Les rendez-vous experts

Contrats IT

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

Le Data Act est un règlement européen mal compris. D'une part, il est proche dans son intitulé de son cousin le Data Governance Act. Pour entretenir la confusion, ils traitent tous deux de la donnée en général, qu'elle soit personnelle ou non (contrairement au RGPD qui ne traite que de la donnée personnelle).

Le Data Governance Act encourage « l'altruisme » en matière de partage de données dans l'UE pour des objectifs d'intérêt général et non lucratifs. Ces acteurs « altruistes » bénéficient alors d'un logo « OAD ».

Le Data Act traite de sujets beaucoup plus industriels liés en général au régime de l'accessibilité de la donnée. Ce règlement pose d'ailleurs l'un des jalons de ce que l'on a de plus proche au sujet (tabou, au moins chez les juristes) de la propriété de la donnée.

Le Data Act est aussi assez difficile à résumer tant il est différent d'un chapitre à l'autre. On peut néanmoins classer ces règles dans trois volets que nous reconnaissons imparfaits et déséquilibrés :

- Le premier volet du Data Act concerne l'internet des objets (plus souvent appelé par son acronyme anglophone « IoT » pour Internet of Things. On y trouve tous les rapports commerciaux B2B et B2C qui concernent de près ou de loin les objets connectés (engins agricoles connectés, capteurs connectés, dispositifs médicaux connectés, Smart TV, imprimantes, etc …) et même des objets connectés « par nature » comme les smartphones et les ordinateurs. Sont en revanche exclus les serveurs et les routeurs.

- Le deuxième volet du Data Act concerne la question du changement de service de traitement de données (ce que la presse spécialisée a rapidement baptisée « cloud switching ») qui contient notamment ce fameux dispositif permettant de changer aisément de fournisseur cloud (suppression progressive des frais de réversibilité sortante jusqu'au 12 janvier 2027).

- Le troisième volet du Data Act contient les obligations que l'on pourrait, selon le point de vue, qualifier de « résiduelles », comme le partage de données avec les organes de l'Etat en cas d'urgence et plus généralement les obligations B2A, ou encore les dispositions propres aux

« smart contracts » et aux « espaces européens de données », deux nébuleuses à la portée encore incertaine.

L'ensemble se complète dans une cohérence globale mais ce sont ces deux premiers volets qui attirent l'attention du rédacteur de contrat.

Les pages des revues spécialisées se sont noircies au sujet du cloud switching. Pendant ce temps, les chapitres II, III et IV du Data Act, qui concernent l'IoT, semblent en reste, alors que de ceux-ci découlent de nombreuses obligations qui s'appliquent presque tout aussi largement aux consommateurs comme aux entreprises, tant les objets connectés ont afflué dans leurs quotidiens respectifs.

1. L'intérêt des clauses de redondance

Le Data Act est entré en vigueur récemment (le 12 septembre 2025 pour la plupart de son dispositif) et certaines dispositions spécifiques entreront en vigueur progressivement jusqu'en 2027.

En manque cruel de recul sur le sens et la portée du règlement, les parties peuvent vouloir rappeler expressément au contrat que le règlement leur est applicable. C'est une pratique courante qui vient donner une assise contractuelle à une situation de fait qui pourrait faire l'objet d'un débat.

Dit autrement, ce qui est dans le marbre du contrat ne fait pas débat, quand bien même sans l'écrire, les évènements futurs auraient prouvé que ce qui avait été prévu était vrai. Par exemple, les parties ont un doute sur la qualification d'un acteur au sens du texte (fabricant de produit connecté, tiers détenteur des données, destinataire des données, etc) et préfèrent le stipuler.

Il s'agit là de la même logique que la clause du contrat de travail qui rappelle la convention collective applicable. Les tribunaux considèrent généralement que cette référence sert uniquement à informer le salarié du cadre collectif applicable et ne contractualise pas les avantages qui y sont associés.

Cette technique permet aussi de faire une synthèse des droits qui seraient, avec ou sans clause, applicables au contrat, car d'ordre public (le droit d'accès aux données et la portabilité, l'interdiction d'espionnage industriel, la protection contre les clauses abusives).

Mais ces clauses vont plus loin, elles servent également à asseoir l'applicabilité d'une disposition du Data Act en particulier, pour insister sur le fait qu'elle s'applique bien à la situation de l'espèce visée par le contrat, pour appuyer par exemple la qualification d'un acteur du contrat en rappelant une obligation qui n'est applicable qu'à la qualification associée.

Il nous semble donc essentiel d'insérer au contrat certaines clauses de redondance dont le but est d'écarter d'un débat futur la question de l'applicabilité d'une disposition, notamment lorsque le doute est permis sur la qualification ou le régime applicable à une situation de fait.

2. Préciser les zones d'ombre du Data Act

Le Data Act ouvre la porte à de nouveaux horizons en matière de partage de données. Il crée des obligations qui pèsent principalement sur les fabricants de produits connectés, les fournisseurs de services connexes et les détenteurs de données, ces qualifications pouvant désigner une seule et

même entreprise. Le règlement élargit ainsi également le champ de la négociation contractuelle, principalement pour les rapports B2B entre clients et fournisseurs (les consommateurs ne négociant en pratique que très peu les contrats concernés).

Sans prétendre à l'exhaustivité, nous remarquons que les marges d'interprétation pour les rédacteurs de contrats sont notamment les suivantes.

Le Data Act prévoit que le fournisseur ne peut utiliser les données non personnelles qu'exclusivement sur la base d'un contrat avec son client. Il convient alors de rédiger une clause d'usage qui autorise le fournisseur à utiliser les données pour la maintenance de la machine, mais exclut expressément la revente à des tiers ou la création de modèles statistiques externes, à moins d'une contrepartie financière ou d'une remise sur le prix de l'équipement.

Le Data Act donne accès aux données "brutes" et "prétraitées", mais exclut les informations "dérivées ou déduites" issues d'algorithmes complexes du fabricant. L'enjeu ici est donc un enjeu classiquement renouvelé, celui des définitions. Les fabricants arguent que la moindre donnée traitée par sa machine est une donnée "dérivée" couverte par sa propriété intellectuelle, et en refusent l'accès. Juristes et techniciens devront unir leurs forces pour définir, dans la liste la plus exhaustive possible (idéalement en annexe technique), le périmètre exact des données brutes et des métadonnées qui seront fournies (ex : données de télémétrie, température, consommation), en précisant que toute opération basique de formatage ou de nettoyage effectuée par le fabricant ne transforme pas ces données en données "dérivées".

Le Data Act permet également au fabricant de bloquer ou de refuser le partage de certaines données s'il estime qu'elles constituent des "secrets d'affaires" pouvant lui causer un préjudice économique grave, particulièrement s'il craint une fuite vers des pays tiers. Le fabricant ne peut pas décréter unilatéralement que tout est secret. Le texte exige que les parties conviennent de mesures de confidentialité avant la divulgation. Il convient alors de rédiger et annexer un accord de confidentialité (NDA) qui identifie et marque précisément quelles données spécifiques relèvent du secret des affaires. Il est également utile de prévoir à l'avance quelles sont mesures techniques (chiffrement, contrôles d'accès) que le client s'engage à respecter.

Enfin, le Data Act ne prévoit pas de "droit à l'effacement" automatique pour les données non-personnelles (contrairement au RGPD). Si l'objet connecté est revendu ou était loué, le fournisseur n'a pas spécifiquement l'obligation de supprimer l'historique de vos données industrielles, ce qui engendre le risque que le futur acquéreur ou le fabricant ait accès à un historique de production. Dans le silence du texte, une clause de purge est donc de mise.

Les éléments à retenir

Règle 1 – Se méfier des qualifications diverses et complexes du règlement

Règle 2 – Se servir des clauses de redondances pour figer ces qualifications juridiques

Règle 3 – Clarifier les zones d'ombres avec des clauses et des annexes techniques

[PROCHAIN rdv] RDV le 22 juin pour notre prochain épisode :
Contrats IA : comment sécuriser la propriété des outputs ?

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 ?

A propos de l'auteur – Guillaume Jagerschmidt, avocat

Guillaume Jagerschmidt est spécialisé en droit des données à caractère personnel, de l'informatique et de la propriété intellectuelle appliquée aux secteurs du numérique. Il dispose d'une compétence particulière sur les données de santé.

Il est également enseignant à l'Université Paris-Cité (ex-Paris V Descartes) en droit des obligations, tant en droit des contrats qu'en droit de la responsabilité civile. C'est dans cette université qu'il a été diplômé d'un master 2 droit des obligations civiles et commerciales, complété par un second master 2 en droit du commerce électronique et de l'économie numérique à la Sorbonne. Il enseigne également le droit de la protection des données personnelles dans le Master DPO d'Oteria Cyber School.

Il est avocat au Barreau de Paris depuis 2022 et a rejoint Racine en 2024.

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.

Guillaume Jagerschmidt
Avocat collaborateur
gjagerschmidt@racine.eu
Tel. : +33 (0)1 44 82 43 00
www.racine.eu