Nations Unies A/CN.9/974

Assemblée générale

Distr. générale
27 juillet 2018
Français
Original : anglais

Commission des Nations Unies pour le droit commercial international
Cinquante-deuxième session
Vienne, 8-26 juillet 2019

Projet d'aide-mémoire sur les principales questions liées aux contrats d'informatique en nuage

Note du Secrétariat

1. À sa cinquante et unième session, en 2018, la Commission a examiné la recommandation du Groupe de travail IV (Commerce électronique) tendant à ce qu'elle examine le projet d'aide-mémoire sur les principales questions liées aux contrats d'informatique en nuage à sa cinquante-deuxième session, en 2019, et en autorise la publication ou la diffusion sous la forme d'un outil de référence en ligne, dans les deux cas comme produit issu des travaux du Secrétariat (A/CN.9/936, par. 44). À l'issue de la discussion, elle a décidé d'examiner le projet d'aide-mémoire à sa cinquante-deuxième session, en 2019[1].

2. Toujours à sa cinquante et unième session, la Commission a prié le Secrétariat de mettre au point, dans la limite des ressources disponibles, un outil en ligne pilote contenant le projet d'aide-mémoire sur les principales questions liées aux contrats d'informatique en nuage, qu'elle examinerait à sa cinquante-deuxième session, en 2019. Elle l'a aussi prié d'élaborer une note récapitulant les considérations relatives à la conception de cet outil, y compris les conséquences budgétaires et autres, ainsi que les changements que cela représenterait par rapport à la politique actuelle de la CNUDCI en matière de publication[2].

3. L'annexe à la présente note contient le texte du projet d'aide-mémoire sur les principales questions liées aux contrats d'informatique en nuage, tel qu'il a été établi par le secrétariat de la CNUDCI. Les termes apparaissant en caractères gras dans le projet d'aide-mémoire sont définis dans le glossaire figurant à la fin du document. Une note du Secrétariat concernant un outil en ligne pilote contenant le projet d'aide-mémoire sera soumise séparément, sous la cote A/CN.9/975.

---

[1] *Documents officiels de l'Assemblée générale, soixante-treizième session, Supplément nº 17* (A/73/17), par. 150.

[2] Ibid., par. 155.

Annexe

Aide-mémoire sur les principales questions liées aux contrats d'informatique en nuage (établi par le secrétariat de la Commission des Nations Unies pour le droit commercial international, 2019)

Table des matières

Introduction

1. Le présent aide-mémoire aborde les principales questions liées aux contrats d'informatique en nuage conclus entre des entités commerciales dans lesquels une partie (le fournisseur) fournit à l'autre partie (le client) un ou plusieurs **services d'informatique en nuage** à des fins d'utilisation finale. Les contrats prévoyant la revente ou d'autres formes de redistribution de ces services sont exclus de la portée de l'aide-mémoire, de même que les contrats conclus avec des **partenaires de services d'informatique en nuage** ou d'autres tiers qui peuvent participer à la fourniture de ces services au client (par exemple, contrats passés avec des sous-traitants ou des fournisseurs de services Internet).

2. Selon la loi applicable, les contrats d'informatique en nuage pourront être qualifiés de contrat de service, de location, de sous-traitance, de licence, de contrat mixte ou autre. Les exigences légales relatives à la forme et au contenu de ces contrats peuvent varier en conséquence. Dans certains pays, les parties peuvent elles-mêmes, dans le contrat, en qualifier le type lorsque la législation ne dit rien, ou reste vague à ce sujet. Le tribunal tiendra compte de cette qualification pour interpréter les termes du contrat, à moins que cela ne soit contraire à la législation, à la pratique judiciaire, à la véritable intention des parties, à la situation de fait ou aux coutumes ou pratiques commerciales.

3. Les questions abordées dans le présent aide-mémoire peuvent se poser en relation avec des contrats d'informatique en nuage, indépendamment du type de **services d'informatique en nuage** qu'ils concernent (par exemple, **infrastructure en tant que service** (**IaaS**), **plateforme en tant que service** (**PaaS**) ou **logiciel en tant que service** (**SaaS**)), de leur **modèle de déploiement** (par exemple, **public**, **communautaire**, **privé** ou **hybride**) et des conditions de paiement (contre ou sans rémunération). L'aide-mémoire met avant tout l'accent sur les contrats d'informatique en nuage public de type **SaaS** prévoyant une rémunération.

4. La capacité de négocier des clauses contractuelles d'informatique en nuage dépendra de nombreux facteurs, en particulier de la question de savoir si le contrat prévoit des **solutions d'informatique en nuage normalisées pour multiabonnés** ou des solutions individuelles sur mesure, de l'existence ou non d'offres concurrentes, et du pouvoir de négociation des éventuelles parties. La capacité de négocier les termes d'un contrat, en particulier les clauses relatives à la suspension, à la résiliation ou à la modification unilatérale du contrat par le fournisseur, ainsi que les clauses de responsabilité, peut représenter un facteur important dans le choix d'un fournisseur, lorsqu'un tel choix existe. S'il a été établi principalement à l'intention des parties négociant un contrat d'informatique en nuage, l'aide-mémoire pourrait aussi être utile aux clients qui examinent les conditions générales proposées par des fournisseurs pour déterminer si elles correspondent véritablement à leurs besoins.

5. L'aide-mémoire ne devrait pas être considéré comme une source exhaustive d'informations pour la rédaction de contrats d'informatique en nuage, ni comme un substitut à l'obtention de conseils et de services juridiques et techniques auprès de conseillers professionnels. Il vise plutôt à présenter les aspects que d'éventuelles parties devraient prendre en considération avant et pendant la rédaction d'un contrat, sans toutefois donner à entendre que l'ensemble de ces aspects doit systématiquement être examiné. Les différentes solutions proposées dans l'aide-mémoire ne régiront pas la relation entre les parties, à moins que celles-ci n'en conviennent expressément, ou que ces solutions ne résultent de dispositions de la loi applicable. Le libellé, ainsi que l'ordre dans lequel apparaissent les titres et sous-titres utilisés dans l'aide-mémoire, ne doivent pas être considérés comme étant obligatoires, ni comme indiquant une préférence de structure ou de style pour les contrats d'informatique en nuage. La forme, le contenu, le style et la structure des contrats d'informatique en nuage peuvent sensiblement varier en fonction des traditions juridiques, des styles rédactionnels, des exigences légales et des besoins et préférences des parties.

6. L'aide-mémoire n'entend pas refléter l'opinion de la Commission des Nations Unies pour le droit commercial international (CNUDCI), ni de son secrétariat, en ce qui concerne l'opportunité de conclure des contrats d'informatique en nuage.

7. L'aide-mémoire se présente en deux parties, suivies d'un glossaire. La première partie porte sur les principaux aspects précontractuels que les parties voudront peut-être examiner avant de conclure un tel contrat. La seconde porte sur les principales difficultés contractuelles que les parties peuvent rencontrer lorsqu'elles rédigent un tel contrat. Quant au glossaire, il décrit certains termes techniques utilisés dans l'aide-mémoire afin d'en faciliter la compréhension.

Première partie. Principaux aspects précontractuels

A. Vérification des dispositions de droit impératif et autres exigences

8. Le cadre juridique applicable au client, au fournisseur ou aux deux peut imposer des conditions pour la conclusion d'un contrat d'informatique en nuage. Ces conditions peuvent aussi provenir d'engagements contractuels, comme des **licences de propriété intellectuelle**. Les parties devraient en particulier avoir connaissance des lois et règlements relatifs aux **données personnelles**, à la cybersécurité, au contrôle des exportations, aux douanes, aux impôts et aux secrets commerciaux**,** ainsi que des règlements relatifs à la propriété intellectuelle et des **règlements sectoriels** qui peuvent leur être applicables, ainsi qu'à tout contrat qu'elles pourront conclure. La non-observation de conditions impératives peut avoir de graves conséquences, comme la nullité ou le caractère non-exécutoire de tout ou partie d'un contrat, des pénalités administratives ou la responsabilité pénale.

9. Les conditions de conclusion d'un contrat d'informatique en nuage peuvent varier selon le secteur et le pays concernés. Elles peuvent notamment concerner l'obligation de prendre des mesures spéciales pour assurer la protection des **droits des sujets de données**, de déployer un modèle particulier (par exemple, **nuage privé** plutôt que **public**), de chiffrer les données placées dans le nuage et d'enregistrer auprès des autorités publiques une transaction ou un logiciel utilisé dans le **traitement de données personnelles**. Elles peuvent aussi comprendre des exigences en matière de **localisation des données**, ainsi que des exigences concernant le fournisseur.

Localisation des données

10. Les **exigences en matière de localisation des données** peuvent en particulier découler de la loi applicable aux données personnelles, aux données comptables et aux données du secteur public, de la législation sur le contrôle des exportations et des règlements susceptibles de limiter le transfert de certains logiciels ou informations en provenance ou à destination de certains pays ou régions. Il est essentiel, pour les parties, de se conformer aux exigences en matière de localisation des données énoncées dans la loi applicable. Le contrat ne pourra pas ne pas en tenir compte.

11. Ces exigences peuvent aussi découler d'engagements contractuels de tiers, comme des **licences de propriété intellectuelle** prévoyant par exemple, que le contenu sous licence doit être stocké sur les serveurs sécurisés de l'utilisateur. La **localisation des données** peut en outre être privilégiée à des fins purement pratiques, par exemple pour diminuer le **temps de latence**, ce qui est surtout important pour les opérations en temps réel comme le négoce en bourse. (En ce qui concerne les garanties contractuelles relatives à la localisation des données, voir deuxième partie, par. 74, 75 et 78).

Choix d'une partie contractante

12. Le choix d'une partie contractante peut être limité, outre par les conditions du marché, par des exigences légales. Ainsi, il peut être interdit par la loi de conclure un contrat d'informatique en nuage avec des personnes étrangères, des ressortissants de certains pays ou des personnes non accréditées/certifiées auprès des autorités publiques compétentes. La loi peut exiger qu'une personne étrangère constitue une coentreprise avec une entité nationale ou acquière des licences et autorisations locales, y compris des autorisations d'exportation, pour fournir des **services d'informatique en nuage** dans un pays donné. Le choix d'une partie contractante peut aussi être influencé par les exigences en matière de **localisation des données** (voir par. 10 et 11 ci-avant), ainsi que par les obligations imposées par la loi à chaque partie de divulguer les données et autres contenus, ou de donner accès à ceux-ci, aux autorités publiques d'autres États.

B. Évaluation précontractuelle des risques

13. Les dispositions de droit impératif peuvent exiger qu'il soit procédé à une évaluation des risques avant la conclusion d'un contrat d'informatique en nuage. Même en l'absence d'exigences légales, les parties peuvent décider de procéder à une telle évaluation en vue de définir une stratégie de réduction des risques, y compris la négociation de clauses contractuelles adéquates.

14. Tous les risques inhérents à un contrat d'informatique en nuage ne sont pas spécifiquement liés au nuage. Certains seront abordés en dehors d'un contrat d'informatique en nuage (par exemple, les risques liés à une interruption de la connectivité en ligne) et tous ne pourront pas être limités à un coût acceptable (par exemple, une atteinte à la réputation). De plus, l'évaluation des risques ne se résume pas à une étape unique avant la conclusion d'un contrat. Elle peut se poursuivre pendant la durée d'existence du contrat, et ses résultats peuvent entraîner la modification, voire la résiliation du contrat.

Vérification des informations relatives à un service d'informatique en nuage particulier et à la partie contractante sélectionnée

15. Les informations suivantes peuvent être pertinentes pour les parties lorsqu'elles envisagent de recourir à un **service d'informatique en nuage** particulier et de sélectionner une partie contractante :

a) Les **licences de propriété intellectuelle** requises pour utiliser un service d'informatique en nuage particulier ;

b) La politique existante en matière de protection de l'information, de confidentialité et de sécurité, en particulier en ce qui concerne la prévention des accès non autorisés, l'utilisation, l'altération ou la destruction des données pendant leur traitement, leur transit ou leur transfert au moyen de l'infrastructure d'informatique en nuage ;

c) Les mesures mises en place pour assurer l'accès continu aux **métadonnées**, aux journaux d'audit et à d'autres journaux attestant des mesures de sécurité ;

d) Le plan existant de reprise après sinistre et les obligations de notification en cas d'atteinte à la sécurité ou de dysfonctionnement du système ;

e) Les politiques adoptées en ce qui concerne la migration vers le nuage et l'assistance à la fin du contrat, ainsi que l'**interopérabilité** et la **portabilité** ;

f) Les mesures existantes pour effectuer des vérifications au sujet des employés, sous-traitants et autres tiers impliqués dans la fourniture des services d'informatique en nuage, ainsi que les former ;

g) Des statistiques relatives aux **incidents de sécurité** et des informations relatives aux expériences faites avec les procédures de reprise après sinistre ;

h) La certification de conformité aux normes techniques par un tiers indépendant ;

i) Des informations concernant la régularité et la portée des audits effectués par un organe indépendant ;

j) La viabilité financière ;

k) Les polices d'assurance ;

l) D'éventuels conflits d'intérêts ;

m) Le volume de la sous-traitance et des **services d'informatique en nuage en couches** ; et

n) La mesure dans laquelle est assuré l'isolement des données et autres contenus dans l'infrastructure d'informatique en nuage.

Risque d'atteinte à la propriété intellectuelle

16. Il peut exister un risque d'atteinte à la propriété intellectuelle lorsque, par exemple, le fournisseur n'est ni le propriétaire ni le concepteur des ressources fournies à ses clients, qu'il utilise en vertu d'un contrat de **licence de propriété intellectuelle** conclu avec un tiers. Un tel risque peut aussi survenir lorsque le client est tenu, pour l'exécution du contrat, d'autoriser le fournisseur à utiliser le contenu qu'il souhaite placer dans le nuage. Dans certains pays, le stockage de contenu dans le nuage, même à des fins de sauvegarde, peut être qualifié de reproduction et exiger une autorisation préalable du propriétaire des droits de propriété intellectuelle.

17. Il est de l'intérêt des deux parties de s'assurer, avant la conclusion du contrat, que l'utilisation des services d'informatique en nuage ne portera pas atteinte aux droits de propriété intellectuelle et ne constituera pas un motif de retrait des licences de propriété intellectuelle qui leur auront été accordées. Le coût d'une atteinte à la propriété intellectuelle peut être très élevé. Il faudra peut-être prévoir le droit de conclure une sous-licence, ou envisager une licence directe avec le donneur de licence concerné, qui conférera le droit de gestion des licences. Pour pouvoir utiliser des logiciels ou autres contenus libres, il peut être nécessaire d'obtenir au préalable le consentement des tiers concernés et de divulguer le code source avec toute modification apportée au logiciel ou autre contenu libre.

Risques en matière de sécurité, d'intégrité, de confidentialité et de protection des données

18. Avec la migration de tout ou partie de ses données vers le nuage, le client perd le contrôle exclusif sur ces données et sa capacité de déployer les mesures nécessaires pour garantir l'intégrité et la confidentialité des données, ou pour vérifier si le traitement et la conservation des données sont assurés de manière adéquate. La portée de cette perte de contrôle dépendra du type de **service d'informatique en nuage** concerné.

19. En raison de certaines caractéristiques inhérentes aux **services d'informatique en nuage**, comme le **large accès via le réseau**, l'**architecture multilocataire** et la **mutualisation des ressources**, les parties pourront devoir prendre plus de précautions pour empêcher l'interception des communications et autres cyberattaques, qui peuvent entraîner la perte ou la compromission des identifiants permettant d'accéder aux services d'informatique en nuage, une perte de données et d'autres atteintes à la sécurité. Des mesures adéquates d'isolement des ressources et de ségrégation des données, ainsi que des procédures de sécurité efficaces sont particulièrement importantes dans un environnement partagé comme l'informatique en nuage.

20. Les mesures de sécurité sont la responsabilité partagée des parties dans un environnement d'informatique en nuage, indépendamment du type de services d'informatique en nuage utilisés. L'évaluation précontractuelle des risques est l'occasion pour les parties de définir, sans aucune ambiguïté, leurs rôles et responsabilités en ce qui concerne la sécurité, l'intégrité, la confidentialité et la protection des données. Les clauses contractuelles jouent un rôle important en ce qu'elles traduisent l'accord des parties au sujet de la répartition, entre elles, des risques et des responsabilités liés à ces aspects, et à d'autres aspects de la fourniture de services d'informatique en nuage (voir deuxième partie, par. 125 à 137). Ces clauses ne sauraient toutefois primer sur les règles de droit impératives.

Tests d'intrusion, audits et inspections physiques

21. Des mesures peuvent être prises au stade précontractuel pour vérifier si l'isolement des ressources et la ségrégation des données, les procédures d'identification et les autres mesures de sécurité sont adéquats. Ces vérifications devraient viser à déterminer si les parties doivent prendre des précautions

supplémentaires pour prévenir les atteintes à la sécurité des données et d'autres dysfonctionnements dans la fourniture des services d'informatique en nuage au client.

22. Les lois et règlements peuvent exiger la tenue d'**audits**, de tests d'intrusion et l'inspection physique des centres de données impliqués dans la fourniture des **services d'informatique en nuage**, afin en particulier de déterminer si leur emplacement satisfait bien aux exigences légales en matière de **localisation des données** (voir par. 10 et 11 ci-dessus). Les parties devront convenir des conditions relatives à ces vérifications, notamment en ce qui concerne le moment où elles seront entreprises, la répartition des coûts et l'indemnisation en cas de dommage causé par ces vérifications.

Risque de verrouillage

23. La capacité d'éviter ou de réduire le risque de **verrouillage**, qui est souvent lié au manque d'**interopérabilité** et de **portabilité**, est peut-être l'une des considérations les plus importantes pour les parties. Ce risque pourra être plus important avec un contrat à long terme ou avec un contrat à court ou moyen terme automatiquement renouvelable.

24. Le risque de verrouillage des applications et des données est particulièrement élevé pour les modèles **SaaS** et **PaaS**. Les données peuvent exister dans des formats spécifiques à un système d'informatique en nuage, qui ne seront pas utilisables dans d'autres systèmes. De plus, l'utilisation d'une application ou d'un système propriétaire pour l'organisation des données pourra nécessiter que l'on ajuste les conditions de licence pour permettre l'exploitation dans un autre réseau. Il pourra être nécessaire de réécrire les programmes d'interaction avec les interfaces de programmation d'applications (API) pour tenir compte de l'API du nouveau système. La mise à niveau des connaissances des utilisateurs finaux peut aussi s'avérer coûteuse.

25. Dans le modèle **PaaS**, il y a aussi un risque de verrouillage des logiciels d'exécution puisque ces derniers (à savoir les logiciels conçus pour permettre l'exécution de programmes informatiques écrits dans un langage de programmation spécifique) sont souvent fortement personnalisés (par exemple, pour des aspects tels que l'allocation ou la libération de mémoire, le débogage, etc.). Dans le modèle **IaaS**, si le risque de verrouillage varie en fonction des services d'infrastructure consommés, le client peut également être confronté au verrouillage des applications en cas de dépendance face à certaines caractéristiques de la politique du fournisseur (par exemple, les contrôles d'accès) ou au verrouillage des données en cas de déplacement de données supplémentaires vers le nuage à des fins de stockage.

26. Au stade précontractuel, il est possible d'effectuer des essais pour vérifier si les données et autres contenus peuvent être exportés vers un autre système et y être utilisés. Il peut être nécessaire d'assurer la synchronisation entre le nuage et les plateformes internes et la reproduction des données en un autre lieu. La négociation avec plusieurs parties et le choix d'une combinaison de divers types de **services d'informatique en nuage**, avec leur propre **modèle de déploiement** (par exemple, sources d'approvisionnement multiples), peuvent être des éléments clefs de la stratégie visant à atténuer les risques de **verrouillage**, même s'ils peuvent entraîner des coûts et d'autres conséquences. Les clauses contractuelles peuvent aussi contribuer à limiter ces risques (voir deuxième partie, en particulier par. 84, 85 et 143).

Risques concernant la continuité des opérations

27. Les parties pourront se préoccuper de la continuité des opérations en relation non seulement avec la fin programmée du contrat, mais aussi une éventuelle suspension unilatérale ou résiliation anticipée, notamment si l'une ou l'autre partie cesse ses activités. La législation pourra exiger la mise au point, en amont, d'une stratégie appropriée pour assurer la continuité des opérations, et notamment pour éviter les incidences négatives de la cessation ou de la suspension des services sur les

utilisateurs finaux. L'élaboration de clauses contractuelles pourra aussi contribuer à limiter les risques en la matière (voir deuxième partie, par. 114, 115, 153, 173 et 182).

Stratégies de retrait

28. Pour garantir le succès de la stratégie de retrait, les parties pourront devoir déterminer dès le début : a) le contenu à retirer (par exemple, uniquement les données que le client aura entrées dans le nuage ou aussi les **données dérivées des services en nuage**) ; b) les modifications qu'il conviendra d'apporter aux **licences de propriété intellectuelle** pour pouvoir continuer d'utiliser ledit contenu dans un autre système ; c) le contrôle des clefs de déchiffrement et l'accès à ces dernières ; et d) le délai requis pour achever le retrait. Les clauses contractuelles relatives à la fin du contrat traduisent généralement l'accord des parties sur ces points (voir deuxième partie, par. 157 à 167).

C. Autres questions précontractuelles

Divulgation d'informations

29. La loi applicable peut exiger d'éventuelles parties à un contrat qu'elles se fournissent mutuellement les informations nécessaires pour décider en toute connaissance de cause si elles souhaitent ou non conclure ledit contrat. L'absence de communication, ou en tout cas de communication claire, à l'autre partie d'informations permettant de satisfaire à cette obligation avant la conclusion d'un contrat peut entraîner la nullité, en tout ou en partie, du contrat ou fonder la partie lésée à réclamer des dommages-intérêts.

30. Dans certains pays, les informations précontractuelles peuvent être considérées comme faisant partie intégrante du contrat. Dans ce cas, les parties devront veiller à ce que celles-ci soient correctement enregistrées et que toute incohérence entre ces informations et le contrat même soit évitée. Elles devront aussi se préoccuper des incidences de ces informations divulguées avant la conclusion du contrat en matière de flexibilité et d'innovation pendant la phase d'exécution du contrat.

Confidentialité

31. Certaines des informations divulguées avant la conclusion du contrat peuvent être jugées confidentielles (en particulier celles ayant trait aux mesures de sécurité, d'identification et d'authentification, aux sous-traitants et à l'emplacement et au type de centres de données, ces dernières pouvant permettre d'identifier le type de données qui y sont enregistrées et les modalités d'accès des autorités publiques, qu'elles soient locales ou étrangères). Les parties peuvent convenir que certaines informations divulguées avant la conclusion du contrat doivent être traitées comme des données confidentielles. Des engagements écrits de confidentialité ou des accords de non-divulgation pourront également être exigés des tiers impliqués dans les vérifications précontractuelles (par exemple, auditeurs).

Migration vers le nuage

32. Avant d'effectuer la migration vers le nuage, le client devra généralement classer les données à migrer et les protéger en fonction de leur caractère sensible ou critique, et indiquer au fournisseur le niveau de protection exigé pour chaque type de données. Il sera peut-être aussi censé lui communiquer d'autres informations nécessaires pour la fourniture de services (par exemple, le calendrier de conservation et d'élimination de ses données, les mécanismes de gestion des identités et des accès et les procédures d'accès, le cas échéant, aux clefs de déchiffrement).

33. Outre le transfert des données et autres contenus vers le nuage du fournisseur, la migration vers le nuage peut aussi impliquer des opérations d'installation, de configuration, de chiffrement, des tests et la formation du personnel et des autres utilisateurs finaux du client. Ces aspects peuvent faire partie du contrat passé avec le

fournisseur ou faire l'objet d'un accord distinct passé avec le fournisseur ou des tiers, notamment des **partenaires de services d'informatique en nuage**. Des dépenses supplémentaires peuvent être engagées. Les parties impliquées dans la migration s'entendront généralement sur leurs rôles et responsabilités respectifs pendant la migration, les conditions de leur engagement, le format dans lequel les données et autres contenus seront migrés vers le nuage, le calendrier de la migration, une procédure d'acceptation pour attester de sa bonne exécution et d'autres détails relatifs au plan de migration.

Deuxième partie. Rédaction d'un contrat

A. Considérations générales

Liberté contractuelle

34. Le principe de la liberté contractuelle, largement reconnu dans les relations commerciales, permet aux parties de conclure un contrat et d'en déterminer le contenu. Cette liberté peut être restreinte par la législation relative aux conditions non négociables applicable à certains types de contrats ou par des règles qui sanctionnent l'abus de droits et les atteintes à l'ordre public, à la moralité, etc. Les conséquences du non-respect de ces restrictions peuvent aller du caractère non exécutoire de tout ou partie d'un contrat à une responsabilité civile, administrative ou pénale.

Formation du contrat

35. Les concepts d'offre et d'acceptation de l'offre sont traditionnellement utilisés pour déterminer si et à quel moment les parties se sont entendues sur leurs droits et obligations respectifs, qui les lieront pendant toute la durée du contrat. La loi applicable peut exiger que certaines conditions soient remplies pour que la proposition de conclusion du contrat constitue une offre définitive et irrévocable (par exemple, cette proposition doit indiquer de manière suffisamment précise les services d'informatique en nuage couverts et les conditions de paiement).

36. Le contrat est conclu lorsque l'acceptation de l'offre devient effective. Il peut exister divers mécanismes d'acceptation (par exemple, le client coche une case sur une page Web, il s'enregistre en ligne pour un service d'informatique en nuage, ou il commence à utiliser un service ou à payer une commission ; le fournisseur commence ou continue de fournir des services ; les deux parties signent un contrat en ligne ou sur papier). Lorsque des modifications importantes sont apportées à l'offre (par exemple, concernant les responsabilités, la qualité et la quantité de services à fournir ou les conditions de paiement), cela peut constituer une contre-offre, qui devra être acceptée par l'autre partie pour que le contrat soit conclu.

37. Les **solutions d'informatique en nuage normalisées pour multiabonnés** sont généralement offertes par le biais d'applications interactives (par exemple, accords par clic). Dans ce cas, il y aura souvent très peu, voire pas, de marge de manœuvre pour négocier et ajuster l'offre standard. Pour conclure un tel contrat, il suffit de cliquer sur la mention « J'accepte », « OK » ou « Je suis d'accord ». Lorsqu'un contrat est négocié, la formation du contrat peut résulter d'une série d'étapes, notamment l'échange préliminaire d'informations, les négociations, la remise et l'acceptation d'une offre et la préparation du contrat.

Forme du contrat

38. Les contrats d'informatique en nuage sont généralement conclus en ligne. Ils peuvent s'intituler différemment (accords de services d'informatique en nuage, accords-cadres de services, ou conditions de service) et comprendre un ou plusieurs documents, comme une **politique d'utilisation acceptable**, un **accord de niveau de service**, un accord de traitement des données ou une politique de protection des données, une politique en matière de sécurité et un accord de licence.

39. Les règles législatives applicables aux contrats d'informatique en nuage peuvent exiger que le contrat soit conclu par **écrit**, surtout lorsqu'il implique le **traitement de données personnelles**, et que tous les documents qui y sont mentionnés soient joints au contrat-cadre. Même lorsque la forme **écrite** n'est pas requise, les parties peuvent décider, par souci de commodité, de clarté et d'exhaustivité, ainsi qu'afin d'assurer l'exécution et l'efficacité du contrat, de conclure celui-ci par **écrit**, en lui incorporant tous les accords accessoires.

40. La loi applicable peut exiger la signature du contrat sur papier à des fins spécifiques, notamment fiscales, même si ce type d'exigence se rencontre de plus en plus rarement dans l'environnement dématérialisé.

Définitions et terminologie

41. Compte tenu de la nature des **services d'informatique en nuage**, les contrats y relatifs contiennent nécessairement de nombreux termes techniques. On pourra inclure un glossaire dans le contrat, ainsi que des définitions des principaux termes qui y sont utilisés, afin d'éviter toute ambiguïté dans leur interprétation. Les parties voudront peut-être envisager d'utiliser la terminologie établie à l'échelle internationale pour assurer la cohérence et la clarté juridique du texte.

Contenu minimal du contrat

42. Un contrat devra normalement : a) désigner les parties contractantes ; b) définir son objet et sa portée ; c) préciser les droits et obligations des parties, y compris les conditions de paiement ; d) établir la durée du contrat et les conditions de résiliation et de renouvellement ; e) prévoir des recours en cas de rupture du contrat et des exemptions de responsabilité ; et f) prévoir les effets de la résiliation du contrat. Il contient aussi généralement des clauses relatives au règlement des litiges et au choix de la loi et du for.

B. Désignation des parties contractantes

43. La désignation correcte des parties au contrat peut avoir des incidences directes sur la formation et l'exécution du contrat. La loi applicable précisera les informations requises pour déterminer la personnalité juridique d'une entité commerciale et sa capacité de conclure un contrat. La législation pourra exiger des renseignements supplémentaires à des fins spécifiques, par exemple un numéro d'identification fiscal ou une procuration pour déterminer la capacité d'une personne physique de signer et de s'engager pour le compte d'une personne morale.

C. Définition de l'objet et de la portée du contrat

44. Les contrats d'informatique en nuage varient sensiblement, de par le type et la complexité de leur objet, compte tenu de la diversité des **services d'informatique en nuage** concernés. Cet objet peut changer au cours de la durée d'un contrat : certains services pourront être annulés et d'autres ajoutés. Il peut prévoir la fourniture de services de base, auxiliaires et optionnels.

45. L'indication de l'objet du contrat contient généralement une description du type de services d'informatique en nuage (**SaaS**, **PaaS**, **IaaS** ou combinaison de ceux-ci), de leur **modèle de déploiement** (**public**, **communautaire**, **privé** ou **hybride**), de leurs caractéristiques techniques, en termes de qualité et de performance et de toute norme technique applicable. Plusieurs documents qui constituent le contrat peuvent entrer en ligne de compte pour en déterminer l'objet (voir par. 38 ci-avant).

Accord de niveau de service

46. L'**accord de niveau de service** définit les **paramètres de performance** à l'aide desquels la fourniture des services d'informatique en nuage et la portée des obligations contractuelles et d'une éventuelle rupture du contrat par le fournisseur seront mesurées. Des informaticiens interviennent normalement dans la formulation des **paramètres de performance**.

47. Les paramètres de performance quantitatifs concernent généralement la capacité (capacité donnée de stockage de données ou quantité donnée de mémoire disponible pour le programme en cours), le **temps d'arrêt** ou **d'interruption**, le **temps de latence**, la **pérennité du stockage de données**, le **temps de disponibilité**, les services

d'assistance (par exemple, pendant les horaires de bureau du client ou 24 heures sur 24 et 7 jours sur 7) et les plans de gestion des incidents et des sinistres et plans de reprise. Ces derniers peuvent comprendre le temps maximum de résolution des incidents, le **temps** maximum **de réaction initiale**, l'**objectif de point de reprise** et l'**objectif de délai de reprise**.

48. Les paramètres de performance qualitatifs peuvent concerner la **suppression des données**, les **exigences en matière de localisation des données**, la **portabilité**, la sécurité et la protection des données/confidentialité. Certains aspects des services peuvent être mesurés à l'aune de paramètres de performance tant qualitatifs que quantitatifs. Ainsi, l'**élasticité** et l'**extensibilité** peuvent être définies par rapport soit aux ressources maximales disponibles pendant une période minimum spécifiée, soit à la qualité et à la sécurité des mesures susceptibles d'être adaptées aux différents niveaux de sensibilité des données client stockées. Le chiffrement peut être exprimé sous la forme d'un nombre donné de bits pour les données au repos, en transit et en utilisation. En plus ou à la place de ce paramètre quantitatif, on peut aussi mesurer le chiffrement à l'aune d'un paramètre qualitatif (par exemple, le fournisseur doit s'assurer que les données des clients sont chiffrées lorsqu'elles sont transportées par un réseau de communication public et lorsqu'elles sont au repos dans des centres de données utilisés par le fournisseur).

49. On pourra convenir de divers engagements (par exemple, obligations de résultats ou de moyens) en fonction, notamment, des conditions de paiement et de l'existence ou non de **solutions normalisées pour multiabonnés**. Le type d'engagement aura des implications, notamment en ce qui concerne la charge de la preuve en cas de litige.

Mesure de la performance

50. Les parties peuvent prévoir dans le contrat une méthode et des procédures de mesure, et définir en particulier la période de référence choisie pour mesurer les services (quotidienne, hebdomadaire, mensuelle, etc.), les mécanismes de communication d'informations relatives à la fourniture des services (c'est-à-dire la fréquence et la forme de cette communication), les rôles et responsabilités des parties et le type de mesures à effectuer (par exemple, mesure au moment de la fourniture ou de la consommation des services). Les parties pourront s'entendre sur un mécanisme indépendant de mesure de la performance et la répartition des frais y relatifs.

51. Le client s'intéresse normalement aux mesures effectuées pendant les heures de pointe, c'est-à-dire au moment où les services sont le plus nécessaire. Il est généralement à même de mesurer – ou de vérifier les mesures fournies par le fournisseur ou un tiers – les données chiffrées reflétant la performance du système au moment de la consommation, mais pas celles reflétant la performance au moment de la fourniture des services. Il pourra peut-être évaluer ces dernières à partir des rapports sur la performance communiqués par le fournisseur ou un tiers. Le fournisseur pourra accepter de fournir de tels rapports à la demande du client, à un rythme régulier (quotidien, hebdomadaire, mensuel, etc.) ou à la suite d'un incident particulier. Il pourra aussi autoriser le client à examiner ses données relatives à l'évaluation du niveau de service. Certains fournisseurs autorisent leurs clients à suivre les données relatives à la performance du service en temps réel.

52. Le contrat pourra obliger l'une des parties, voire les deux, à conserver les données relatives à la fourniture et à la consommation de services pendant une certaine durée. Ces informations peuvent être utiles pour négocier tout changement à apporter au contrat ou en cas de litige.

Politique d'utilisation acceptable

53. La **politique d'utilisation acceptable** définit les conditions de l'utilisation, par le client et ses utilisateurs finaux, des services d'informatique en nuage visés par le contrat. Elle entend protéger le fournisseur contre toute responsabilité découlant de la conduite de ses clients et de leurs utilisateurs finaux. Tout client potentiel devra

accepter cette politique, qui fera partie du contrat passé avec le fournisseur. La grande majorité des politiques standard interdisent toute une série d'activités dont les fournisseurs considèrent qu'elles constituent une utilisation abusive ou illégale des **services d'informatique en nuage**. Les **politiques d'utilisation acceptable** peuvent restreindre non seulement le type de contenus susceptibles d'être placés dans le nuage, mais aussi le droit du client de donner accès aux données et autres contenus envoyés dans le nuage à des tiers (par exemple, des ressortissants de certains pays ou des personnes figurant sur des listes de sanctions). Les parties peuvent convenir d'écarter certaines interdictions pour tenir compte des besoins commerciaux spécifiques du client, dans les limites autorisées par la loi.

54. Les conditions générales du fournisseur prévoient habituellement que les utilisateurs finaux du client doivent aussi observer la **politique d'utilisation acceptable** et que le client doit déployer ses meilleurs efforts ou des efforts commercialement raisonnables pour en assurer le respect. Certains fournisseurs peuvent exiger des clients qu'ils empêchent activement tout usage non autorisé ou abusif par des tiers des services d'informatique en nuage offerts au titre du contrat. Les parties pourront s'entendre sur des obligations limitées, par exemple en prévoyant que le client communique la **politique d'utilisation acceptable** aux utilisateurs finaux connus, n'autorise pas, ni ne permet en connaissance de cause, de tels usages, et notifie au fournisseur tout usage non autorisé ou abusif dont il aura connaissance.

55. Dans un petit nombre de pays, la loi peut imposer au fournisseur des devoirs en ce qui concerne les contenus hébergés sur son infrastructure d'informatique en nuage, par exemple l'obligation de signaler la présence de contenus illicites aux autorités publiques. Il se peut que ces obligations ne puissent pas être transférées au client ou aux utilisateurs finaux par la **politique d'utilisation acceptable** ou autrement. Elles peuvent avoir des incidences sur la confidentialité, entre autres, et comptent parmi les facteurs à prendre en compte pour choisir un fournisseur adéquat (voir première partie, par. 12).

Politique de sécurité

56. La sécurité du système, y compris celle des données du client, implique un partage des responsabilités des parties. Le contrat précisera les rôles et responsabilités de chaque partie dans ce domaine, en tenant compte des obligations qui peuvent leur être imposées par les dispositions de droit impératif.

57. Habituellement, le fournisseur suit sa propre politique en matière de sécurité. Dans certains cas, il sera peut-être possible de s'accorder pour qu'il suive la politique du client en la matière. Ceci n'est toutefois pas possible pour les **solutions d'informatique en nuage normalisées pour multiabonnés**. Le contrat pourra prévoir des mesures de sécurité précises (par exemple, exigences de nettoyage ou de suppression des données dans un support endommagé, stockage de paquets de données séparés à différents endroits, stockage des données du client sur du matériel spécifique qui lui est propre). La divulgation excessive d'informations concernant la sécurité dans le contrat peut toutefois poser un risque.

58. Certaines mesures de sécurité ne nécessitent pas la contribution de l'autre partie, et portent exclusivement sur les activités habituelles de la partie concernée, par exemple les inspections, par le fournisseur, du matériel sur lequel les données sont stockées et les services sont fournis, et la prise de mesures efficaces pour assurer un accès contrôlé à celui-ci. Dans d'autres cas, pour permettre à la partie concernée de remplir ses obligations ou d'évaluer et de contrôler la qualité des mesures de sécurité mises en œuvre, l'intervention de l'autre partie pourra être nécessaire. Le client, par exemple, devra mettre à jour la liste des identifiants des utilisateurs et de leurs droits d'accès et communiquer tout changement au fournisseur en temps utile pour garantir le bon fonctionnement des mécanismes de gestion des identités et des accès. Il devra aussi indiquer au fournisseur le niveau de sécurité à attribuer à chaque catégorie de données.

59. Certaines menaces à la sécurité peuvent être extérieures au cadre contractuel entre le client et le fournisseur et exiger l'alignement des conditions du contrat d'informatique en nuage sur d'autres contrats passés par le fournisseur et le client (par exemple, avec des fournisseurs de services Internet).

Intégrité des données

60. Les contrats standard du fournisseur peuvent contenir une clause de non-responsabilité générale prévoyant que la responsabilité finale en ce qui concerne la préservation de l'intégrité des données incombe au client.

61. Certains fournisseurs accepteront peut-être de prendre un engagement concernant l'intégrité des données (par exemple, par le biais de sauvegardes régulières), éventuellement moyennant paiement. Indépendamment de l'arrangement contractuel passé avec le fournisseur, le client pourra se demander s'il serait utile de garantir l'accès à une copie utilisable au moins de ses données placée hors du contrôle, de la portée et de l'influence du fournisseur et de ses sous-traitants, et n'impliquant pas leur participation.

Clause de confidentialité

62. La volonté du fournisseur de s'engager à garantir la confidentialité des données client dépend de la nature des services qu'il lui fournit au titre du contrat et, en particulier, de la question de savoir s'il aura besoin d'avoir un accès non chiffré aux données pour fournir lesdits services. Certains fournisseurs ne seront peut-être pas en mesure de proposer une clause de confidentialité ou de non-divulgation et pourront expressément écarter toute obligation de confidentialité en la matière. D'autres pourront être disposés à assumer une responsabilité pour la confidentialité des données divulguées par le client lors de la négociation du contrat, mais pas pour les données traitées dans le cadre de la fourniture des services. Certaines clauses standard de confidentialité offertes par les fournisseurs ne seront pas suffisantes pour assurer le respect de la loi applicable.

63. En l'absence d'engagements contractuels et d'obligations légales auxquels le fournisseur peut être soumis pour ce qui est d'assurer la confidentialité, le client pourra devoir assumer l'entière responsabilité de la confidentialité des données, par exemple à travers le chiffrement. Lorsqu'il n'est pas possible de négocier une clause générale de confidentialité applicable à toutes les données client placées dans le nuage, les parties peuvent prendre un engagement de confidentialité pour certaines données sensibles (avec un régime de responsabilité distinct en cas de violation de la confidentialité de ces dernières). Le client pourra en particulier s'inquiéter de la protection de ses secrets commerciaux, de son savoir-faire et des informations dont il doit assurer la confidentialité conformément à la législation ou à des engagements pris auprès de tiers. Les parties peuvent convenir de limiter l'accès à ces données à un nombre limité de membres du personnel, dont elles exigeront des engagements de confidentialité à titre individuel, en particulier de ceux qui exercent une fonction à risque (par exemple, administrateurs de système, auditeurs et personnes s'occupant des dispositifs de détection des intrusions et de la réponse aux incidents). Dans ces cas, le client indiquera normalement au fournisseur les informations concernées, le niveau de protection requis, toute loi ou exigence contractuelle applicable et tout changement concernant ces informations, y compris tout changement apporté à la législation applicable.

64. Dans certains cas, la divulgation des données du client sera nécessaire aux fins de l'exécution du contrat. Dans d'autres, elle sera exigée par la loi, par exemple au titre de l'obligation de fournir des informations aux autorités publiques compétentes (voir par. 82 ci-après). Il sera alors nécessaire de prévoir des exceptions appropriées aux clauses de confidentialité.

65. Le fournisseur pourra, de son côté, imposer au client l'obligation de ne pas divulguer d'informations au sujet de ses mesures de sécurité, ni d'autres détails concernant les services qu'il lui fournit au titre du contrat ou de la loi.

Protection des données/politique de confidentialité ou accord de traitement des données

66. Les **données personnelles** font l'objet d'une protection particulière en vertu de la loi dans de nombreux pays. La loi applicable au **traitement** de ces données peut différer de la loi applicable au contrat. Elle prévaudra sur toute clause contractuelle non conforme.

67. Le contrat peut contenir une clause relative à la protection des données ou à la confidentialité ou un accord de traitement des données ou autre type d'accord similaire, même si certains fournisseurs s'engageront uniquement de manière générale à respecter la législation applicable en matière de protection des données. Dans certains pays, un tel engagement général sera peut-être insuffisant et le contrat devra énoncer au minimum l'objet et la durée, la nature et l'objectif du **traitement des données personnelles**, le type de données et les catégories de **sujets de données**, et les droits et obligations du **responsable du contrôle des données** et du **responsable du traitement des données**. Lorsqu'il n'est pas possible de négocier une clause de protection des données dans le contrat, le client souhaitera peut-être examiner les conditions générales pour déterminer si celles-ci lui donnent des garanties suffisantes quant au traitement licite des données personnelles et prévoient des recours en dommages-intérêts adéquats.

68. Le client jouera probablement le rôle de **responsable du contrôle des données** et assumera la responsabilité du respect de la législation relative à la protection des données en ce qui concerne les **données personnelles** réunies et traitées dans le nuage. Les parties peuvent convenir de clauses contractuelles visant à assurer le respect des règles applicables en matière de protection des données, y compris les demandes liées aux **droits des sujets de données**. Elles peuvent aussi convenir de voies de droit distinctes en cas de violation de ces clauses, notamment la résiliation unilatérale du contrat et l'indemnisation.

69. Les contrats standard des fournisseurs prévoient généralement que ceux-ci n'assument aucun rôle de **responsable de contrôle des données**. Normalement, le fournisseur agit en tant que **responsable du traitement des données** uniquement lorsqu'il traite les données du client conformément à ses instructions, dans le seul but de lui fournir des services d'informatique en nuage. Dans certains pays, il pourra toutefois être considéré comme assumant le rôle de **responsable du contrôle des données**, indépendamment des clauses contractuelles, lorsqu'il traite plus avant les données à ses propres fins ou selon les instructions des autorités publiques, et pourrait par conséquent assumer la pleine responsabilité de la protection des **données personnelles** pour ce qui est de ce traitement supplémentaire (voir par. 125 ci-après).

Obligations découlant d'une violation des données et d'autres incidents de sécurité

70. Les parties peuvent être tenues, de par la loi ou les dispositions contractuelles, voire les deux, de se notifier mutuellement tout **incident de sécurité** ayant un lien avec le contrat ou tout soupçon en la matière qui vient à leur connaissance. Cette obligation peut s'ajouter à l'obligation générale, qui peut être prévue par la loi, de notifier tout incident de sécurité aux parties prenantes concernées, y compris les **sujets de données**, les assureurs et les autorités publiques, ou alors au grand public, afin de prévenir les incidents ou d'en minimiser l'impact.

71. La loi peut prévoir des exigences spécifiques en matière de notification d'un incident de sécurité, et préciser notamment le moment où celle-ci doit être donnée et les personnes responsables de ce faire. Sous réserve de ces dispositions obligatoires, les parties peuvent préciser dans le contrat le délai de notification (par exemple, un jour après la prise de connaissance, par la partie, de l'incident ou de la menace), la forme et le contenu de la notification relative à l'incident de sécurité. Cette dernière indique généralement les circonstances et la cause de l'incident, le type de données touchées, les mesures à prendre pour résoudre l'incident, le moment où celui-ci devrait être résolu et le plan d'urgence, le cas échéant, à mettre en œuvre en attendant qu'il soit réglé. Elle peut également comporter des informations sur les tentatives de

violations et les attaques contre des cibles spécifiques (par utilisateur client, par application donnée, par appareil spécifique), ainsi que des tendances et des statistiques. Toute exigence en matière de notification tient normalement compte de la nécessité de ne pas divulguer d'informations sensibles susceptibles de nuire au système, aux opérations ou au réseau de la partie affectée.

72. Le fournisseur, le client ou les deux, peuvent être tenus de par la loi, ou par le contrat, à prendre des mesures à la suite d'un incident de sécurité (« mesures postincident »), y compris en faisant intervenir un tiers. Ces mesures peuvent comprendre l'isolement ou la mise en quarantaine des zones touchées, l'analyse des causes profondes et l'élaboration d'un rapport d'analyse de l'incident. Ce dernier peut être établi par la partie touchée, seule ou conjointement avec l'autre partie, ou par un tiers indépendant. Ces mesures peuvent varier en fonction des catégories de données stockées dans le nuage et d'autres facteurs.

73. Un incident de sécurité grave entraînant par exemple la perte de données pourra déboucher sur la résiliation du contrat.

Exigences en matière de localisation des données

74. Dans ses conditions générales, le fournisseur peut expressément se réserver le droit de stocker les données client dans tout pays dans lequel lui-même ou ses sous-traitants exercent des activités. Le plus souvent, une telle pratique sera suivie même en l'absence d'un droit contractuel explicite, car il est clair que les **services d'informatique en nuage** sont, de par leur nature, généralement fournis à partir de plusieurs endroits (par exemple, la sauvegarde et la protection antivirus peuvent être assurées à distance, et l'assistance être offerte depuis le monde entier, selon un **modèle ajusté aux fuseaux horaires** (modèle « **follow the sun** »). Cette pratique ne sera peut-être pas conforme aux **exigences en matière de localisation des données** applicables à l'une ou l'autre partie, voire aux deux (voir première partie, par. 10 et 11).

75. Des garanties visant à assurer le respect des **exigences en matière de localisation des données** peuvent être incluses dans le contrat, comme l'interdiction de déplacer les données et autres contenus en dehors de l'emplacement prévu, ou l'obligation d'obtenir l'approbation préalable de l'autre partie. Ainsi, on pourra inclure un paramètre de performance qualitatif dans l'**accord de niveau de service** pour garantir que les données client (y compris toute copie, **métadonnée** et sauvegarde) seront exclusivement stockées dans des centres de données physiquement situés dans les pays indiqués dans le contrat et détenus et exploités par des entités établies dans ces pays. Autrement, on pourra prévoir par exemple que les données ne doivent jamais sortir d'un certain pays ou d'une certaine région, mais peuvent être copiées dans un pays tiers donné ou ailleurs, mais en aucun cas dans tel autre pays qui sera expressément mentionné.

D. Droit d'accéder aux données client et à d'autres contenus

Droit du fournisseur d'accéder aux données client pour la fourniture des services

76. Les fournisseurs se réservent généralement le droit d'accéder aux données client conformément au principe du « besoin d'en connaître ». Avec une telle disposition, les employés, sous-traitants et autres tiers (par exemple, auditeurs) peuvent accéder aux données du client lorsqu'ils en ont besoin pour fournir les services d'informatique en nuage (y compris à des fins de maintenance, d'assistance et de sécurité) ou pour vérifier le respect de la **politique d'utilisation acceptable**, de **licences de propriété intellectuelle**, d'un **accord de niveau de service** et d'autres documents contractuels. Les parties peuvent convenir des circonstances dans lesquelles le fournisseur sera autorisé à accéder aux données client et de mesures permettant d'assurer la confidentialité et l'intégrité de ces données.

77. On peut considérer que le client octroie implicitement au fournisseur certains droits d'accès à ses données lorsqu'il demande qu'un certain service lui soit fourni. Sans ces droits, le fournisseur ne pourrait en effet pas fournir le service en question. Par exemple, si le fournisseur a pour instruction de sauvegarder régulièrement les données du client, il devra pour s'acquitter de cette tâche se voir conférer le droit de copier celles-ci. De même, si des sous-traitants doivent traiter les données du client, le fournisseur doit être en droit de les leur transférer.

78. Le contrat peut préciser les droits liés aux données requises pour l'exécution du contrat que le client confère au fournisseur, la mesure dans laquelle ce dernier est autorisé à les transférer à des tiers (par exemple, à ses sous-traitants) et la portée dans le temps et dans l'espace des droits accordés de manière implicite ou explicite. Les restrictions géographiques peuvent être particulièrement importantes lorsque les données ne peuvent sortir d'une région ou d'un pays particulier aux termes de la loi (voir première partie, par. 10 et 11). Les contrats précisent souvent si le client peut retirer un droit accordé de manière implicite ou explicite, et à quelles conditions. Étant donné que la capacité de fournir des services, au niveau de qualité exigé, peut dépendre des droits accordés par le client, le retrait de certains droits peut avoir pour conséquence d'entraîner la modification ou la fin du contrat.

Utilisation à d'autres fins des données client par le fournisseur

79. La plupart des pays ne confèrent pas au fournisseur le droit automatique d'utiliser les données client à ses propres fins. Le fournisseur pourra demander d'utiliser ces données à d'autres fins que la fourniture des services d'informatique en nuage prévus dans le contrat (par exemple, à des fins publicitaires, pour l'établissement de statistiques, de rapports analytiques ou prévisionnels ou pour d'autres pratiques d'extraction de données). Dans ce contexte, on se posera notamment les questions suivantes : a) la nature des informations concernant le client ou ses utilisateurs finaux qui seront réunies, ainsi que les raisons et le but de cette collecte et de leur utilisation par le fournisseur ; b) si ces informations seront partagées avec d'autres organisations, entreprises ou particuliers et, le cas échéant, pour quelles raisons, et si ce partage se fera avec ou sans le consentement du client ; et c) la manière dont le respect des politiques en matière de confidentialité et de sécurité sera assuré si le fournisseur partage ces informations avec des tiers. Si l'utilisation par le fournisseur des données du client concerne des **données personnelles**, on attendra généralement des parties qu'elles évaluent soigneusement leurs obligations en matière de respect des règlements au titre de la législation applicable relative à la protection des données.

80. Lorsque le contrat confère au fournisseur le droit d'utiliser les données client à ses propres fins, il peut aussi énumérer les motifs légitimes d'utilisation, prévoir des obligations en ce qui concerne la désidentification et l'anonymisation des données client pour garantir le respect de toute réglementation relative à la protection des données ou autre réglementation applicable et imposer des limites à la reproduction des contenus et à la communication d'informations au public. Il arrive fréquemment que le fournisseur soit autorisé à utiliser ces données à ses propres fins uniquement sous forme de données ouvertes rendues anonymes, ou de données agrégées et désidentifiées, pendant la durée du contrat ou au-delà.

Utilisation par le fournisseur du nom, du logo et de la marque du client

81. Les conditions générales du fournisseur peuvent lui accorder le droit d'utiliser le nom, le logo et la marque du client à des fins publicitaires. Les parties peuvent convenir de supprimer ou de modifier ces dispositions, y compris en limitant cette utilisation au nom du client, ou en exigeant l'approbation préalable de ce dernier pour l'utilisation de son nom, de son logo ou de sa marque.

Mesures prises par le fournisseur à l'égard des données client sur ordre de l'État ou aux fins du respect des règlements

82. Dans ses conditions générales, le fournisseur peut se réserver le droit de divulguer, s'il le juge approprié, des données client aux autorités publiques ou de leur donner accès à celles-ci (par exemple, avec une formule du type « lorsque cela sert au mieux les intérêts du fournisseur »). Ces conditions prévoient aussi généralement le droit du fournisseur de supprimer ou de bloquer des données client dès qu'il prend connaissance ou conscience d'un contenu illégal, ou lorsqu'il doit mettre en œuvre le **droit à l'oubli** du **sujet de données**, afin d'éviter toute responsabilité prévue par la loi (procédure « de notification et de retrait » (voir par. 128 ci-après)). Les parties peuvent convenir de limiter les circonstances dans lesquelles le fournisseur peut prendre ce genre de mesures, par exemple lorsqu'il reçoit l'ordre d'un tribunal ou d'une autre autorité publique de fournir un accès aux données ou de supprimer ou modifier celles-ci.

83. Les parties pourront convenir, au minimum, que le client sera notifié sans délai de tout ordre reçu de l'État ou des décisions du fournisseur concernant ses données, avec des précisions relatives aux données concernées, à moins qu'une telle notification ne soit contraire à la loi. Lorsqu'une notification préalable et l'intervention du client ne sont pas possibles, le contrat peut exiger du fournisseur qu'il adresse une notification *ex post* immédiate au client contenant les mêmes informations. Les parties peuvent aussi convenir de dispositions concernant la conservation de tous les ordres, requêtes et autres activités concernant les données du client, et la fourniture à ce dernier d'un accès à ces informations et aux registres correspondants.

Droits relatifs aux données dérivées des services en nuage

84. Les parties peuvent s'entendre sur les droits du client relatifs aux **données dérivées des services en nuage** et la manière dont ces droits peuvent être exercés pendant la relation contractuelle et au terme du contrat.

Clause de protection des droits de propriété intellectuelle

85. Certains types de contrats d'informatique en nuage peuvent entraîner la création d'objets de droits de propriété intellectuelle, soit conjointement par le fournisseur et le client (par exemple, améliorations du service proposées par le client) soit par le client uniquement (nouvelles applications, nouveaux logiciels et autres œuvres originales). Le contrat pourra contenir une clause expresse relative à la propriété intellectuelle, qui déterminera la partie au contrat qui jouira des droits de propriété intellectuelle sur divers objets déployés ou développés dans le nuage et l'utilisation que les parties pourront faire de ces droits. Lorsqu'il n'existe pas de possibilité de négociation dans ce domaine, le client pourra souhaiter examiner toute clause relative à la propriété intellectuelle pour déterminer si le fournisseur lui offre des garanties suffisantes et des moyens appropriés pour protéger ses droits et en jouir, et éviter tout risque de **verrouillage** (voir première partie, par. 23 à 26).

Interopérabilité et portabilité

86. La loi n'exigera pas nécessairement que l'**interopérabilité** et la **portabilité** soient assurées. Il peut appartenir entièrement au client de créer des routines d'exportation compatibles, à moins que le contrat n'en dispose autrement, par exemple en prévoyant des engagements en ce qui concerne l'interopérabilité et la portabilité, et l'assistance pour l'exportation des données à la fin du contrat (voir par. 161 ci-dessous). Le contrat pourra exiger l'utilisation de formats d'exportation de données et autres contenus qui soient normalisés ou interopérables et couramment utilisés, ou permettre le choix parmi les formats disponibles. On pourra également prévoir des clauses contractuelles concernant les droits aux produits communs et aux applications ou logiciels, sans lesquels l'utilisation des données et autres contenus dans un autre système risque d'être impossible (voir par. 85 ci-avant).

Extraction de données à des fins judiciaires

87. Les clients pourront avoir à rechercher des données placées dans le nuage sous leur forme initiale à des fins judiciaires, notamment dans le cadre d'une enquête. Les documents électroniques pourront devoir satisfaire à des exigences en matière d'audit et de preuve. Certains fournisseurs pourront offrir une assistance aux clients en vue de l'extraction de données dans le format requis par la loi. Le contrat pourra définir la forme et les conditions de cette assistance.

Suppression des données

88. La question de la **suppression des données** pourra se poser pendant la durée du contrat, mais surtout à la fin de ce dernier (voir par. 162 ci-après). Ainsi, certaines données devront peut-être être supprimées conformément au plan de conservation du client. Les données sensibles devront peut-être être détruites à un moment donné (par exemple, destruction des disques durs à la fin de la durée de vie des supports sur lesquels ces données ont été stockées). Les données devront peut-être aussi être détruites pour répondre à une demande de suppression émanant des services de police ou en cas d'atteinte avérée à la propriété intellectuelle (voir par. 82 ci-avant).

89. Les conditions générales du fournisseur peuvent ne contenir que des déclarations concernant la suppression occasionnelle des données client. Les parties pourront convenir de la suppression immédiate, effective, irrévocable et définitive des données, sauvegardes et **métadonnées**, conformément au calendrier de conservation et d'élimination ou à une autre forme d'autorisation ou de requête que le client aura communiqué au fournisseur. Le contrat pourra définir les délais et autres conditions relatifs à la suppression des données, y compris les obligations concernant la confirmation de la suppression des données et l'accès aux journaux d'audit y relatifs.

90. Des normes ou techniques de suppression particulières pourront être définies, en fonction de la nature et du caractère sensible des données. Il pourra être nécessaire de supprimer des données stockées à différents emplacements et sur divers supports, y compris sur les systèmes des sous-traitants et d'autres tiers, avec des niveaux de suppression différents, allant du nettoyage des données pour en assurer la confidentialité jusqu'à leur suppression complète, voire à la destruction du matériel. Une suppression plus sûre impliquant la destruction, plutôt que le redéploiement du matériel, risque d'être plus coûteuse et de ne pas toujours être possible (par exemple, si les données d'autres personnes sont stockées sur le même support). Par conséquent, on pourra souhaiter prévoir dans le contrat que le fournisseur doit utiliser une infrastructure isolée pour stocker les données les plus sensibles du client.

E. Audits et suivi

Activités de suivi

91. Les parties pourront devoir surveiller leurs activités respectives pour assurer le respect des règlements et des dispositions contractuelles (par exemple, respect par le client et ses utilisateurs finaux de la **politique d'utilisation acceptable** et des **licences de propriété intellectuelle**, et respect par le fournisseur de l'**accord de niveau de service** et de la politique de protection des données). Certaines activités de suivi, liées notamment au **traitement des données personnelles**, peuvent être exigées par la loi.

92. Le contrat pourra préciser les activités régulières ou périodiques de suivi et la partie qui sera chargée de les exécuter, ainsi que l'obligation de l'autre partie de faciliter ce suivi. Il pourra aussi anticiper toute activité de suivi exceptionnelle et prévoir les modalités d'exécution y relatives. Enfin, il pourra aussi prévoir l'obligation de communiquer des informations à ce sujet à l'autre partie, ainsi que tout engagement de confidentialité en relation avec ces activités de suivi.

93. Un suivi excessif peut avoir des conséquences négatives sur la performance et augmenter le coût des services. Le contrat pourra prévoir l'obligation de suspendre le suivi dans certaines circonstances, par exemple si celui-ci porte gravement atteinte à la fourniture de services. Cette préoccupation pourra concerner particulièrement les services qui requièrent une performance en temps quasi réel.

Audits et tests de sécurité

94. Les audits et tests de sécurité sont courants, surtout ceux qui visent à contrôler l'efficacité des mesures de sécurité. Certains peuvent être exigés par la loi. Le contrat peut inclure des clauses relatives aux droits en matière d'audit des deux parties, à la portée et au rythme de ces audits, ainsi qu'aux formalités et coûts y relatifs. Il peut aussi obliger les parties à partager les résultats des audits ou tests de sécurité qu'elles font réaliser. Dans le contrat, on pourra mettre en regard d'une part les droits contractuels ou obligations légales en matière d'audits et de tests de sécurité, et d'autre part l'obligation de l'autre partie de faciliter l'exercice de ces droits ou l'exécution de ces obligations (par exemple, en donnant accès aux centres de données concernés).

95. Les parties pourront convenir que les audits et les tests de sécurité peuvent uniquement être réalisés par des organisations professionnelles, ou que le fournisseur ou le client peuvent choisir de les confier à une telle organisation. Le contrat pourra prévoir les qualifications requises du tiers concerné et les conditions de son engagement, y compris la répartition des coûts. Les parties pourront convenir de dispositions particulières concernant la réalisation d'audits ou de tests de sécurité à la suite d'un incident, en fonction de la gravité et du type d'incident (par exemple, la partie responsable de l'incident pourra être tenue de rembourser partiellement ou intégralement les coûts).

F. Conditions de paiement

Facturation à l'usage

96. Le prix est une condition essentielle du contrat, et le fait de ne pas y inclure le prix ou un mécanisme de fixation du prix peut entraîner la nullité de celui-ci.

97. Dans des services d'informatique en nuage caractérisés par le **libre-service à la demande**, la facturation se fera généralement **à l'usage**. Il arrive couramment que le contrat précise le prix à l'unité pour le volume convenu de services fournis (par exemple, pour un nombre défini d'utilisateurs, d'utilisations ou en fonction du temps utilisé). Les barèmes ou autres ajustements de prix, y compris les rabais de volume, peuvent être conçus comme des mesures incitatives ou dissuasives pour l'une ou l'autre des parties. Les essais gratuits sont courants, de même que la fourniture de certains services à titre gracieux. S'il peut y avoir de nombreuses options en matière de calcul des prix, une clause claire et transparente dans ce domaine, bien comprise par les deux parties, permettra peut-être d'éviter des conflits et des litiges.

Frais de licence

98. Les parties voudront peut-être préciser dans le contrat si le coût des services d'informatique en nuage englobe les frais pour toute licence que le fournisseur peut accorder au client en relation avec ces services. Les contrats de type **SaaS**, en particulier, prévoient souvent l'utilisation, par le client, de logiciels donnés en licence par le fournisseur.

99. Les frais de licence peuvent être calculés par poste ou par instance et varier en fonction de la catégorie d'utilisateurs (par exemple, les utilisateurs professionnels, par opposition aux utilisateurs non professionnels, pourront entrer dans l'une des catégories les plus chères). Des structures de paiement différentes peuvent avoir des incidences différentes. Ainsi, les frais de licence d'un client peuvent considérablement augmenter si le logiciel est facturé par instance, chaque fois qu'une

nouvelle machine est reliée, même si le client utilise le même nombre d'instances de machines pour la même durée.

100. Le contrat pourra préciser le nombre total d'utilisateurs potentiels du logiciel couvert par l'accord de licence, le nombre d'utilisateurs dans chaque catégorie (par exemple, employés, entrepreneurs indépendants et fournisseurs) et les droits à accorder à chaque catégorie. Il pourra aussi préciser les droits d'accès et d'utilisation qui entreront dans la portée de la licence, ainsi que les cas d'accès et d'utilisation par le client et ses utilisateurs finaux qui nécessiteront l'élargissement de cette portée et entraîneront par conséquent une hausse des frais de licence.

Coûts supplémentaires

101. Le prix peut comprendre également les coûts non récurrents (par exemple, pour la configuration et la migration vers le nuage (voir première partie, par. 32 et 33)). On peut également envisager des services supplémentaires proposés par le fournisseur et facturés séparément (par exemple, assistance après les heures de bureau, facturée au temps passé ou de manière forfaitaire).

102. La question de savoir si les services d'informatique en nuage entrent dans la catégorie des biens ou services imposables dépendra d'un pays à l'autre. Les parties pourront souhaiter aborder, dans le contrat, la question de l'impact fiscal sur les conditions de paiement.

Autres conditions de paiement

103. Les conditions de paiement peuvent prévoir les modalités de facturation (par exemple, facturation électronique), ainsi que la forme et le contenu des factures, aux fins notamment du respect des obligations fiscales. Les autorités fiscales de certains pays pourront ne pas accepter les factures électroniques (même si cela devient de moins en moins courant dans l'environnement dématérialisé), ou exiger qu'elles se présentent sous une forme particulière, et notamment qu'elles indiquent séparément les taxes applicables aux services d'informatique en nuage.

104. Les parties pourront souhaiter préciser, parmi les conditions de paiement, les échéances, la monnaie, le taux de change applicable, les modalités de paiement, les sanctions en cas de retards de paiement et les procédures de règlement de tout litige relatif à une demande de paiement.

G. Modification des services

105. Les **services d'informatique en nuage** sont par nature souples et variables. À travers de nombreuses options contractuelles, le client peut tirer parti de certaines caractéristiques de ces services, à savoir l'**élasticité**, l'**extensibilité** et le **libre-service à la demande**, afin d'ajuster la consommation de services en fonction de ses besoins. Cela lui évite d'avoir à renégocier le contrat chaque fois qu'il souhaite modifier sa consommation.

106. De son côté, le fournisseur peut se réserver le droit d'ajuster son portefeuille de services selon qu'il le juge approprié. Il pourra être nécessaire de traiter différemment, dans le contrat, les changements concernant les services de base et ceux qui concernent les services auxiliaires et les aspects relatifs à l'assistance. Il pourra également être nécessaire de traiter différemment les changements qui pourraient avoir une incidence négative sur les services, et ceux qui apportent une amélioration (par exemple, le passage d'une offre classique à une offre améliorée comportant des niveaux de sécurité plus élevés ou des délais de réponse plus courts). Certaines modifications unilatérales apportées aux clauses et conditions contractuelles par le fournisseur peuvent avoir de graves conséquences pour le client et se traduire, en particulier, par des frais élevés de migration vers un autre système.

Modification du prix

107. Le fournisseur peut se réserver le droit de modifier unilatéralement le prix ou les barèmes de prix. Les parties peuvent convenir de définir dans le contrat la méthode de fixation des coûts (par exemple, la fréquence et l'ampleur des éventuelles augmentations). Les prix peuvent être liés à un indice des prix à la consommation particulier, limités à un pourcentage défini ou fixés selon le barème de prix du fournisseur à un moment donné. Le contrat peut exiger la notification préalable de toute hausse de prix et prévoir les conséquences de la non-acceptation, par le client, d'une telle hausse.

Mises à jour

108. Si elles peuvent être dans l'intérêt du client, les mises à jour peuvent également perturber la disponibilité des services d'informatique en nuage, car elles peuvent se traduire par des **temps d'arrêt** relativement longs pendant les heures ouvrables normales, même si le service est censé être fourni 24 heures sur 24 et 7 jours sur 7. Les parties peuvent convenir que le client doit être notifié à l'avance des mises à jour prévues et de leurs implications, et que celles-ci doivent, en règle générale, être effectuées pendant des périodes de faible demande ou d'absence de demande pour le client. Le contrat peut aussi prévoir des procédures pour signaler et pour résoudre les problèmes éventuels.

109. Les mises à jour peuvent avoir d'autres effets négatifs, par exemple exiger des modifications des applications ou des systèmes informatiques des clients, ou la mise à niveau des connaissances des utilisateurs. Le contrat peut prévoir la répartition des coûts découlant des mises à jour. Dans les cas où des modifications importantes doivent être apportées à une version en cours d'utilisation, les parties peuvent aussi convenir de maintenir en parallèle les ancienne et nouvelle versions pendant une période convenue, afin d'assurer au client la continuité de ses activités commerciales. Le contrat peut également prévoir l'assistance qui pourra être offerte par le fournisseur dans le contexte des modifications à apporter aux applications ou aux systèmes informatiques du client et, le cas échéant, de la mise à niveau des connaissances des utilisateurs finaux.

Dégradation ou interruption des services

110. Les développements technologiques, la pression concurrentielle et d'autres raisons peuvent entraîner la dégradation ou l'interruption de certains services d'informatique en nuage, avec ou sans remplacement par d'autres services. Dans le contrat, le fournisseur peut se réserver le droit d'adapter son offre, par exemple en mettant fin à une partie des services. L'abandon de certains services par le fournisseur peut toutefois engager la responsabilité du client vis-à-vis de ses utilisateurs finaux.

111. Le contrat peut prévoir la notification préalable de tels changements au client, le droit de ce dernier de résilier le contrat en cas de changements inacceptables ainsi qu'un délai de conservation adéquat pour garantir la **réversibilité** en temps utile des données ou d'autres contenus concernés du client. Certains contrats interdisent toute modification susceptible d'affecter négativement la nature, l'étendue ou la qualité des services fournis, ou limitent les changements autorisés aux « modifications commercialement raisonnables ».

Notification des modifications

112. Aux termes de leurs conditions générales, les fournisseurs peuvent être tenus d'informer le client des modifications des conditions de service. Dans le cas contraire, les clients seront peut-être censés vérifier régulièrement si des changements ont été apportés au contrat. Le contrat peut être constitué par plusieurs documents (voir par. 38 ci-avant). Certains contrats peuvent renvoyer à des conditions et politiques contenues dans d'autres documents, lesquels peuvent aussi renvoyer à d'autres conditions et politiques, tous ces documents pouvant faire l'objet de modifications unilatérales de la part du fournisseur. Ces différents documents ne seront pas

nécessairement tous publiés au même endroit sur le site Internet du fournisseur, si bien qu'il sera parfois difficile de repérer les éventuels changements introduits par le fournisseur.

113. La poursuite de l'utilisation des services par le client étant réputée valoir acceptation des conditions modifiées, les parties pourront convenir que le client sera notifié des changements destinés à être apportés aux conditions de service dans un délai suffisant avant leur date d'entrée en vigueur. Elles pourront aussi convenir que le client aura accès aux journaux d'audit relatifs à l'évolution des services et que toutes les conditions convenues et les services définis par référence à une version particulière seront conservés.

H. Suspension des services

114. Les conditions générales des fournisseurs peuvent leur octroyer le droit de suspendre les services à tout moment, s'ils le jugent opportun. Pour justifier la suspension unilatérale des services, les fournisseurs invoquent souvent des « événements imprévisibles », qui sont habituellement définis comme englobant de manière générale tous les obstacles échappant au contrôle du fournisseur, y compris les défaillances de sous-traitants, de sous-fournisseurs et d'autres tiers impliqués dans la fourniture des services d'informatique en nuage au client, notamment les fournisseurs de réseaux Internet.

115. Les parties peuvent convenir qu'une telle suspension pourra uniquement intervenir dans certains cas limités, indiqués dans le contrat (par exemple, en raison d'une violation fondamentale du contrat par le client, notamment en cas du non-paiement de sommes dues). Le droit de suspension en raison d'événements imprévisibles peut être subordonné à la bonne mise en œuvre d'un plan de continuité des opérations et de reprise après sinistre. Le contrat peut exiger que ce plan contienne des mesures de protection contre les facteurs qui menacent le plus fréquemment la prestation des services d'informatique en nuage et qu'il soit soumis aux commentaires et à l'approbation de l'autre partie. Parmi les mesures de protection, on mentionnera l'établissement, dans un lieu géographiquement distinct, d'un site de reprise après sinistre assurant une transition sans heurt, ainsi que l'utilisation d'une alimentation électrique sans coupure et de générateurs de secours.

I. Sous-traitants, sous-fournisseurs et externalisation

Identification de la chaîne de sous-traitance

116. La sous-traitance, les **services d'informatique en nuage en couches** et l'externalisation se rencontrent fréquemment dans l'environnement de l'informatique en nuage. Dans leurs conditions générales, les fournisseurs peuvent se réserver expressément le droit d'avoir recours à des tiers pour la prestation des services en nuage au client, ou alors ce droit peut être implicite du fait de la nature des services à fournir. Le fournisseur peut souhaiter conserver autant de latitude que possible à cet égard.

117. La loi pourra exiger que les parties identifient dans le contrat les tiers intervenant dans la fourniture des services d'informatique en nuage. Une telle identification pourra aussi être dans l'intérêt du client à des fins de vérification, notamment pour vérifier le respect, par les tiers, des exigences législatives ou contractuelles en matière notamment de sécurité, de confidentialité et de protection des données, et l'absence de conflit d'intérêt de la part des tiers.

118. Ces informations peuvent aussi être utilisées pour réduire les risques de non-exécution du contrat par le fournisseur en raison de défaillances des tiers. Ainsi, le client peut choisir de conclure un accord directement avec les tiers qui interviennent dans l'exécution du contrat d'informatique en nuage, en particulier en ce qui concerne des questions sensibles telles que la confidentialité et le **traitement des données**

personnelles. Il peut également essayer de négocier avec les tiers les plus importants une obligation d'intervenir si le fournisseur n'exécute pas le contrat comme il se doit (notamment s'il devient insolvable).

119. Le fournisseur pourra être en mesure d'identifier les tiers qui jouent un rôle important, mais pas nécessairement tous les tiers impliqués. L'ensemble de tiers qui interviennent dans la fourniture des services d'informatique en nuage peut varier pendant la durée du contrat (voir par. 120 et 121 ci-après).

Modifications de la chaîne de sous-traitance

120. Les changements unilatéraux de la chaîne de sous-traitance sont fréquents. Le contrat peut préciser si de tels changements sont autorisés et prévoir, le cas échéant, dans quelles conditions, par exemple en prévoyant que le client peut se réserver le droit d'effectuer des vérifications et d'opposer son veto à tout nouveau tiers intervenant dans la fourniture des services d'informatique en nuage, avant que cette intervention ne devienne effective. Une autre solution est d'inclure dans le contrat une liste de tiers préalablement approuvés par le client, à laquelle le fournisseur pourra se référer en cas de besoin. Une autre solution encore consiste à soumettre les changements à l'approbation, à posteriori, par le client. En l'absence de cette approbation, les services continuent d'être fournis par le tiers précédent ou un autre tiers préalablement approuvé, ou par un autre tiers choisi d'un commun accord par les parties. Dans les autres cas, le contrat peut être résilié.

121. La législation impérative applicable peut prévoir les circonstances dans lesquelles des modifications de la chaîne de sous-traitance d'un fournisseur peuvent entraîner la résiliation du contrat.

Harmonisation des conditions du contrat avec les contrats liés

122. La loi ou le contrat même peut exiger des parties qu'elles harmonisent les conditions dudit contrat avec les contrats existants ou futurs qui lui sont liés afin d'assurer la confidentialité et le respect des exigences en matière de **localisation** et de protection **des données**. Le contrat peut obliger les parties à se communiquer mutuellement des copies des contrats liés à des fins de vérification.

Responsabilité des sous-traitants, des sous-fournisseurs et d'autres tiers

123. Bien qu'ils puissent être énumérés dans le contrat, les tiers qui jouent un rôle dans l'exécution du contrat d'informatique en nuage ne sont pas eux-mêmes parties au contrat entre le fournisseur et le client. Les obligations qu'ils sont tenus d'exécuter sont celles qui découlent de leurs propres contrats avec le fournisseur. Le fait de créer des droits de tiers bénéficiaire au profit du client dans des contrats liés ou de faire du client une partie à ces contrats, permettrait à celui-ci de se retourner directement contre le tiers en cas d'inexécution, par ce dernier, des obligations lui incombant au titre d'un contrat lié.

124. Conformément au contrat ou à la loi applicable, le fournisseur peut être tenu responsable envers le client de tout problème relevant de la responsabilité d'un tiers qu'il a fait intervenir aux fins de l'exécution du contrat. En particulier, la responsabilité conjointe du fournisseur et de ses sous-traitants peut être établie par la loi pour tout problème lié au **traitement des données personnelles**, selon le degré de participation des sous-traitants à ce traitement.

J. Responsabilité

Dispositions légales limitant la liberté contractuelle

125. Si la plupart des systèmes juridiques reconnaissent généralement le droit des parties contractantes de répartir les risques et les responsabilités et de limiter ou d'exclure la responsabilité par le biais de dispositions contractuelles, ce droit est

habituellement soumis à diverses limitations et conditions. Ainsi, le rôle que chaque partie assume en ce qui concerne les **données personnelles** placées dans le nuage constitue un facteur important pour la répartition des risques et des responsabilités dans le cadre du **traitement des données personnelles**. Dans certains pays, la législation sur la protection des données impose une plus grande responsabilité aux **responsables du contrôle des données** qu'aux **responsables du traitement** des **données personnelles**. Nonobstant les dispositions contractuelles, c'est le maniement de ces données qui déterminera généralement le régime juridique auquel la partie serait soumise en vertu du droit applicable. Les **sujets de données** qui ont subi une perte résultant du traitement illicite de données personnelles ou de tout acte incompatible avec les dispositions nationales relatives à la protection des données peuvent être fondés à être indemnisés directement par le **responsable du contrôle des données**.

126. En outre, dans de nombreux pays, l'exclusion totale de la responsabilité du fait personnel n'est pas admissible ou est sujette à des limitations. Il est parfois impossible d'exclure totalement la responsabilité liée aux dommages corporels (y compris la maladie et le décès) et à la négligence grave, aux dommages intentionnels, aux défauts, à la violation des obligations essentielles du contrat ou au non-respect des exigences réglementaires applicables. On pourra juger abusives, et par conséquent nulles, certains types de clauses limitatives, comme une clause d'exonération de responsabilité du fournisseur pour les **incidents de sécurité** dans les cas où le client n'a aucun contrôle ni moyen d'assurer cette sécurité. Les conditions des contrats d'adhésion, qui ne sont généralement pas négociées mais préétablies par l'une des parties, pourront faire l'objet d'un examen plus poussé. Par ailleurs, la loi peut prévoir la responsabilité illimitée pour certains types de défauts (par exemple, matériels ou logiciels défectueux).

127. La législation peut limiter la capacité qu'ont les institutions publiques d'assumer certaines responsabilités ou leur imposer d'obtenir l'approbation préalable d'un organe compétent de l'État pour ce faire. Il peut aussi leur être interdit d'accepter l'exclusion ou la limitation de la responsabilité des fournisseurs soit de manière générale soit en ce qui concerne des omissions ou des actes définis dans la législation.

128. D'autre part, la législation applicable peut prévoir une exonération de responsabilité si certains critères sont remplis par une partie dont la responsabilité risquerait autrement d'être engagée. Par exemple, en vertu de la procédure dite de notification et de retrait qui a cours dans certains pays, le fournisseur sera dégagé de toute responsabilité relative à l'hébergement d'un contenu illicite sur son infrastructure en nuage s'il supprime ce contenu lorsqu'il en prend connaissance.

129. Dans certains pays, les clauses de non-responsabilité et de limitation de responsabilité convenues par les parties doivent être incluses dans le contrat pour être exécutoires. La loi applicable peut imposer des exigences, notamment de forme, pour que ces clauses soient valables et exécutoires.

Autres considérations à prendre en compte pour la rédaction de clauses de responsabilité

130. Dans la négociation relative à la répartition des risques et des responsabilités, on examinera tant le montant susceptible d'être facturé pour les services d'informatique en nuage que les risques liés à la prestation de ces services. Bien que les parties tendent généralement à exclure ou à limiter leur responsabilité en ce qui concerne les facteurs sur lesquels elles n'ont pas ou que peu de contrôle (par exemple, le comportement des utilisateurs finaux, les actes ou les omissions des sous-traitants), le niveau de contrôle n'est pas toujours une considération décisive. Une partie peut être prête à assumer les risques et les responsabilités liés à certains éléments qu'elle ne contrôle pas afin de se distinguer sur le marché. Il est néanmoins probable que les risques et les responsabilités de la partie augmentent progressivement en proportion des éléments qu'elle contrôle.

131. Par exemple, dans les modèles **SaaS** impliquant l'utilisation d'un logiciel de bureautique standard, il est probable que le fournisseur sera responsable de la quasi-totalité des ressources fournies au client et que sa responsabilité pourra être engagée en cas de non-fourniture ou de dysfonctionnements de ces ressources. Néanmoins, même dans ces cas, le client pourrait rester responsable de certains aspects des services, tels que le chiffrement ou la sauvegarde des données sous son contrôle. En cas de perte de données, le client qui n'aura pas effectué les sauvegardes de rigueur pourrait être privé de son droit de recours contre le fournisseur. Dans les modèles **IaaS** et **PaaS**, le fournisseur pourrait n'être responsable que de l'infrastructure ou des plateformes fournies (comme le matériel informatique, les systèmes d'exploitation ou les logiciels médiateurs) tandis que le client assumerait la responsabilité de tous les éléments lui appartenant (comme les applications exécutées au moyen de l'infrastructure ou des plateformes fournies et les données qu'elles contiennent).

Conditions générales du fournisseur

132. Les conditions générales des fournisseurs peuvent exclure toute responsabilité découlant du contrat et faire valoir que les clauses de responsabilité ne sont pas négociables. Selon une autre possibilité, le fournisseur peut accepter la responsabilité (même illimitée) pour des violations qu'il est en mesure de contrôler (comme une violation des licences de propriété intellectuelle concédées au fournisseur par le client) mais pas pour des violations qui peuvent survenir pour des raisons indépendantes de sa volonté (par exemple, événements imprévisibles ou fuites de données confidentielles, entre autres).

133. Les conditions générales des fournisseurs excluent généralement toute responsabilité pour des dommages indirects (par exemple, perte de chiffre d'affaires résultant de l'indisponibilité du service d'informatique en nuage). Lorsque la responsabilité est acceptée de façon générale ou pour certains cas précis, les conditions générales des fournisseurs limitent souvent le montant des pertes qui seront couvertes (par incident, par série d'incidents ou par période de temps). En outre, les fournisseurs fixent souvent un plafond global de responsabilité dans le cadre du contrat, qui peut être lié aux recettes attendues du contrat, au chiffre d'affaires du fournisseur ou à la couverture d'assurance.

134. Les conditions générales des fournisseurs rendent généralement le client responsable en cas de non-respect de la **politique d'utilisation acceptable**.

Modifications possibles des conditions générales

135. Certains événements (comme une violation de la protection des données personnelles ou une atteinte aux droits de propriété intellectuelle) peuvent exposer l'une ou l'autre partie à la responsabilité – potentiellement élevée – à l'égard des tiers ou donner lieu à des amendes réglementaires. Par conséquent, il arrive fréquemment que les parties conviennent d'un régime de responsabilité plus strict (responsabilité illimitée ou dédommagement plus élevé) pour les événements qui résultent d'une faute ou d'une négligence de l'autre partie.

136. Par contre, la responsabilité des parties pour des actes commis par des tiers qui échappent à leur contrôle (par exemple, responsabilité du client pour les actes des utilisateurs finaux ou du fournisseur pour des actes du client ou de ses utilisateurs finaux) pourra être limitée, voire exclue par le contrat ou par la loi.

Assurance responsabilité

137. Le contrat peut prévoir des obligations en matière d'assurance visant l'une ou l'autre partie, voire les deux, notamment en ce qui concerne les exigences de qualité que les compagnies d'assurance doivent remplir et le montant minimal de la couverture d'assurance demandée. Il peut également préciser que les parties doivent s'aviser mutuellement de toute modification apportée à la couverture d'assurance ou se communiquer des copies des polices d'assurance en vigueur.

K. Recours en cas de violation du contrat

Types de recours

138. Les parties sont libres de choisir des recours dans les limites du droit applicable. Parmi les recours figurent les demandes de réparations en nature, qui visent à fournir à la partie lésée le même avantage ou un avantage équivalent à celui attendu de l'exécution du contrat (entre autres le remplacement du matériel défectueux), les demandes de réparations pécuniaires (par exemple, les crédits de service) ou le recours en résiliation du contrat. Le contrat pourrait établir une distinction entre les types de violations et préciser les recours correspondants.

Suspension ou résiliation des services

139. La suspension ou la résiliation de la prestation des services d'informatique en nuage constitue un recours habituel du fournisseur en cas de rupture de contrat de la part du client ou de violation de la **politique d'utilisation acceptable** par les utilisateurs finaux du client. Le contrat peut prévoir des garanties contre les droits étendus de suspension ou de résiliation. Par exemple, le droit du fournisseur de suspendre ou de résilier la prestation des services d'informatique en nuage au client pourra être limité aux cas de violations fondamentales du contrat par le client et de menaces sérieuses pour la sécurité ou l'intégrité des systèmes du fournisseur, et aux cas énoncés dans la législation applicable. Le droit de suspension ou de résiliation du fournisseur pourra aussi être limité aux services affectés par la violation, lorsque cette possibilité existe.

Crédits de service

140. Le système des crédits de service est un mécanisme souvent utilisé pour indemniser le client lorsque le fournisseur ne remplit pas ses obligations. Ces crédits se présentent sous la forme d'une baisse du prix des services fournis conformément au contrat au cours de la période mesurée suivante. Un barème dégressif peut s'appliquer, c'est-à-dire qu'un pourcentage de la réduction du prix peut dépendre de l'écart entre la performance effective du fournisseur au titre du contrat et les paramètres définis dans l'**accord de niveau de service** ou dans d'autres parties du contrat. Un plafond global en matière de crédits de service peut également s'appliquer. Les fournisseurs peuvent limiter les circonstances dans lesquelles des crédits de service sont accordés, par exemple aux cas où les défaillances sont dues à des aspects qu'ils contrôlent, ou limiter les délais dans lesquels les clients peuvent utiliser ces crédits. Certains fournisseurs peuvent aussi être disposés à rembourser des frais déjà payés ou à fournir un ensemble de services amélioré au cours de la période mesurée suivante (comportant par exemple un soutien informatique gratuit). S'il existe un éventail d'options, les conditions générales des fournisseurs peuvent préciser que toute réparation en cas d'inexécution de la part du fournisseur sera laissée au choix de ce dernier.

141. Le fait de prévoir les crédits de service comme seul et unique recours contre un fournisseur qui ne remplit pas ses obligations contractuelles peut limiter le droit du client de se prévaloir d'autres recours, y compris des actions en réparation ou en résiliation du contrat. En outre, il peut être inutile de proposer des crédits de service sous la forme d'une baisse du coût ou d'un ensemble de services amélioré au cours de la période mesurée suivante si le contrat est résilié. Enfin, la mise en œuvre de tels crédits peut être impossible si ceux-ci sont considérés comme une approximation déraisonnable du préjudice lors de la formation du contrat. D'autres mesures, comme l'imposition de pénalités, seront peut-être mieux à même d'assurer le respect des obligations contractuelles.

Formalités à observer en cas de violation du contrat

142. Le contrat peut prévoir des formalités à respecter en cas de violation, par exemple exiger d'une partie qu'elle notifie l'autre partie en cas de violation présumée

d'une de ses clauses et qu'elle lui donne l'occasion de remédier à la violation invoquée. Des délais de recours peuvent également être fixés.

L. Durée et résiliation du contrat

Date d'entrée en vigueur du contrat

143. La date d'entrée en vigueur du contrat peut différer de la date de signature, de la date d'acceptation de l'offre ou de la date d'acceptation de la configuration et d'autres actions requises pour que le client migre ses données vers le nuage. On peut considérer que la date d'entrée en vigueur du contrat est celle à laquelle le fournisseur met les services d'informatique en nuage à la disposition du client, même si ce dernier ne les utilise pas effectivement. Il est également possible de considérer que le contrat entre en vigueur le jour où le client effectue le premier paiement correspondant aux services d'informatique en nuage, même si le fournisseur ne les a pas encore mis à sa disposition. Pour ces raisons, et pour éviter toute incertitude, les parties pourront indiquer dans le contrat la date d'entrée en vigueur de celui-ci.

Durée du contrat

144. Le contrat peut être de durée courte, moyenne ou longue. Dans le cadre des **solutions d'informatique en nuage normalisées pour multiabonnés**, il est fréquent de prévoir une durée initiale fixe (courte ou moyenne), avec des renouvellements automatiques, à moins de résiliation par l'une ou l'autre partie. Le fournisseur peut convenir de notifier à l'avance au client la prochaine expiration du contrat. Différentes considérations pourront influer sur la décision de renouvellement d'un contrat, notamment le risque de **verrouillage** et le risque de passer à côté d'une offre plus intéressante.

Résiliation anticipée

145. Les contrats mentionnent généralement les motifs de résiliation autres que l'expiration de la durée fixe, comme la résiliation pour convenance ou pour violation, entre autres. Le contrat peut prévoir des modalités de résiliation anticipée, y compris l'obligation d'un préavis suffisant, la **réversibilité** et d'autres engagements de fin de contrat (voir par. 157 à 167 ci-après).

Résiliation pour convenance

146. En particulier dans le cadre des **solutions d'informatique en nuage normalisées pour multiabonnés**, les fournisseurs se réservent généralement le droit, dans leurs conditions générales, de résilier le contrat à tout moment sans qu'il y ait défaillance du client. Les parties peuvent convenir de limiter les circonstances dans lesquelles ce droit pourra s'exercer et d'obliger le fournisseur à signifier au client un préavis de résiliation suffisamment long.

147. Le droit du client de résilier le contrat pour convenance (c'est-à-dire sans qu'il y ait de défaillance du fournisseur) se rencontre surtout dans les contrats publics. Dans ce cas, le fournisseur peut exiger le paiement d'indemnités de résiliation anticipée, paiement que la législation peut toutefois limiter dans le cas des entités publiques. Dans les contrats à durée indéterminée, les fournisseurs peuvent être plus enclins à accepter la résiliation pour convenance par le client sans demander de compensation, mais peuvent pour cela demander un tarif plus élevé dans le contrat.

Résiliation pour violation

148. La violation fondamentale du contrat en justifie généralement la résiliation. Afin d'éviter toute ambiguïté, les parties peuvent définir dans le contrat des événements qu'elles considéreront comme constituant une violation fondamentale. Parmi les violations fondamentales commises par le fournisseur, on mentionnera la perte ou l'utilisation abusive de données, les infractions à la protection des données

personnelles, les **incidents de sécurité** récurrents (à savoir plus d'un certain nombre de fois par période mesurée), les violations de confidentialité et l'indisponibilité des services à certains moments ou pendant une certaine durée. Le défaut de paiement par le client et la violation de la **politique d'utilisation acceptable** par le client ou ses utilisateurs finaux sont les motifs les plus fréquents de résiliation du contrat par le fournisseur. Le droit d'une partie de résilier le contrat peut être subordonné à la notification d'un préavis, à la tenue de consultations de bonne foi et à la possibilité de remédier à la situation. Cette partie peut être tenue, conformément au contrat, de rétablir l'exécution du contrat dans un certain délai après que des mesures correctives ont été prises.

149. Le contrat pourra évoquer les engagements de fin de contrat du fournisseur qui survivraient à une violation fondamentale de celui-ci par le client, y compris la **réversibilité** des données et autres contenus du client (voir par. 157 à 167 ci-après).

Résiliation pour cause de modifications inacceptables du contrat

150. Certaines modifications apportées au contrat par une partie pourront ne pas être jugées acceptables par l'autre partie et justifier la résiliation du contrat. Il peut s'agir de changements portant sur les **exigences en matière de localisation des données** ou sur les conditions de sous-traitance. Le contrat peut conférer le droit au client de le résilier dans son intégralité si des modifications découlant de la restructuration du portefeuille de services du fournisseur entraînent la cessation ou le remplacement de certains services (voir par. 105 à 124 ci-avant et par. 155 ci-après).

Résiliation pour cause d'insolvabilité

151. Les risques d'insolvabilité peuvent être identifiés lors de l'évaluation des risques (voir première partie, par. 15 j)) et pendant la durée du contrat, par exemple dans le cas où ce dernier exige la communication périodique d'informations au sujet de la situation financière des parties. On rencontre fréquemment des clauses prévoyant la résiliation du contrat en cas d'insolvabilité de l'une des parties, clauses qui peuvent toutefois être primées par les dispositions impératives de la législation sur l'insolvabilité.

152. Un client insolvable aura peut-être besoin de continuer à utiliser les services d'informatique en nuage pendant qu'il résout ses difficultés financières. Les parties peuvent limiter le droit d'invoquer l'insolvabilité comme seul motif de résiliation du contrat en l'absence, par exemple, de défaut de paiement des montants dus au titre du contrat par le client.

153. Les parties peuvent préciser dans le contrat, ou la loi prévoir, des mécanismes permettant de récupérer les données client en cas d'insolvabilité du fournisseur (par exemple, libération automatique du code source ou des clefs sous séquestre permettant d'accéder aux données et autres contenus du client). Autrement, le client pourra avoir des difficultés à récupérer ses données et autres contenus hébergés sur l'infrastructure en nuage du fournisseur insolvable. Lorsqu'une crise de confiance dans la situation financière du fournisseur provoque des sorties et des retraits de contenus à grande échelle, le fournisseur insolvable ou un **représentant de l'insolvabilité** peuvent limiter les quantités de contenus (données et code applicatif) susceptibles d'être retirées dans un délai donné, ou décider de remplir les engagements de fin de contrat dans l'ordre des demandes (« premiers venus, premiers servis »).

Résiliation en cas de changement de contrôle

154. Le changement de contrôle peut impliquer, par exemple, un changement de propriété ou des changements dans la capacité de déterminer, directement ou indirectement, les politiques opérationnelles et financières du fournisseur, ce qui peut entraîner des modifications du portefeuille de services de ce dernier. Il peut également entraîner la cession ou la novation du contrat, avec transfert à un tiers soit uniquement des droits, soit des droits et des obligations découlant du contrat. En conséquence,

une partie initiale au contrat peut être remplacée, ou certains aspects du contrat, par exemple les paiements, peuvent devoir être accomplis par un tiers.

155. La législation applicable peut imposer la résiliation du contrat si, du fait du changement de contrôle, il devient impossible de remplir certaines dispositions législatives impératives (concernant notamment les **exigences en matière de localisation des données** ou l'interdiction de traiter avec certaines entités placées sous un régime de sanctions internationales ou constituant une menace à la sécurité nationale). Les contrats publics en particulier peuvent être affectés par des limitations réglementaires en matière de changement de contrôle. De plus, les parties peuvent convenir de résilier le contrat en cas de changement de contrôle en particulier si, en raison de ce changement, le fournisseur ou le contrat sont repris par un concurrent du client ou si la reprise entraîne l'abandon ou la transformation du portefeuille des services. Il est courant d'exiger la notification préalable d'un changement de contrôle à venir et des incidences prévues sur le contrat.

Clause relative à l'inactivité du compte

156. L'absence d'activité de la part du client pendant une période précisée dans le contrat peut justifier la résiliation unilatérale de ce dernier par le fournisseur. Les contrats portant sur la fourniture, contre rémunération, de services d'informatique en nuage d'entreprise à entreprise comportent toutefois rarement de telles clauses relatives à l'inactivité du compte.

M. Engagements de fin de contrat

157. Les engagements de fin de contrat peuvent soulever des questions non seulement contractuelles mais également réglementaires. Les parties pourront chercher à parvenir à un équilibre entre les intérêts du client, qui souhaite continuer à avoir accès à ses données et autres contenus (notamment pendant la période de transition) et ceux du fournisseur, à qui il importe de mettre fin, le plus rapidement possible, à toutes ses obligations à l'égard de son ancien client.

158. Les engagements de fin de contrat peuvent être identiques quelle que soit la cause de résiliation du contrat, ou être différents selon que la résiliation découle d'une violation du contrat ou d'autres raisons. Les parties pourront souhaiter aborder dans leur contrat notamment les questions suivantes.

Délais d'exportation

159. Les parties peuvent préciser dans le contrat un délai d'exportation, qui sera suffisamment long pour permettre au client d'effectuer dans de bonnes conditions la migration de ses données et autres contenus vers un autre système.

Accès du client aux contenus faisant l'objet de l'exportation

160. Le contrat précisera les données et autres contenus qui sont susceptibles d'être exportés ainsi que les modalités d'accès des clients à ces données, y compris les éventuelles clefs de déchiffrement qui pourraient être détenues par le fournisseur ou des tiers (voir première partie, par. 28). Pour faciliter cette exportation et limiter au maximum l'intervention du fournisseur, les parties peuvent convenir d'un arrangement de séquestre (c'est-à-dire l'intervention d'un tiers autorisé à remettre automatiquement au client le code source, les clefs de déchiffrement ou d'autres éléments lui donnant accès à ses données et autres contenus en cas de survenue de certains événements, notamment la résiliation du contrat (voir aussi par. 153 ci-avant)). Le contrat précise également, autant que possible, les options d'exportation (notamment les formats et les processus), tout en reconnaissant la possibilité qu'elles changent au fil du temps.

Aide à l'exportation apportée par le fournisseur

161. Le fournisseur ne sera peut-être pas toujours disposé à aider activement le client à exporter ses données vers un autre système, mais il pourra être tenu, de par la loi, de veiller à ce que cette exportation soit possible et simple. Lorsque les parties conviennent de l'intervention du fournisseur dans l'exportation des données client, le contrat peut préciser les détails, comme la portée, la procédure et la durée de cette assistance. Le fournisseur pourra exiger d'être payé séparément pour les frais relatifs à l'assistance à l'exportation. Dans ce cas, les parties pourront fixer le prix de cette assistance dans le contrat ou convenir de se reporter à la liste des tarifs du fournisseur à un moment donné. Autrement, les parties peuvent convenir qu'une telle assistance fait partie du prix du contrat et qu'aucun frais supplémentaire ne sera facturé si la résiliation du contrat résulte d'une violation par le fournisseur.

Suppression de données

162. Le contrat pourra devoir préciser les règles relatives à la **suppression des données** de l'infrastructure en nuage du fournisseur lors de l'exportation ou à l'expiration de la période prévue dans le contrat pour l'exportation. Cette suppression pourra être effectuée automatiquement par le fournisseur, par exemple en cas de survenue de certains événements, à l'expiration de délais convenus par les parties ou lorsque la loi l'exige. Autrement, les données peuvent uniquement être supprimées à la demande du client et suivant ses instructions spécifiques. Les parties peuvent convenir que la suppression de données à venir sera notifiée au client et que ce dernier se verra remettre une attestation, un rapport ou une déclaration confirmant que les données ont été supprimées, notamment des systèmes des tiers.

Conservation de données après la fin du contrat

163. Le fournisseur peut être tenu de conserver les données client par la loi, en particulier la législation sur la protection des données, cette dernière pouvant par ailleurs préciser une durée de conservation. Les parties peuvent convenir de la conservation des données du client par le fournisseur après la fin du contrat. Certains fournisseurs peuvent proposer, contre rémunération, de les conserver pendant une certaine période après la fin du contrat.

164. Les parties peuvent prévoir des exigences particulières concernant les données qui ne sont pas ou ne peuvent pas être retournées au client et dont la suppression ne serait pas possible. Par exemple, le contrat peut prévoir que toutes les informations personnelles doivent être désidentifiées et que les données doivent être conservées sous forme chiffrée, ou dans un format utilisable et interopérable permettant leur extraction si besoin est. Les parties peuvent aussi convenir de leurs responsabilités respectives en ce qui concerne la conservation des données dans le format spécifié après la fin du contrat.

Clause de confidentialité après la fin du contrat

165. Les parties peuvent convenir d'une clause de confidentialité applicable après la fin du contrat. Les obligations de confidentialité peuvent survivre au contrat pendant un nombre d'années spécifié après sa résiliation (par exemple, cinq ou sept ans) ou se poursuivre indéfiniment, en fonction de la nature des données et autres contenus des clients qui ont été placés dans l'infrastructure en nuage du fournisseur.

Audits après la fin du contrat

166. Les audits à réaliser après la fin du contrat peuvent être convenus par les parties ou imposés par la loi. Les parties peuvent s'entendre sur les conditions d'exécution de ces audits, y compris pour ce qui est du calendrier et de la répartition des coûts.

Reliquats de compte

167. Les parties peuvent s'entendre sur les conditions de restitution au client du reliquat de son compte ou sur la déduction du montant de ce reliquat des sommes qui resteraient éventuellement dues au fournisseur, notamment pour les activités de fin de contrat ou pour régler des dommages-intérêts.

N. Règlement des litiges

Méthodes de règlement des litiges

168. Les parties peuvent convenir du mode de règlement des éventuels différends contractuels. Parmi ces méthodes figurent la négociation, la médiation, la conciliation, le règlement des litiges en ligne, l'arbitrage et la procédure judiciaire. Différents types de différends peuvent justifier la mise en œuvre de différentes procédures de règlement. Ainsi, les litiges portant sur des questions financières et techniques peuvent être soumis à la décision contraignante d'un tiers expert (qu'il s'agisse d'un particulier ou d'un organisme) tandis que des négociations directes entre les parties peuvent s'avérer plus efficaces pour résoudre d'autres types de différends. Pour les litiges de faible montant, les négociations assistées ou la médiation en ligne peuvent constituer des méthodes rapides et économiques permettant aux parties de parvenir à un accord en ligne. Pour les litiges portant sur un montant plus élevé, le règlement des litiges en ligne spécifique à l'informatique en nuage peut offrir une plateforme spécialisée compétente et faciliter les procédures judiciaires. La législation de certains pays peut imposer aux parties d'épuiser certains mécanismes alternatifs de règlement des litiges avant de pouvoir saisir la justice.

Procédures arbitrales

169. Si les parties en sont convenues, les différends qui ne sont pas réglés à l'amiable peuvent être soumis à l'arbitrage. Toutes les questions ne peuvent toutefois pas être réglées par cette voie ; certaines doivent, de par la loi, être tranchées par un tribunal. Les parties pourront par conséquent souhaiter vérifier l'arbitrabilité de leur différend avant d'opter pour ce mode de règlement. La clause d'arbitrage contenue dans un contrat renverra généralement à un règlement d'arbitrage destiné à régir toute procédure arbitrale. Le contrat peut comprendre une clause type faisant référence à l'utilisation d'un règlement internationalement reconnu pour la conduite des procédures de règlement des différends (par exemple, le Règlement d'arbitrage de la CNUDCI). À défaut d'une telle précision, la procédure arbitrale est normalement régie par le droit procédural de l'État où l'arbitrage se déroule ou, si une institution arbitrale est choisie par les parties, par le règlement de cet organisme.

Règlement des litiges en ligne

170. Les parties peuvent opter pour un mécanisme de règlement des litiges en ligne pour certaines, voire toutes les catégories de litiges découlant de leur contrat, sous réserve des limites imposées par la loi. Le contrat pourra préciser la nature des questions soumises à ce type de règlement, la plateforme utilisée et les règles à appliquer dans la procédure. Dans certains cas, le règlement des litiges en ligne peut faire partie intégrante de l'ensemble de services en nuage offert par le fournisseur, avec la possibilité d'une exclusion expresse.

171. La procédure de règlement des litiges en ligne comprend généralement les étapes suivantes : a) la négociation menée entre les parties par l'intermédiaire de la plateforme de règlement des litiges en ligne ; b) le règlement assisté par un tiers neutre désigné qui communique avec les parties pour tenter de parvenir à un accord ; et c) la dernière étape, lors de laquelle l'administrateur de la procédure de règlement des litiges en ligne ou le tiers neutre présente aux parties la nature de la dernière étape et la forme que celle-ci pourrait prendre. Le résultat de la procédure n'est pas contraignant pour les parties, à moins que le contrat ou la loi applicable n'en disposent autrement.

Procédure judiciaire

172. Si une procédure judiciaire doit avoir lieu, plusieurs États pourront se déclarer compétents en raison de la nature particulière des **services d'informatique en nuage**. Dans la mesure du possible, les parties peuvent convenir d'une clause attributive de compétence les obligeant à soumettre tout litige à un tribunal particulier (voir par. 175 à 181 ci-après).

Conservation des données

173. Pendant la phase de règlement du litige, il peut être essentiel pour le client de continuer d'accéder à ses données, notamment aux **métadonnées** et autres **données dérivées des services en nuage**, non seulement aux fins de la continuité de ses opérations, mais aussi aux fins de sa participation à la procédure de règlement (par exemple, pour étayer une demande ou une demande reconventionnelle). Le contrat peut prévoir expressément qu'en cas de différend opposant les parties, les données du client sont conservées par le fournisseur et le client peut y avoir accès pendant une période de temps raisonnable, indépendamment de la nature du litige. Les parties peuvent aussi convenir d'un arrangement de séquestre (voir par. 160 ci-avant).

Délais de prescription pour les demandes

174. Les parties peuvent préciser dans le contrat les délais de prescription applicables aux demandes. Les délais de prescription prévus dans la loi peuvent être applicables et, le cas échéant, l'emporteront sur les conditions non conformes du contrat.

O. Dispositions relatives au choix de la loi et du for

175. En règle générale, la liberté contractuelle (voir par. 34 ci-avant) permet aux parties de choisir la loi qui s'appliquera à leur contrat ainsi que la juridiction ou le for qui connaîtra des différends. Selon l'objet du litige, la législation impérative (sur la protection des données, par exemple) peut cependant l'emporter sur les clauses relatives au choix de la loi applicable et du for convenues par les parties contractantes. En outre, indépendamment du choix de la loi et du for, plusieurs lois impératives (loi sur la protection des données, loi sur l'insolvabilité, par exemple), qui peuvent émaner de plusieurs pays, peuvent être applicables au contrat.

Considérations relatives au choix de la loi et du for

176. Les clauses relatives au choix de la loi applicable et du for sont liées. La question de savoir si la loi choisie par les parties s'appliquera en fin de compte dépendra du for où la clause de choix de loi sera présentée à un tribunal ou à un autre organe juridictionnel, par exemple un tribunal arbitral. C'est la loi de ce for qui déterminera si la clause est valide et si le for respecte le choix de la loi applicable fait par les parties. En raison de l'importance de la loi du for pour la clause de choix de loi, tout contrat comportant une telle clause comporte généralement aussi une clause d'élection de for.

177. Pour choisir le for, les parties tiennent habituellement compte de l'incidence de la loi choisie ou autrement applicable et de la mesure dans laquelle une décision judiciaire rendue dans ce for serait reconnue et exécutoire dans les pays où l'exécution serait probablement demandée. Il peut être important de préserver une certaine souplesse dans les options d'exécution, en particulier s'agissant d'un environnement d'informatique en nuage où de nombreux facteurs habituellement pris en compte dans la formulation des clauses relatives au choix de la loi applicable et du for peuvent être incertains, notamment l'emplacement des actifs intervenant dans la prestation des services, et le lieu de situation du fournisseur et du client.

Loi et for obligatoires

178. La loi et le for d'un pays donné peuvent être obligatoires pour divers motifs, par exemple :

a) Le fait que les services d'informatique en nuage soient accessibles sur le territoire d'un État donné peut être suffisant pour que s'applique la législation de cet État en matière de protection des données ;

b) La nationalité ou le lieu de résidence du **sujet de données** ou des parties contractantes, en particulier du **responsable du contrôle des données**, peuvent déclencher l'application de la loi dont relève ce sujet ou la partie concernée ; et

c) Le lieu d'origine de l'activité (l'emplacement du matériel) ou le lieu auquel cette activité est destinée à des fins de profit peut déclencher l'application de la loi de ce lieu. L'utilisation d'un domaine national de premier niveau associé à un lieu particulier, d'une langue locale pour le site Web, la tarification en monnaie locale et l'existence de points de contact locaux comptent parmi les facteurs qui peuvent être pris en compte pour cette détermination.

Loi et for du lieu d'établissement du fournisseur ou du client

179. Les contrats relatifs à des **solutions d'informatique en nuage normalisées pour multiabonnés** précisent souvent qu'ils sont régis par le droit du lieu où le fournisseur a son établissement principal. En règle générale, ils accordent aux tribunaux de ce pays la compétence exclusive pour connaître de tous les litiges qui pourraient découler du contrat. Le client peut préférer la loi et la compétence de son propre pays. Ainsi, la capacité d'institutions publiques de consentir à l'application de la loi et à la compétence de pays étrangers serait très limitée. Les fournisseurs qui sont actifs dans plusieurs pays peuvent faire preuve de souplesse s'agissant d'accepter le choix de la loi et du for du pays où le client est situé.

Options multiples

180. Les parties peuvent également préciser diverses options pour le choix de la loi et du for pour différents aspects du contrat. Elles peuvent aussi opter pour la juridiction du défendeur afin d'éliminer l'avantage dont bénéficie le demandeur quand le for est celui de son pays de domicile et de favoriser ainsi le règlement informel des différends.

Absence de choix de loi ou d'élection de for

181. Les parties peuvent préférer ne pas inclure, dans leur contrat, de clause relative au choix de la loi applicable et du for, laissant la question ouverte à un examen ultérieur, le cas échéant. Dans certains cas, il pourrait s'agir de la seule solution viable. Le règlement des litiges en ligne peut aussi faire partie de la solution pour les questions de compétence et de droit applicable (voir par. 170 et 171).

P. Notifications

182. Les clauses de notification portent généralement sur la forme, la langue, le destinataire et les moyens de notification, ainsi que sur le moment d'entrée en vigueur de la notification (lors de la remise, de l'expédition ou de l'accusé de réception). En l'absence de dispositions législatives contraignantes, les parties peuvent convenir des formalités de notification, qui peuvent être uniformes ou varier en fonction de l'importance, de l'urgence et d'autres considérations. Elles pourront convenir d'exigences plus strictes que pour les notifications de routine, par exemple, en cas de suspension ou de résiliation unilatérale du contrat. Les parties peuvent convenir des délais, en tenant compte de la nécessité d'assurer la **réversibilité** et la continuité des opérations. Le contrat peut contenir des références aux notifications et délais imposés par la loi.

183. Les parties peuvent opter pour que les notifications **écrites** soient remises à l'adresse physique ou électronique des personnes de contact indiquées dans le contrat. Le contrat peut préciser les conséquences juridiques d'un manquement à l'obligation de notification et de l'absence de réponse à une notification qui en exige une.

Q. Dispositions diverses

184. Les parties regroupent souvent sous l'intitulé « divers » les dispositions qui ne relèvent pas d'autres parties du contrat. Certaines d'entre elles peuvent contenir un texte normalisé figurant dans tous les types de contrats commerciaux (en quelque sorte des « dispositions standard »). Il peut s'agir, par exemple, d'une clause de sauvegarde permettant de supprimer les dispositions invalides du contrat tout en conservant le reste ou d'une clause linguistique identifiant une certaine version linguistique du contrat comme faisant foi en cas de conflit d'interprétation entre différentes versions linguistiques. Le fait de placer des clauses contractuelles au sein de ces dispositions diverses n'enlève rien à leur signification juridique. Les parties pourront adapter certaines d'entre elles aux spécificités des **services d'informatique en nuage**.

R. Modification du contrat

185. L'une ou l'autre des parties pourra souhaiter apporter des modifications au contrat. Ce dernier précisera la procédure à suivre pour introduire des modifications et les rendre effectives. Il pourra également aborder les conséquences du rejet des modifications par l'une ou l'autre partie.

186. Compte tenu de la nature des **services d'informatique en nuage**, il peut être difficile de distinguer les changements qui constituent une modification du contrat de ceux qui n'en constituent pas. Par exemple, l'utilisation par le client de n'importe quelle option mise à sa disposition dès l'entrée en vigueur du contrat ne constituerait pas nécessairement une modification du contrat initial, pas plus que des changements des services qui résulteraient de l'entretien ordinaire et d'autres activités du fournisseur prises en compte dans le contrat (voir par. 105 et 106 ci-avant). En revanche, l'ajout d'éléments non couverts dans les conditions initialement convenues et justifiant ainsi des modifications de prix peut constituer une modification du contrat. Toute mise à jour entraînant des changements importants des conditions et politiques convenues antérieurement peut également constituer une modification du contrat.

187. L'ampleur des modifications susceptibles d'être apportées aux contrats publics peut être limitée par les règles de passation des marchés publics, qui restreignent généralement la liberté des parties de renégocier les clauses d'un marché ayant fait l'objet d'une procédure d'adjudication publique.

188. Compte tenu des modifications fréquentes des conditions initialement convenues, chaque partie pourra souhaiter conserver sa propre copie de l'ensemble de ces conditions initialement convenues et leurs modifications.

Glossaire

Accord de niveau de service : Partie du contrat d'informatique en nuage entre le fournisseur et le client où sont indiqués les services d'informatique en nuage couverts par le contrat et le niveau de service attendu ou à atteindre aux termes du contrat (voir les **paramètres de performance**).

Audit : Processus consistant à examiner le respect des exigences légales et contractuelles ou des normes techniques. Il peut couvrir des aspects techniques (tels que la qualité et la sécurité du matériel et des logiciels) ; le respect de toute norme sectorielle applicable ; et l'existence de mesures appropriées, y compris l'isolement, pour empêcher l'accès non autorisé au système et son utilisation et pour garantir l'intégrité des données. L'audit peut être interne ou externe ou être effectué par un tiers indépendant nommé par le fournisseur ou par le client, ou par les deux parties. L'**accord de niveau de service** peut contenir des paramètres de performance spécifiques en matière d'audit, par exemple prévoir que les services fournis au titre du contrat doivent être certifiés au moins une fois par an par un auditeur indépendant, à l'aide de la norme de sécurité prévue dans le contrat.

Données dérivées des services en nuage : Données placées sous le contrôle du fournisseur qui sont dérivées de l'utilisation, par le client, des services d'informatique en nuage proposés par ce fournisseur. Il s'agit notamment des **métadonnées** et de toutes autres données enregistrées générées par les fournisseurs, qui indiquent l'identité des utilisateurs des services, les dates et heures d'utilisation des services, ainsi que les fonctions et les types de données concernés. Elles peuvent également englober des renseignements sur les utilisateurs autorisés, leurs identifiants, et les configurations, personnalisations et modifications éventuelles.

Données personnelles : Données à caractère sensible ou non qui peuvent servir à identifier la personne physique à laquelle elles se rapportent. Dans certains pays, la définition des données personnelles peut englober toutes les données ou informations directement ou indirectement liées ou relatives à une personne identifiée ou identifiable (voir le **sujet de données**).

Droits des sujets de données : Droits associés aux **données personnelles** des **sujets de données**. En fonction de la législation, les **sujets de données** peuvent bénéficier du droit d'être informés de toutes les informations importantes relatives à leurs données personnelles, notamment l'emplacement de ces données, leur utilisation par des tiers, et d'éventuelles fuites et autres violations. Ils peuvent également disposer du droit d'accéder à tout moment à ces données personnelles, du droit à l'effacement (conséquence du droit à l'oubli), du droit d'en limiter le **traitement** et du droit à la **portabilité** de ces données.

Écrit ou **par écrit** : Informations accessibles de façon à pouvoir être utilisées ultérieurement à des fins de référence. Le terme s'applique aux informations disponibles sur papier ou contenues dans une communication électronique. Le mot « accessible » implique que les informations se présentant sous la forme de données informatisées doivent pouvoir être lues et interprétées et que le logiciel qui pourrait être nécessaire pour assurer cette lisibilité doit être conservé. Les mots « être utilisées » visent tant l'usage par des personnes que le traitement informatique.

Exigences en matière de localisation des données : Exigences relatives à l'emplacement des données et d'autres contenus, des centres de données ou des fournisseurs. Elles peuvent interdire que certaines données (notamment des **métadonnées** et sauvegardes) soient stockées dans certains territoires ou pays, ou passent par ceux-ci, ou exiger pour ce faire l'autorisation préalable d'une instance publique compétente. Elles sont fréquemment énoncées dans des lois et règlements relatifs à la protection des données, lesquels sont susceptibles d'interdire en particulier que les **données personnelles** soient stockées ou passent dans des pays qui ne respectent pas certaines normes en matière de protection des données personnelles.

Incident de sécurité : Événement indiquant que l'intégrité du système ou des données a été compromise ou que les mesures adoptées pour protéger ceux-ci n'ont pas été efficaces. Un incident de sécurité perturbe le fonctionnement normal. On mentionnera comme exemple une tentative d'accès de sources non autorisées aux systèmes ou aux données, une perturbation non planifiée des services ou un déni de service, le traitement ou le stockage non autorisés de données et l'introduction de changements non autorisés dans l'infrastructure du système.

Infrastructure en tant que service (IaaS) : Types de **services d'informatique en nuage** par le biais desquels le client peut obtenir et utiliser des ressources liées au traitement, au stockage et aux réseaux. Le client ne gère ni ne contrôle les ressources physiques ou virtuelles sous-jacentes, mais il contrôle les systèmes d'exploitation, les espaces de stockage et les applications déployées qui font usage de ces ressources. Il peut également exercer un contrôle restreint sur certaines composantes des réseaux (par exemple, les pare-feu hôtes).

Interopérabilité : Capacité de deux ou plusieurs systèmes ou applications à échanger des informations et à utiliser mutuellement les informations échangées.

Licence de propriété intellectuelle : Contrat conclu entre un titulaire de droits de propriété intellectuelle (donneur de licence) et une personne autorisée à utiliser ces droits (preneur de licence). Ces contrats imposent habituellement des restrictions et des obligations quant à la portée du contrat et à la manière dont le preneur de licence ou les tiers peuvent utiliser le bien sous licence. Par exemple, les logiciels et les contenus visuels (modèles, mises en page et images) peuvent faire l'objet d'une licence en vue d'une exploitation spécifique, ne permettant pas la copie, la modification ou l'amélioration, et être limités à un support donné. Les licences peuvent être limitées à un marché particulier (par exemple, marché national ou (sous-)régional), à un nombre d'utilisateurs ou d'appareils donné, ou être limitées dans le temps. Les accords de sous-licence peuvent être interdits. Le donneur de licence peut exiger que le titulaire des droits de propriété intellectuelle soit mentionné chaque fois que ceux-ci sont utilisés.

Logiciel en tant que service (**SaaS**) : Types de **services d'informatique en nuage** par le biais desquels le client peut utiliser les applications du fournisseur dans le nuage.

Métadonnées : Informations de base sur les données (comme l'auteur, la date de création, la date de modification et la taille du fichier). Elles contribuent à faciliter la recherche et l'utilisation des données et peuvent être requises pour garantir l'authenticité des données enregistrées. Elles peuvent être générées par le client ou par le fournisseur.

Modèle ajusté aux fuseaux horaires (« Follow-the-sun ») : Modèle dans lequel la charge de travail est répartie entre plusieurs sites géographiques de façon à mieux équilibrer les ressources et la demande. Ce modèle peut viser à fournir des services 24 heures sur 24 et à minimiser la distance moyenne entre les serveurs et les utilisateurs finaux pour essayer de limiter les **temps de latence** et de maximiser la vitesse de transmission des données entre appareils (taux de transfert des données ou débit).

Modèles de déploiement : Différentes manières d'organiser les services d'informatique en nuage en fonction du contrôle et du partage des ressources physiques ou virtuelles :

a) **Nuage public** : Les **services d'informatique en nuage** sont susceptibles d'être proposés à n'importe quel client et les ressources sont contrôlées par le fournisseur ;

b) **Nuage communautaire** : Les **services d'informatique en nuage** sont mis à la disposition exclusive d'un groupe donné de clients liés les uns aux autres et ayant des exigences communes, et les ressources sont contrôlées par au moins un membre de ce groupe ;

c) **Nuage privé** : Les **services d'informatique en nuage** sont mis à la disposition exclusive d'un seul client, qui contrôle les ressources ;

d) **Nuage hybride** : Solution faisant intervenir au moins deux modèles de déploiement différents.

Objectif de délai de reprise : Délai dans lequel tous les services d'informatique en nuage et les données doivent être rétablis à la suite d'une interruption imprévue.

Objectif de point de reprise : Durée maximale précédant une interruption de service imprévue pendant laquelle les modifications apportées à des données risquent d'être perdues. Si le contrat précise par exemple un objectif de point de reprise équivalent à deux heures avant l'interruption des services, cela signifie que toutes les données devraient être accessibles après la reprise dans la forme où elles existaient deux heures avant l'interruption.

Paramètres de performance : Paramètres quantitatifs (objectifs chiffrés, indicateurs ou fourchette de performance) ou qualitatifs (assurance de la qualité des services). Ils peuvent mesurer la conformité aux normes applicables, y compris la date d'expiration de toute certification de conformité (par exemple, le fournisseur doit avoir mis en œuvre une politique de gestion des clefs conforme à la norme internationale définie dans le contrat). Pour être significatifs, les paramètres devraient permettre au client de mesurer, de manière simple et vérifiable, les performances qui revêtent de l'importance pour lui. Ils peuvent varier en fonction des risques encourus et des besoins de l'entreprise (par exemple, la criticité de certains services, données ou applications et la priorité correspondante en matière de reprise). Par exemple, un système non essentiel conçu pour utiliser le nuage à des fins d'archivage n'aura pas besoin du même **temps de disponibilité** ou d'autres conditions de l'**accord de niveau de service** que des opérations essentielles ou en temps réel.

Partenaires de services d'informatique en nuage (notamment auditeurs de services en nuage, courtiers de services en nuage et intégrateurs de système) : Personnes qui mènent des activités de soutien ou auxiliaires à celles des fournisseurs, des clients ou des deux. Les auditeurs de services en nuage procèdent à des **audits** de la prestation et de l'utilisation de **services d'informatique en nuage**. Les courtiers de services en nuage ou les intégrateurs de système apportent leur assistance aux parties à divers égards, par exemple pour trouver la meilleure solution en matière de nuage, négocier des conditions acceptables et organiser la migration du client vers le nuage.

Pérennité du stockage de données : Probabilité que les données stockées dans le nuage ne soient pas perdues pendant la durée du contrat. Elle peut être exprimée dans le contrat sous la forme d'une cible mesurable par rapport à laquelle le client évaluera les mesures prises par le fournisseur pour assurer cette pérennité (par exemple, données intactes/données intactes + données perdues pendant un délai spécifié (par exemple, un mois calendaire)). Il faudra définir dans cette formule le type de données (par exemple, fichiers, bases de données, codes, applications) et l'unité de mesure (nombre de fichiers, longueur de bit).

Plateforme en tant que service (**PaaS**) : Types de **services d'informatique en nuage** par le biais desquels le client peut déployer, gérer et exploiter dans le nuage des applications ou des logiciels qu'il a créés ou acquis en utilisant un ou plusieurs langages de programmation et environnements d'exécution existants pris en charge par le fournisseur.

Politique d'utilisation acceptable : Partie du contrat d'informatique en nuage entre le fournisseur et le client où sont définies les limites de l'utilisation par le client et ses utilisateurs finaux des services d'informatique en nuage couverts par le contrat.

Portabilité : Capacité de transférer facilement des données, des applications et d'autres contenus d'un système à un autre (c'est-à-dire à faible coût, avec un minimum de perturbations et sans avoir à ressaisir les données, à réorganiser les processus ou à reprogrammer les applications). La portabilité est assurée s'il est possible de récupérer les données dans le format accepté dans un autre système ou par

une transformation simple et directe à l'aide d'outils couramment disponibles. L'**accord de niveau de service** peut contenir des paramètres de performance liés à la portabilité, par exemple un paramètre selon lequel le client peut récupérer ses données par le biais d'un seul lien de téléchargement ou d'une interface de programmation d'applications (API) bien documentée ; ou selon lequel le format de données est structuré et documenté de manière suffisante pour permettre au client de le réutiliser ou de le restructurer dans un format différent s'il le désire.

Règlements sectoriels : Règlements relatifs aux finances, à la santé ou au secteur public, ou à d'autres secteurs ou professions particuliers (par exemple, en ce qui concerne le secret professionnel auquel sont tenus les avocats et les professionnels de santé) et règles relatives au traitement des informations classifiées (c'est-à-dire, au sens large, les informations dont la loi ou un règlement limitent l'accès à certaines catégories de personnes).

Représentant de l'insolvabilité : Personne ou organe habilité à administrer le redressement ou la liquidation des biens du débiteur insolvable dans le cadre d'une procédure d'insolvabilité.

Responsable du contrôle des données : Personne qui décide de l'objet et des moyens du traitement des **données personnelles**.

Responsable du traitement des données : Personne qui traite les données pour le compte du **responsable du contrôle des données**.

Réversibilité : Processus permettant au client d'extraire ses données, applications et autres contenus connexes du nuage, et au fournisseur de supprimer les données du client et autres contenus connexes après une période convenue.

Services d'informatique en nuage en couches : Dans ce cadre, le fournisseur n'est pas le propriétaire de l'ensemble, ou d'une partie, des ressources informatiques qu'il utilise pour fournir des services d'informatique en nuage à ses clients ; il est lui-même le client de tout ou partie des **services d'informatique en nuage**. Par exemple, le fournisseur de services de type **PaaS** ou **SaaS** peut utiliser les infrastructures de stockage et de serveur (centres de données, serveurs de données) dont une autre entité est propriétaire ou qu'elle fournit. Par conséquent, un ou plusieurs sous-fournisseurs peuvent intervenir dans la prestation des services d'informatique en nuage au client. Ce dernier ne saura pas nécessairement quelles couches participent à la prestation de services à un moment donné, ce qui complique l'identification et la gestion des risques. Les services d'informatique en nuage en couches sont fréquents dans le modèle **SaaS** en particulier.

Services d'informatique en nuage : Services en ligne caractérisés par :

a) Un **large accès via le réseau**, ce qui signifie qu'il est possible d'accéder aux services par l'intermédiaire du réseau à partir de tout endroit où celui-ci est disponible (par exemple, par Internet), au moyen de divers appareils tels que téléphones portables, tablettes et ordinateurs portables ;

b) Le **service mesuré**, caractéristique qui permet de contrôler l'utilisation des ressources et de facturer le client en conséquence (facturation **à l'usage**) ;

c) **L'architecture multilocataire**, c'est-à-dire l'allocation des ressources physiques et virtuelles à de multiples utilisateurs dont les données sont conservées séparément et inaccessibles aux autres ;

d) Le **libre-service à la demande**, ce qui signifie que le client utilise les services selon ses besoins, automatiquement ou moyennant une interaction minime avec le fournisseur ;

e) L'**élasticité** et l'**extensibilité**, c'est-à-dire la capacité d'adaptation rapide à la hausse ou à la baisse de la consommation de services selon les besoins du client, y compris pour s'adapter aux tendances à grande échelle de l'usage de ressources (par exemple, variations saisonnières) ;

f) La **mutualisation des ressources**, c'est-à-dire la possibilité qu'a le fournisseur de regrouper les ressources physiques ou virtuelles pour servir un ou plusieurs clients, sans que ceux-ci contrôlent les processus en jeu ou en aient connaissance ;

g) Une **large gamme de services**, allant de la fourniture et de l'utilisation de services de connectivité et d'informatique de base (comme le stockage, les courriers électroniques et les applications bureautiques) à la fourniture et à l'utilisation de l'ensemble des infrastructures informatiques physiques (par exemple, serveurs et centres de données) et des ressources virtuelles nécessaires pour que le client puisse créer sa propre plateforme informatique, ou déployer, gérer et exploiter des applications ou des logiciels créés ou acquis par le client. L'infrastructure en tant que service (**IaaS**), la plateforme en tant que service (**PaaS**) ou le logiciel en tant que service (**SaaS**) sont des types de services d'informatique en nuage.

Solutions d'informatique en nuage normalisées pour multiabonnés : **Services d'informatique en nuage** fournis à un nombre illimité de clients en tant que ressource ou produit de masse, à des conditions standard non négociables déterminées par le fournisseur. Dans ce type de solutions, on trouve fréquemment des clauses de non-responsabilité générales et d'exonération de responsabilité du fournisseur. Le client pourra comparer différents fournisseurs et les contrats qu'ils proposent et choisir celui qui correspondra le mieux à ses besoins, mais il ne pourra pas négocier son contrat.

Sujet de données : Personne physique qui peut être identifiée, directement ou indirectement, par des données, notamment des identifiants tels que le nom, un numéro d'identification, un emplacement et tout facteur se rapportant à l'identité physique, génétique, mentale, économique, culturelle ou sociale de la personne. Dans un certain nombre de pays, les sujets de données jouissent, en vertu des règles de protection des données ou de confidentialité, de certains droits relatifs aux données susceptibles de les identifier. Ces règles peuvent encourager l'inclusion, dans l'**accord de niveau de service**, de paramètres de performance se rapportant spécifiquement à la protection des données, par exemple un paramètre selon lequel les services fournis au titre du contrat doivent être certifiés au moins une fois par an par un auditeur indépendant qui applique la norme de protection des données/confidentialité prévue dans le contrat. (Voir aussi les définitions des **droits des sujets de données** et des **données personnelles**.)

Suppression des données : Série d'opérations visant à supprimer de manière irréversible des données, y compris les sauvegardes et métadonnées correspondants, et autres contenus de l'infrastructure d'informatique en nuage (physique et virtuelle). Dans certains cas, la suppression des données exige la destruction de l'infrastructure physique (par exemple, serveurs) sur laquelle celles-ci sont stockées. L'**accord de niveau de service** peut contenir un paramètre de performance spécifique lié à la suppression des données, par exemple selon lequel le fournisseur doit veiller à ce que les données du client soient supprimées de manière effective, irrévocable et définitive à la demande de celui-ci dans un certain délai précisé dans le contrat et conformément à la norme ou méthode prévue dans le contrat.

Temps d'arrêt ou d'interruption : Période pendant laquelle les clients n'ont pas accès aux services d'informatique en nuage. Cette période est exclue du calcul du **temps de disponibilité** ou de fonctionnement sans interruption. On inclut généralement dans le temps d'arrêt le temps nécessaire pour la maintenance et les mises à jour. Dans l'**accord de niveau de service**, cette période peut être définie comme le nombre d'interruptions d'une durée limitée acceptables pendant une certaine période de temps, par exemple pas plus d'une interruption d'une heure par jour, celle-ci ne pouvant intervenir entre 8 heures et 17 heures.

Temps de disponibilité : Période pendant laquelle les services d'informatique en nuage sont accessibles et susceptibles d'être utilisés. Elle peut être exprimée en tant que quantité ou pourcentage, en tant que formule détaillée ou encore en tant que dates

ou jours et heures spécifiques pendant lesquels le service d'une application particulière doit absolument être disponible.

Temps de latence : Temps qui s'écoule entre la demande du client et la réponse du fournisseur. Ce temps, qui affecte l'exploitabilité pratique des **services d'informatique en nuage**, est généralement exprimé en millisecondes dans l'**accord de niveau de service**.

Temps de réaction initiale : Délai qui s'écoule entre le moment où un client signale un incident et la première réaction du fournisseur.

Traitement des données personnelles : Collecte, enregistrement, organisation, stockage, adaptation ou altération, extraction, consultation, utilisation, divulgation par transmission, diffusion ou toute autre forme de mise à disposition, alignement ou combinaison, blocage, effacement ou destruction de données personnelles.

Verrouillage : Situation dans laquelle le client dépend d'un fournisseur unique parce que les coûts liés à un changement de prestataire sont considérables. Dans ce contexte, la notion de coût s'entend au sens large comme englobant non seulement les dépenses monétaires, mais aussi l'effort, le temps et les aspects relationnels.