellement exerçable et avoir anticipé ce que l'on fera une fois l'audit déclenché. Sans protocole d'audit définissant ses modalités d'exercice, une clause d'audit risque de demeurer inopérante, privant ainsi le client de la protection qu'il croyait avoir obtenue.

[PROCHAIN rdv] RDV le 7 septembre pour notre prochain épisode :
Les spécificités du contrat cloud

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 ?

A propos de l'auteur

Tudi Quistinic, avocat

Avocat au barreau de Paris, j'accompagne mes clients sur les problématiques de droit de la propriété intellectuelle, du numérique et de la protection des données personnelles. Titulaire d'un Master 2 en droit du numérique de la Faculté de droit et de science politique de l'Université de Rennes 1, j'ai rejoint Racine en 2025 après avoir prêté serment en 2024. Au sein de l'équipe j'interviens plus particulièrement pour les clients « publics ».

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.

Tudi Quistinic
Avocat collaborateur
tquistinic@racine.eu
Tel. : +33 (0)1 44 82 43 00
www.racine.eu