Tour d’horizon des contrats SaaS

Maître Olivia Flipo, Docteur en droit – Avocat au Barreau de Paris

Mardi 7 septembre 2021

Définition : SaaS

Pas de définition légale

- Logiciel hébergé dans le Cloud et exécuté par l'éditeur pour les utilisateurs qui y accèdent par Internet
  - Logiciel « dématérialisé » (instance virtuelle) : données stockées dans le Cloud
  - Logiciel « distribué en tant que service » : abonnement à un service
  - Logiciel toujours à jour : perpétuelle évolution, mise à jour permanente, difficile d'identifier les versions
  - Logiciel toujours accessible : utilisable partout et n'importe quand

- Contrat SaaS
  - Un contrat de service
  - Inclut un droit d'utilisation en faveur du client (licence)
  - Conclu entre le client utilisateur et l'éditeur/fournisseur du service/revendeur qui « implique » un hébergeur/fournisseur d'infrastructure cloud
  - Le standard du fournisseur

Définition : SaaS

Conséquence de l’absence de définition légale

- En matière de responsabilité, une question demeure, qui sera certainement portée un jour à l'attention des juridictions :

❖ l'obligation essentielle du prestataire cloud est-elle la mise à disposition d'une solution digitale ou la mise à disposition continue d'une solution digitale sécurisée ?

❖ comment résoudre le vide juridico-conceptuel qui existe à propos de ce qu'est un service cloud ? (selon la réponse, le régime de responsabilité associé au manquement est bien différent (et la rédaction du contrat aussi)

❖ comment couvrir les risques assumés par les parties ?

Clause contractuelle

Décrire précisément le contenu des services fournis (standard et options)

- Un service standard ou sur-mesure selon le business model du prestataire
- Le fournisseur doit définir les contours de son engagement/de son service : backup (standard, au choix, niveau de sécurité standard, au choix, système redondant), maintenance corrective, évolutive, règlementaire, réversibilité (obligation essentielle), etc.
- Le fournisseur doit stipuler que l'ensemble formé par les services qu'il propose est indivisible, pour éviter en cas de contentieux judiciaire, un éventuel découpage de son service aboutissant à déformer le calcul de son prix (par un juge)

Clause essentielle

Décrire la disponibilité ou la continuité du service

- les risques d'indisponibilité et leurs conséquences doivent être abordés entre les parties et documentés contractuellement pour avoir une visibilité claire et exhaustive sur ce qui constitue une indisponibilité du service et sur les risques encourus de part et d'autre.
- Une des obligations principales du fournisseur

❖ Un engagement chiffré (niveau de service ou SLA)

- Définir les métriques : engagement mesurable objectivement qualitativement et quantitativement
- Limiter la responsabilité du fournisseur du fait d'une indisponibilité qui durerait et qui pourrait avoir des effets sur plusieurs clients (un data center entier, par exemple). Ce risque doit être traité de manière systématique et harmonisée avec l'ensemble des clients.
- Garantie : obligation de résultat
- Inclut la maintenance
- Peut être utile de se référer au versioning des éditeurs de navigateur (prérequis)

❖ Souvent, le client réclame une clause « pénalités » (pénalités moratoires)

- Evaluation forfaitaire et anticipé du préjudice
- Fixer les manquements déclenchant la mise en œuvre de la clause (qualitativement et quantitativement) et les modalités de calcul de la pénalité (forfait, pourcentage, plafond mensuel, annuel)
- Sont libératoires qu'elles soient ou non qualifiées de telles

Clause essentielle

Décrire les mesures de protection des données

- La protection des données est consolidée autour de trois aspects :

❖ la propriété des données/du contenu du client (téléchargé ou créé)

❖ leur confidentialité

❖ leur sécurité :

- Le fournisseur fournit la politique standard de sécurité. Le client doit vérifier que cette politique répond bien à ses propres exigences dans la matière (annexe = contrat)
- Il peut s'agir de la politique de l'hébergeur (pas au-delà)
- Lorsque le client est un Opérateur d'Importance Vitale, l'ensemble des mesures de sécurité que l'ANSSI impose à cet OIV vont impacter techniquement et juridiquement la relation entre l'OIV et le fournisseur.

Clause essentielle

Décrire la sécurité de façon plus large :

❖ Programmes malveillants :

- Engagement : Le fournisseur a l'obligation de "faire leurs meilleurs efforts" afin de détecter et bloquer les malwares connus et non répertoriés : obligation de moyens : se référer à l'état de l'art
- Définition des programmes malveillants (malwares, virus, cheval de Troie, etc.) : désigne un logiciel d'un éditeur tiers inconnu installé de manière illégitime dans le système d'information d'une Partie et destiné à porter atteinte à la sécurité de tout logiciel, données ou matériel composant ce système d'information.

❖ Vulnérabilités :

- Engagement : Idem
- Définition des vulnérabilités : désigne toute faille, faiblesse, défaut de conception qui peuvent être intentionnellement ou accidentellement exploités par un tiers et affectant le service fourni dans le cadre du contrat.

Données personnelles : sanction du défaut de sécurité

- Depuis 2017, plusieurs décisions de condamnation de la CNIL utilisent expressément les notions de cyber attaque et de vulnérabilité.
- L'article 32 du RGPD impose aux professionnels de sécuriser techniquement leurs systèmes d'information lorsqu'ils traitent des "données à caractère personnel".

CNIL, 19 décembre 20218 (cyber attaque)

CNIL, 28 mai 2019 (vulnérabilité d'un site web)

Clause essentielle

La répartition des risques

- Les fournisseurs SaaS ne peuvent pas, en l'état de l'art, tout détecter : limitation du risque de trois manières
  - Des pénalités libératoires lui permettant d'avoir une visibilité sur l'étendue de son risque financier
  - Exclusion de certains risques (malware, vulnérabilité)
  - Exclusion de certains dommages pouvant découler d'une indisponibilité ou d'un défaut de sécurité du service (perte de revenus ou de profits, atteinte à l'image, etc.)
- Les clients professionnels utilisateurs doivent accepter certains risques et faire face à des malveillances et/ou à des vulnérabilités non répertorié(e)s qui pourraient infecter leur système d'information.
  - Argument : les dommages subis devraient être supportés par le client, qui reste maitre de la manière dont il utilise le service et des données qu'il y télécharge.

La responsabilité des fournisseurs de systèmes numériques
Rapport à M. le Vice-président du Conseil Général de l'Economie, juin 2020

La répartition des risques

- Côté client :

❖ Pour un ré-équilibrage des relations contractuelles, instaurer par la loi des obligations accessoires aux contrats de service en ligne

❖ Ces obligations accessoires pourraient par exemple poser les principes suivants :

- La fourniture du service est une obligation de résultat
- Le contrat doit comporter un accord sur les niveaux de service (SLA) pour la disponibilité du service, le délai maximum de réponse à une sollicitation du support client, la modification substantielle d'une fonctionnalité ou sa disparition doivent être annoncées avec un délai suffisant pour permettre au client la mise en place d'une solution de contournement économiquement acceptable

Contrat d’adhésion ou de gré à gré ?

Les contrats d’adhésion : régime protecteur des clients (BtoB)

- Code civil :
  - les clauses essentielles figées par l’une ou l’autre des parties qui créent un déséquilibre significatif entre les droits et obligations des parties sont réputées non écrites
  - Le contrat d’adhésion s’interprète contre celui qui l’a proposé
- Code de commerce :
  - Responsabilité du contractant qui tente d’imposer une clause déséquilibrée

Clause essentielle

L’évolution du service / du contrat

- Il peut y avoir une évolution du service, aspects opérationnels sans régression (inhérent au contrat SaaS)
  - ❖ Le contrat renvoie à des documents opérationnels qui peuvent évoluer via des liens URLs et ces documents insérés par référence ont bien valeur contractuelle, à la condition qu'ils aient été portés à la connaissance du co-contractant et qu'ils aient été acceptés par celui-ci.
  - ❖ Un procédé de notification des modifications contractuelles et un délai de préavis doit être prévu au contrat et mis en place pour permettre au client de prendre connaissance (et d’accepter) ces modifications.

- Il ne peut pas y avoir une évolution unilatérale des conditions juridiques et commerciales contractuelles (prix, durée, responsabilité etc.)

Clause essentielle

La suspension du service

- La clause de suspension du service est une spécificité des contrats cloud/SaaS :

❖ Aménagement du principe d'exception d'inexécution des articles 1219 et 1220 du Code civil

- Moyen efficace pour protéger le service d'intrusions tierces menaçant la sécurité
- Moyen efficace pour sanctionner le client qui ne respecterait pas le contrat (règles d'utilisation du service, obligation de payer)

❖ Encadrer la mise en œuvre du principe d'exception d'inexécution

- Prévoir les cas dans lesquels le fournisseur pourra suspendre le service : Attention si service critique pour le client, il peut y avoir interdiction de suspendre ou suspension possible à la condition que manquement suffisamment grave (seuil d'impayés)
- Prévoir l'entendue : suspension limitée ou proportionnée au manquement
- Prévoir des conditions de forme : mise en demeure, préavis

❖ Effet sur d'autres clauses contractuelles : en cas de recours à l'exception d'inexécution par un fournisseur, ses engagements correspondants en termes de disponibilité ou de niveaux de service doivent être suspendus.

Clause essentielle - Vigilance

La suspension des paiements

- Le client peut aussi suspendre le paiement en cas de défaillance du fournisseur
- jurisprudence fréquente : CA Colmar, 1re ch. civ., sect. A, 3 févr. 2020, n° 17/04105
- Préciser que les paiements pourront être suspendus en cas d'inexécution du fournisseur pour les seules prestations inexécutées (et non l'ensemble des prestations, y compris celles correctement exécutées)

Vigilance

L’exécution forcée en nature (C. civ., art. 1221 et 1222)

- La mise en œuvre de l'exécution forcée en nature requiert désormais du créancier une simple mise en demeure préalable et non plus une autorisation judiciaire. En cas d'inexécution et après envoi d'une mise en demeure non suivie d'effet, le client peut donc choisir de faire exécuter l'obligation par un tiers (par exemple un autre prestataire de son choix), et en faire supporter le coût raisonnable au fournisseur défaillant.
- Prévoir d’exclure qu’un concurrent puisse exécuter ses obligations à sa place.
- Prévoir d’exclure son remplacement pour des raisons de confidentialité.

Vigilance

La réduction du prix (C. civ., art. 1223)

- Le client qui n'a pas encore payé tout ou partie des sommes restant dues et estime l'exécution de l'obligation imparfaite peut décider de réduire le prix en notifiant sa décision au fournisseur. Le fournisseur/débiteur pourra soit reconnaître l'inexécution et y remédier dans le délai exigé par la mise en demeure, soit accepter la réduction de prix.
- Le contrat peut librement écarter la mise en demeure de cet article ou au contraire en prévoir les modalités.
- Le contrat peut définir la notion de mauvaise exécution, la soumettre à une procédure d'expertise ou subordonner la réduction du prix à un certain degré d'inexécution.
- Le contrat peut plafonner les montants pouvant donner lieu à réduction, voire identifier les obligations dont la mauvaise exécution pourrait donner droit à une réduction du prix.
- Il convient d’articuler la réduction du prix avec les clauses de pénalités de retard et/ou les niveaux de services.
- L’article peut être exclu.

Clause essentielle

Les métriques de licence

- Le fournisseur confère au client le droit d'utiliser le service, sous réserve du respect de ses conditions d'utilisation
- Les métriques de licence doivent être clairement définies et figées dans le temps
- Le client doit s'assurer que ces conditions sont compatibles avec l'utilisation qu'il compte faire du service
- vérification des métriques de licence
- Licences acquises en quantité suffisante pour l'utilisation envisagée (nombre d'utilisateurs, chiffre d'affaires du client, etc.).
- Le client doit s'assurer que ces conditions sont compatibles avec l'utilisation qu'il compte faire du service
- Evolution du volume d’utilisation ?
- Déterminer les conséquences financières associées ou les conséquences en cas de défaut de mise en conformité
- Déterminer à quel moment le dépassement/la diminution déclenche une facturation ? Si un seul dépassement/diminution déclenche la baisse ou la hausse ? S’il y a rétroactivité ?

Non-respect des termes de la licence

CJUE 18 déc. 2019, IT Development SAS contre Free Mobile SAS, aff. C-666/18

- La Cour a indiqué que la violation d'une clause d'un contrat de licence de logiciel portant sur des droits de propriété intellectuelle relevait de la notion d'« atteinte aux droits de propriété intellectuelle » au sens de la directive 2004/48 et que – par conséquent – ledit titulaire devait pouvoir bénéficier des garanties prévues par cette directive (§42), « indépendamment du régime de responsabilité applicable selon le droit national » (§49).

CA Paris, 19 mars 2021, Orange Business Services / Entre'Ouvert, n°19/17493

- La sanction du non-respect des conditions d'utilisation d'un contrat licence de logiciel relève du régime de la responsabilité contractuelle et non de l'action en contrefaçon

❖ Non respect : non-paiement des redevances, dépassement du nombre d'utilisateurs autorisés, etc.

❖ Cette décision fait perdre à l'éditeur le bénéfice de l'action en contrefaçon ainsi que de l'ensemble des mesures protectrices des directives européennes transposées exclusivement dans le Code de la propriété intellectuelle (procédure de saisie-contrefaçon, droit à l'information, compétence d'une juridiction spécialisée, mode de calcul du préjudice subi…).

❖ Le fournisseur conserve le bénéfice des mesures in futurum de l'article 145 du Code de procédure civile.

❖ Situation différente selon que l'auteur des actes litigieux est susceptible d'invoquer ou non l'existence d'un contrat. Pourtant, dans les deux cas, il y aura bien « atteintes aux droits de propriété intellectuelle ». L'éditeur devrait pouvoir à chaque fois bénéficier des mesures de protection qui lui sont le plus favorables.

❖ Si le fondement de la responsabilité contractuelle venait à être confirmé, les Tribunaux de commerce devraient pouvoir être compétents pour trancher les litiges concernant un droit de propriété intellectuelle. Les titulaires de droits perdraient le bénéficie de voir leur litige tranché par des juges spécialisés.

Etendue de la responsabilité du fournisseur

CA Colmar, 30 septembre 2019, nº 17/04831

- Contrat de mise en œuvre d'une solution SaaS clé en mains (intégration, exploitation, pilotage et assistance, maintenance) : dysfonctionnements/lenteurs, annulation de la commande par le client, demande d'indemnisation du prestataire du fait de la résolution unilatérale

❖ Le Tribunal considère que le prestataire est tenu par une obligation de résultat donc responsable

❖ La CA infirme le jugement : le prestataire est tenu à une obligation de moyens

- Il existe une annexe RACI : Le client avait la responsabilité de la mise en place d'un réseau Internet adapté selon les préconisations du prestataire ; préconisations qui n'ont pas été suivies : aléa et contrainte technologiques relevant de la responsabilité du client.
- Les dysfonctionnements relevant du prestataire ont été corrigés.
- La réparation du préjudice subi par le prestataire : la redevance convenue pour la durée totale du contrat.

Obligation de délivrance conforme et Maintenance règlementaire (paramétrage)

CA Rouen 21 juin 2018 n° 16/05587

- A la suite d'un contrôle, l'Urssaf réclame 87.767 € à titre de régularisation. Le client poursuit alors le fournisseur pour manquement à son devoir de conseil.
- Sa demande est rejetée : en l'absence de stipulation contractuelle en ce sens, le fournisseur d'un logiciel n'a pas l'obligation d'assurer, en cours d'exécution du contrat, le paramétrage du logiciel pour qu'il soit conforme aux évolutions législatives.
- le prestataire a satisfait à son obligation de conseil envers son client lors de la conclusion du contrat ;
- en qualité de professionnel, le fournisseur du logiciel de gestion de paie devait connaître la nécessité d'adapter les fonctionnalités de celui-ci aux nouvelles dispositions de réduction fiscale et l'entreprise cliente, en sa qualité d'employeur, ne pouvait davantage ignorer les nouvelles mesures ;
- dès lors que le contrat souscrit ne prévoyait aucune prestation d'adaptation particulière du logiciel aux besoins réglementaires de l'entreprise ni aucune obligation de veiller à l'actualisation du paramétrage fiscal en cours d'exécution du contrat.

Obligation de délivrance conforme et Maintenance règlementaire (paramétrage)

CA Aix-en-Provence, 7 mai 2019, n° 15/12810

- Le client constate le mauvais paramétrage de son logiciel de paie à l'occasion d'un contrôle URSSAF ayant mis en évidence des erreurs de calcul au regard d'une réforme récente (trop payé).

❖ l'obligation de délivrance conforme d'un logiciel est une obligation de moyens qui est pleinement exécutée lorsqu'il y a mise au point effective du logiciel, sous réserve toutefois que le prestataire ait été mis en mesure, à travers les informations transmises par son client, de réaliser ladite mise au point.

- Les juges rejettent les demandes du client dans la mesure où « les dysfonctionnements à l'origine du trop-payé par [le client] ne sont pas liés à la qualité intrinsèque du progiciel ou à l'utilisation elle-même de l'une ou l'autre fonctionnalité mais à l'introduction, dans le cadre de l'opération de paramétrage, de données comptables ou techniques totalement détachées de toute spécificité informatique et qui relèvent de la connaissance, soit du service comptabilité [du client], soit de [son] service des ressources humaines de sorte que, nanti d'informations erronées transmises par [le client], le paramétrage effectué ne pouvait qu'aboutir aux erreurs constatées par l'URSSAF ».
- Le prestataire ne pouvait atteindre seul l'objectif de paramétrage pertinent du logiciel de paie. Il appartient au client de lui fournir toutes les informations « non seulement nécessaires mais encore fiables », étant précisé que le client ne peut « s'affranchir de [son] obligation de contrôler le travail effectué » par son prestataire.

Clause limitative de responsabilité écartée du fait du caractère dérisoire de l'indemnisation

CA Versailles, 12e chambre, 24 octobre 2019, n° 18/07160

- Contrat de fourniture d'accès à internet et d'un certain débit. Or, les débits constatés par le client étaient largement inférieurs aux engagements formulées, sans que l'assistance technique du prestataire, sollicitée à plusieurs reprises, ne soit en mesure de remédier au problème.
- Les juges constatent l'usage de termes clairs et précis et retiennent l'existence d'une obligation de résultat à la charge du prestataire.
- La Cour écarte l'application de la clause limitative de responsabilité, compte tenu du caractère dérisoire de l'indemnisation qui vide de sa substance l'obligation essentielle du prestataire et l'engagement de résolution des dysfonctionnements sous 4h.

FairSoftware.Cloud : les 10 principes de bonne pratique contractuelle selon le Cigref et le CISPE

- **La charte établie des principes directeurs autour de trois axes : l'amélioration des conditions d'utilisation des logiciels (i), la protection accrue des libertés accordées aux clients (ii) et l'optimisation des coûts liés à l'utilisation du logiciel (iii).**

❖ Nécessité de rendre intelligibles, fiables et pérennes les clauses contractuelles, dont celles relatives aux conditions d'utilisation du logiciel, pour une meilleure compréhension des obligations auxquelles sont tenus les clients (n°1 ; n°8).

❖ La liberté des clients de choisir leur fournisseur de cloud (n°5) et la liberté d'utiliser leurs logiciels chez ce dernier (n°3), et ce, sans qu'ils ne puissent faire l'objet de représailles de la part des éditeurs. Les clients doivent, en outre, être libres d'utiliser dans le cloud les logiciels préalablement acquis (n°2) et bénéficier des standards ouverts et interopérables pour les logiciels d'annuaire (n°6).

❖ Une optimisation des coûts par le biais d'une utilisation efficace du matériel informatique y est également inscrite (n°4). Les éditeurs doivent notamment veiller à assurer une égalité de traitement en ne fixant pas le montant des redevances du logiciel en fonction de son lieu d'installation (n°7). Les éditeurs doivent enfin faire preuve de transparence quant à l'étendue de l'utilisation de la licence octroyée afin de prémunir les clients contre d'éventuels coûts supplémentaires (n°9).

❖ En dernier lieu, la liste pose un principe de continuité de l'assistance, assurée par les éditeurs, lorsque les clients sont autorisés à revendre leur licence de logiciel (n°10).

Premier code de conduite européen dédié aux fournisseurs de services d'infrastructure cloud (IaaS) approuvé par la CNIL

Ce code s'adresse aux fournisseurs de services d'infrastructure cloud situés sur le territoire de l'Union européenne.

- aide les adhérents à démontrer à leurs clients qu'ils répondent aux exigences de l'article 28 du RGPD, qui impose aux responsables de traitement de faire appel uniquement à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées. Une adhésion à ce code de conduite servira d'élément pour démontrer l'existence de ces garanties.
- facilite la mise en conformité opérationnelle au regard des principes du RGPD : comporte une méthode de mise en conformité et des solutions pratiques aux problèmes recensés par les fournisseurs.
- fournit une description détaillée de l'ensemble des bonnes pratiques du secteur.

Effet sur le contrat SaaS :

- le fournisseur SaaS pourra faire référence au code de conduite de son hébergeur adhérent (négociation facilitée)
- procéder aux adaptations qui s'imposent au sein du contrat SaaS (les ajustements contractuels seront limités)
- bien prévoir les modalités de contrôle et de répartition des coûts entre le fournisseur SaaS et son hébergeur
- il y a une prime à la souscription au code de conduite puisque l'article 83, 2, j) du RGPD prévoit une présomption de bonne foi avec effet modérateur sur la sanction à intervenir.

Invalidation du privacy shield : impact

CJUE, 16 juillet 2020, affaire Schrems II

- L'arrêt de la CJUE implique de réexaminer la légalité des transferts de données personnelles à destination des US.
- Le RGPD impose aux exportateurs de données d'évaluer les conditions des transferts et de mettre en place des mesures adaptées pour garantir que les données font l'objet d'une protection substantiellement équivalente à celle garantie dans l'Union européenne.
- L'exportateur de données peut solliciter le destinataire de ces transferts pour vérifier si le droit du pays tiers de destination assure une protection appropriée des données transférées.
- Les responsables de traitement et les sous-traitants transférant des données sont comptables de ces exigences.
- Le recours à des outils d'encadrement des transferts (BCR, clauses contractuelles, etc.) ne dispense pas de cette analyse.
- La CNIL propose une méthode pour identifier les transferts et pour mettre en œuvre un plan d'action adapté : son but est de déterminer si les garanties contenues dans l'outil d'encadrement du transfert (CCT, BCR, etc.) peuvent être respectées dans la pratique ou si le cadre juridique de destination du transfert a pour effet de diminuer ou d'écarter l'application de ces garanties (ex : La législation applicable en matière de renseignement et d'accès des autorités publiques compétentes doit faire l'objet d'un examen particulier).

Invalidation du privacy shield : impact (suite)

- la CJUE a déjà analysé la législation des US en matière d'accès, par les services de renseignement, aux données des fournisseurs de services Internet et entreprises de télécommunications et en a conclu que les atteintes portées à la vie privée des personnes dont les données transitent par ou sont transférées à destination de ces organismes sont disproportionnées au regard des exigences européennes.

- Dès lors, les responsables de traitement et sous-traitants souhaitant transférer des données n'ont pas besoin de procéder à cette évaluation : les transferts soumis à une telle législation doivent être encadrés par des mesures supplémentaires à celles qui figurent dans l'outil de transfert BCR et CCT.

- Trois types de mesures peuvent cumulativement être mises en place afin d'assurer la bonne application des garanties prévues dans l'outil d'encadrement des transferts :

- des mesures techniques : chiffrement ou pseudonymisation des données

- des mesures organisationnelles : pour garantir que le destinataire du transfert ne stockera pas les données reçues auprès de ses filiales si elles se trouvent dans des pays tiers qui ont des législations non conformes aux exigences européennes en matière de surveillance par exemple

- des mesures juridiques : le 4 juin 2021, adoption des nouvelles clauses contractuelles type (Décision d'exécution (UE) 2021/914 de la Commission) à conclure tel quel (clarification des notions différemment conçues dans les droits de l'exportateur et de l'importateur, décrire les mesures techniques ou organisationnelles citées ci-dessus).

Invalidation du privacy shield : impact (suite)

- Les CNIL européennes ont détaillé l'ensemble des mesures supplémentaires susceptibles d'être mises en œuvre pour encadrer les transferts de données à destination d'un Etat n'assurant pas un niveau de protection suffisant. Ces recommandations vont être mises à jour, afin d'aider au mieux les exportateurs de données à assurer la conformité des transferts de données auxquels ils procèdent.

- La méthode de la CNIL https://www.cnil.fr/fr/responsables-de-traitement-comment-identifier-et-traiter-des-transferts-de-donnees-hors-ue complète et précise d'un point de vue opérationnel les principales recommandations du CEPD (mise à jour le 18 juin 2021 : https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf) en vue d'assurer la légalité des transferts de données hors de l'Union européenne.

Clause essentielle

Réversibilité

- Il s’agit de la fin du contrat

❖ Le service cesse et l’obligation de continuité du service cessent

❖ Restitution et effacement des données du client telles qu’elles sont au moment de la restitution : gratuit, support, format de données, délai

❖ Réversibilité du service (si opportun) :

- possibilité pour le client de reprendre ou de faire reprendre la fonction externalisée par le prestataire de son choix
- garantir une réelle assistance lors de la période de migration pour faciliter le transfert à un autre prestataire et/ou la reprise par le client sans modification des conditions et des niveaux de services du contrat.
- Assistance : coût à anticiper.
- Prévoir plan de réversibilité : modalités pratiques et mise à jour au cours du contrat (moyen de sécuriser la relation dans la durée en assurant la formation continue des équipes et le maintien des compétences), clause d’audit de réversibilité.

Merci pour votre attention

Olivia Flipo
Docteur en Droit
Avocat à la Cour

06 83 86 70 03
oflipo@flipo-avocat.com
www.flipo-avocat.com

numeum

Engager
le numérique

numeum.fr