racine
AVOCATS

Les rendez-vous experts

Contrats IT

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

De l'obligation réglementaire à l'obligation contractuelle

Le paysage réglementaire européen en matière de cybersécurité a connu une mutation profonde avec l'adoption du règlement DORA et de la directive NIS 2, dont les exigences redessinent les contours de la relation contractuelle entre les entités assujetties et leurs prestataires informatiques.

S'agissant de DORA, le texte impose dans son article 30 l'insertion de stipulations contractuelles dans tout contrat conclu par un client dit « entité financière » avec ses prestataires de services TIC. Ces clauses couvrent notamment la description précise des services fournis, les exigences de sécurité applicables, les modalités de supervision, les droits d'audit ou encore la gestion des incidents. Il ne s'agit plus d'une faculté laissée à l'appréciation des parties, mais d'un contenu contractuel minimum imposé par le régulateur.

La directive NIS 2, quant à elle, retient une approche différente car le texte ne prescrit pas l'insertion de clauses spécifiques dans les contrats informatiques. Ses articles 20 et 21 font peser sur les entités dites « essentielles et importantes » une obligation de sécurisation de leur chaîne d'approvisionnement, impliquant notamment que leurs prestataires IT respectent, par voie contractuelle, des mesures de sécurité à même de répondre aux exigences de gestion des risques de leurs clients.

Ainsi, ces deux textes procèdent d'une même logique : la cybersécurité cesse d'être une obligation purement interne à l'entité pour devenir une exigence contractuelle opposable aux prestataires IT. En d'autres termes, les obligations réglementaires « ruissellent » sur la chaîne contractuelle, et le fournisseur de services informatiques se trouve désormais tenu d'engagements directement adossés au cadre normatif applicable à son client.

L'enjeu des négociations des contrats informatiques ne réside alors pas uniquement dans l'inventaire des obligations à stipuler, mais également dans la façon dont elles pourront plus ou moins avantager l'une ou l'autres des parties au contrat.

L'effet sur le champ des négociations

Si le contenu des obligations n'est pas négociable, leur traduction opérationnelle, elle, l'est.

S'agissant du Règlement DORA, d'un point de vue client, la présence formelle des stipulations obligatoire ne saurait suffire si leur mise œuvre n'est pas envisagée : leur paramétrage détermine l'efficacité du dispositif. Les discussions se concentrent alors sur des points techniques tels que la granularité et la régularité des reportings portant sur les incidents, les vulnérabilités ou les résultats des tests de résilience, les conditions d'exercice des droits d'audit (fréquence de l'audit, méthodologie, etc.) ou encore les modalités concrètes de gestion des incidents. Chacune des parties trouve ainsi sa marge de manœuvre dans la formulation des aspects opérationnels des obligations prévues par l'article 30 du Règlement.

La directive NIS2, à la différence de DORA, laisse aux entités assujetties la liberté d'organiser, par voie contractuelle, la gestion des risques liés à leur chaîne de sous-traitance. Cette souplesse a une conséquence directe : la négociation contractuelle devient le lieu majeur de construction de la conformité du client. Il revient ainsi à chaque entité essentielle ou importante de définir, dès la phase de contractualisation, les modalités concrètes par lesquelles elle s'assurera du respect de ses obligations sur le plan de sa relation avec les prestataires IT.

De telles évolutions transforment les modalités de négociation des contrats IT. Celle-ci ne peut plus être appréhendée comme un exercice purement juridique ou commercial. Elle mobilise désormais de nouvelles fonctions : les équipes de la DSI, qui définissent le niveau d'exigence en matière de sécurité.

L'effet sur le marché

Les nouvelles exigences issues de DORA et NIS 2 produisent, au-delà de leur portée strictement contractuelle, un effet structurant sur l'ensemble du marché des prestataires de services TIC.

Sous la pression de ces nouvelles contraintes pesant d'abord sur les clients, mais aussi, par ricochet, sur les prestataires de services TIC, le marché tend vers un rehaussement progressif du niveau d'exigence. Les prestataires sont conduits à renforcer la qualité de leurs services, en particulier s'agissant de résilience et de continuité opérationnelle, de leurs capacités de reporting et de transparence, ainsi que de leurs dispositifs de sécurité, pour répondre aux standards désormais imposés par leurs clients, soumis à réglementation.

Cette dynamique conduit vers une forme de convergence : l'harmonisation des exigences portant sur la cybersécurité contribue à l'émergence d'offres démontrant une plus grande maturité sur l'ensemble du marché des services informatiques.

Toutefois, cette évolution n'est pas sans effets sur la structure du marché. Les prestataires disposant de ressources suffisantes sont, eux, bien en mesure de s'adapter, d'investir dans leurs dispositifs de sécurité et de faire évoluer leurs offres pour répondre aux nouvelles exigences. À l'inverse, les acteurs de plus petite taille se heurtent à des obstacles significatifs : manque de moyens humains pour

déployer les dispositifs requis, difficulté à absorber les coûts liés à la mise en conformité, difficultés à satisfaire certaines exigences contractuelles spécifiques. Le risque systémique en ressort aggravé.

En synthèse, l'adoption du Règlement DORA et de la directive NIS2 ont d'importantes conséquences sur les contrats IT, aussi bien sur le plan juridique que sur le plan commercial :

Effet 1 – Les obligations en matière de cybersécurité font désormais partie intégrante du contenu contractuel obligatoire.

Effet 2 – Si le principe de ces obligations n'est pas négociable, leur traduction opérationnelle constitue le véritable espace de discussion entre les parties.

Effet 3 – La négociation des contrats IT cesse d'être un exercice exclusivement juridique ou commercial : les équipes de la DSI s'imposent désormais comme des interlocuteurs incontournables à la table des négociations.

Effet 4 – Sous la pression des exigences réglementaires qui pèsent sur leurs clients, les prestataires de services TIC sont contraints d'élever leur niveau de maturité en matière de cybersécurité, ce qui a pour conséquence une montée en maturité des produits et services proposés.

RDV le 11 mai pour notre prochain épisode :
Conformité légale des contrats IT : quelle liberté contractuelle ?

Voir nos précédents épisodes

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

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

A propos de l'auteur – Gabrielle Denoix de Saint Marc, Avocate collaboratrice

Avocate spécialisée dans le domaine de l'IP/IT & Data Protection au sein du cabinet Racine, Gabrielle intervient tant en matière de mise en conformité au RGPD que sur de la rédaction et négociation de contrats informatiques. Plus spécifiquement, Gabrielle a acquis plus une expertise en matière de règlementation sur la cybersécurité et accompagne de nombreux clients sur leur mise en conformité.

Gabrielle est titulaire du Master 2 « Droit de la propriété littéraire, artistique et industrielle » de l'Université Paris 2 Panthéon Assas ainsi que d'un Programme Grande Ecole de l'EM Lyon Business School.

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.

Gabrielle Denoix de Saint Marc
Avocate collaboratrice
gdenoixdesaintmarc@racine.eu
Tel. : +33 (0)1 44 82 43 00
www.racine.eu