

Les rendez-vous experts

Contrats IT

ÉPISODE #9 : Audit amont des prestataires IT : Démarche de style ou étape décisive ?

En quelques années le mode « on prem » a cédé la place au SaaS et autre Cloud c'est en moyenne plus de 90 à 95% de l'IT des entreprises mais aussi des acteurs publics qui se voient confiés à des prestataires IT tiers.

Conséquence : le centre de gravité du risque IT s'est déplacé vers les prestataires extérieurs.

DORA, NIS2, RGPD : ces textes ont un point commun, celui d'imposer aux entreprises davantage de rigueur dans la gestion de leurs prestataires IT.

Cette rigueur s'organise sur 3 plans : la rédaction de contrats/clauses adaptées ; l'audit des prestataires dans le cadre de l'exécution des contrats mais aussi et surtout la vérification amont de la conformité des prestataires IT.

Certaines entreprises ont mis en place des questionnaires de qualification, ce qui est sans doute la bonne approche sur le principe. Mais ces questionnaires souffrent de deux défauts récurrents. D'une part, ils posent parfois des questions inadaptées, standardisées, déconnectées du profil réel du prestataire évalué. D'autre part, et c'est plus grave encore, les réponses obtenues ne font l'objet d'aucune analyse sérieuse : le questionnaire est envoyé, rempli, classé, et personne n'en tire de conséquence opérationnelle.

D'autres entreprises se contentent d'un simple e-mail demandant au prestataire de confirmer qu'il est conforme. Il ne faut pas alors s'étonner que le prestataire réponde « oui » sans apporter la moindre démonstration. Cette démarche, en l'absence de toute vérification, n'apporte strictement aucune garantie.

D'autres encore se satisfont de la présentation d'une certification ou d'une norme, comme si le seul fait de la détenir suffisait à couvrir l'ensemble des risques de la relation. Une norme est un point de départ utile mais ne sera jamais une réponse en soi.

L'audit amont / la qualification préalable d'un prestataire est donc une étape décisive. Elle ne peut pas être considérée comme une simple « démarche de style ».

Une démarche rigoureuse de qualification en amont repose sur trois exigences cumulatives.

1. Un questionnaire adapté au risque que représente la relation pour l'entreprise, et non un questionnaire générique appliqué indifféremment à tous les prestataires. Ce questionnaire n'est d'ailleurs pas un simple questionnaire de sécurité car d'autres questions doivent être posées au prestataire. Au cas particulier d'un sous-traitant RGPD il est utile de poser d'autres questions sur : la désignation ou non d'un DPO, l'existence ou non de contrôle Cnil chez le prestataire, ...
2. Une prise en compte, chaque fois que possible, du profil propre du prestataire : sa taille, la criticité de la prestation, la nature des données traitées, sa maturité en matière de sécurité.
3. Une analyse réelle des réponses obtenues, assortie de conséquences concrètes : demande de compléments, mesures correctives à intégrer au contrat, voire remise en cause du choix du prestataire.

Sans cette dernière étape, tout le dispositif s'effondre. Un questionnaire rempli mais jamais analysé n'est qu'une case cochée. Il ne protège ni le client en cas d'incident, ni sa capacité à démontrer, devant un régulateur ou un juge, qu'il avait correctement sélectionné son prestataire.

Le contrat encadrera la relation. L'audit d'exécution permettra de la contrôler dans la durée. Mais c'est en amont, au moment de la sélection, que se joue la première ligne de défense. Une qualification bien menée oriente la rédaction des clauses, calibre les futurs audits, et surtout, évite de découvrir trop tard qu'un prestataire critique n'était pas à la hauteur des enjeux qui lui avaient été confiés.



[PROCHAIN rdv] RDV le 20 octobre pour notre prochain épisode :

Comment reporter les exigences d'accessibilité numérique dans ses contrats IT ?

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 ?](#)

[ÉPISODE #8 : Contrats cloud : quelles clauses sensibles \(portabilité, réversibilité, continuité, suspension, tarification...\) ?](#)

A propos de l'auteur – Eric Barbry, avocat associé

Avocat spécialisé dans le domaine de l'IP/IT & Data Protection au sein du cabinet Racine, je vous propose une nouvelle approche du droit, résolument pratique, basée sur mon expérience professionnelle : celle d'un avocat qui travaille sur le droit des technologies depuis plus de 25 ans.

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.



Eric Barbry
Avocat associé
ebarbry@racine.eu
Tel. : +33 (0)1 44 82 43 00
www.racine.eu