Les bonnes pratiques contractuelles en matière de SLA

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

Mardi 1er février 2022

Objectif

Préciser les concepts et définitions nécessaires aux fournisseurs pour élaborer leur SLA et décrire les caractéristiques de leur offre

Définition des SLA

Pas de définition légale

Pratique contractuelle importée des États-Unis qui se traduit par Accord ou engagement de niveau de service

Un document technique proposé par le fournisseur

Gestion de la performance

Un accord de niveau de service (SLA) est un engagement entre un fournisseur de services et un client qui précise et fixe le niveaux de performance de certains services.

Obligation ?

Les SLA ne sont pas légalement obligatoires (même vis-à-vis des consommateurs)

Principe de liberté contractuelle

Pourquoi les clients exigent un SLA ?

Plusieurs raisons :

- Lorsque le client est face à une *solution nouvelle*, le fournisseur doit renforcer son rôle de conseil et préciser les contours de son service et de ses engagements.
- La *multiplication des acteurs* peut inquiéter le client. Le Cloud n'est pas la propriété du fournisseur qui ne le maitrise donc pas entièrement (datacenter, hébergeur, opérateur télécoms, éditeur de l'application, etc. …).
- *L'externalisation et la distance entre le client*, ses applications, ses données peut également l'inquiète.
- La *nature essentielle de l'activité externalisée et le besoin de sécurisation* qui en découle.
- La *nature fluctuante de l'activité externalisée et les pics d'activités* qui en découlent.

=> Le client a besoin de savoir qui fait quoi et comment

Quels intérêts pour le fournisseur ?

Parmi les avantages d'une telle pratique, il y a :

- *l'identification des points faibles* des services afin de lancer des actions d'amélioration.
- *l'identification des actions clients et utilisateurs entraînant des incidents* afin d'améliorer ces situations.
- Le *cantonnement des obligations de résultat*.

=> l'amélioration graduelle de la qualité de service

Des types de SLA en fonction des objectifs

Définir des objectifs de niveau de service relatifs à :

- La **performance** : choisir un indicateur de performance
- La **sécurité** et la gestion des données autres que personnelles : choisir un indicateur de fiabilité + Clause Confidentialité
- 3. Autre ?

Il n’existe pas de liste prédéfinie des métriques: la liberté contractuelle est reine en la matière.

Quels contrats sont concernés?

Il n’existe par un modèle de SLA.

L’engagement de niveau de service dépend du contrat :

- ❖ les contrats de fourniture d’« infrastructure » : hébergement, IaaS, PaaS
- ❖ les contrats de « service » : SaaS, infogérance, Support

Souvent des services dépendent d’autres fournisseurs de services :

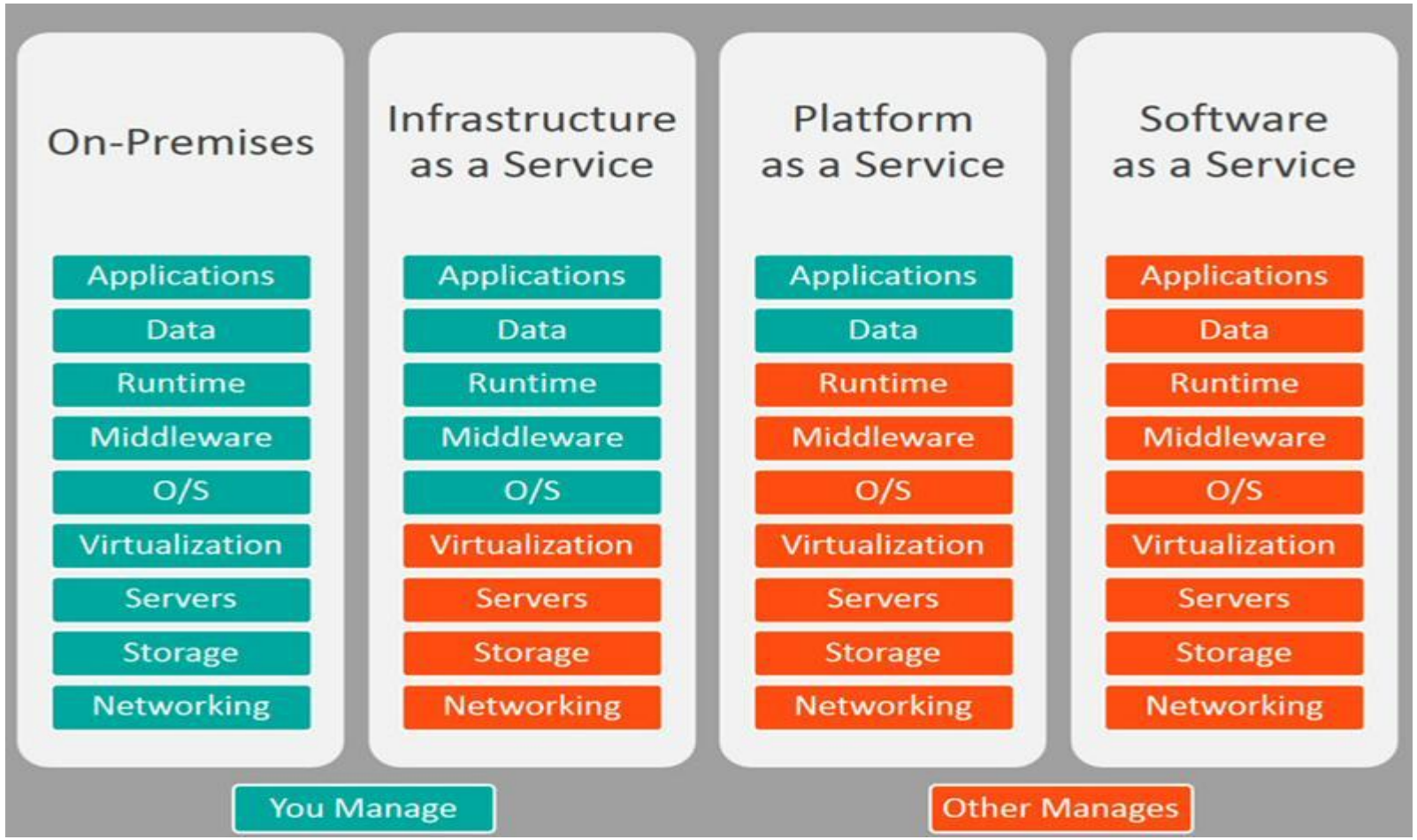
- ❖ Répartition des rôles (éditeur – intégrateur – fournisseur de services managés…) :
- ✓ ne s’engager que sur ce que l’on contrôle effectivement
- ✓ reproduire les engagements des sous-traitants
- ✓ possible de créer des SLA conjointes avec les autres fournisseurs.

Quels contrats sont concernés ?

https://fr.itpedia.nl/2019/06/13/in-de-knel-tussen-paas-en-devops/

Vert : client

Orange : fournisseur



Un engagement contractuel (1/2)

L’accord de niveau de service :

- peut faire partie des articles du contrat (texte principal) pour certains aspects
- Ou être inséré dans une annexe dédiée
- Ou être accessible via un lien hypertexte
- Ou les SLA confidentiels peuvent être accessibles à partir d’un portail client sécurisé par exemple

Opposable aux parties si accepté par renvoi (clause « documents contractuels »).

Négocié entre les parties.

Le plus souvent, c’est un document distinct du contrat qui définit précisément les services attendus ainsi que leur niveau.

Un SLA n’est pas un document technique et devrait être écrit en termes d’affaires, claires et concis : éviter le jargon légal et technique, la terminologie technique non pertinente, fournir un lexique si nécessaire.

Faire relire le SLA par une ressource externe au processus.

Si un aspect d'un service n'a pas été convenu avec le client, il ne s'agit pas d'un "SLA".

Un engagement contractuel (2/2)

Issu de la volonté des parties, il engage et chaque partie peut engager la responsabilité de l'autre à son appui.

Il comporte des obligations de faire ou de ne pas faire.

Il a un impact sur la répartition des responsabilité.

Des dommages et intérêts peuvent être alloués à la partie lésée :

- Il permet au client d'apprécier l'exécution ou non de certains engagements ; client qui dispose alors des moyens de prouver l'inexécution du fournisseur.
- Il est aussi une protection pour le fournisseur qui dispose d'un moyen de prouver que le client a eu ce à quoi le fournisseur s'était engagé.

Le contenu du SLA

Le contenu d’un accord de niveau de service dépend du service.

Possible de proposer plusieurs niveaux de SLA (standard, medium, premium…) et coût associé

Il comporte

- les objectifs à atteindre (indicateurs de performance / métriques).
- les actions préventives
- les actions correctives

=> Les points clés/standards du SLA

Les points clés du SLA

1. Une description détaillée du service fourni

Cette description doit intégrer et détailler les éléments manquants dans le corps principal du contrat.

Par exemple : Dans le cas d'une connectivité réseau IP, le SLA décrit les fonctions d'exploitation et la maintenance de l'équipement réseau, la bande passante de connexion à fournir, etc.

NB : Parallèle avec les finalités des opérations de traitement des données à caractère personnel.

Les points clés du SLA

1. Exemple Contrat de support premium

Article 2. Description du Support Premium

Le Support Premium permet au Client de bénéficier, en supplément des moyens de contacts mis à sa disposition dans le cadre du Support Standard XXcloud (chatbox, outil de ticketing), d'une ligne téléphonique via laquelle celui-ci peut joindre des interlocuteurs privilégiés XXcloud pour ses différentes demandes techniques ou d'assistance (configuration de Services, accompagnement dans la gestion des commandes, etc.) pendant les heures ouvrées telles qu'indiquées sur le Site Internet d'XXcloud.

Les demandes du Client sont prises en charge de manière prioritaire par rapport au Support Standard XXcloud, indépendamment du canal de communication utilisé. Le Support XXcloud est fourni en français uniquement, et les prestations d'information concernant les Services sont fournies en heures ouvrées uniquement. Les infrastructures XXcloud sont supervisées et maintenues en condition opérationnelle 365/24/7, Les informations relatives à la résolution des incidents sont disponibles sur le site xxx. Le Support Premium est délivré conformément aux Conditions Générales du Contrat. XXcloud est soumis à une obligation de moyens.

Les points clés du SLA

2. Une répartition claire des rôles et responsabilités quant au niveau d'exploitation du service

- Qui fait quoi à apprécier à partir du niveau de contrôle « de facto » sur tel ou tel aspect du service
- Lister les cas d'exclusion de l'engagement lorsque le client intervient.

NB : Parallèle avec les mesures de sécurité entre le client et le fournisseur

Les points clés du SLA

3. Les canaux de communications entre le client et le fournisseur

Outils de notification ou les coordonnées du service d’assistance du fournisseur

- Hot line téléphonique
- Email dédié
- Outil de ticketing
- Interface de contrôle

- Horaires de contrôle des performances :

Par exemple, horaires du service d’assistance du fournisseur (ne pas oublier les fuseaux horaires)

Les points clés du SLA

4. Métriques d'appréciation de la qualité de la fourniture du service (performance)

Toutes métriques inclues dans un SLA doivent être mesurables.

Il n'existe pas de liste pré-définie des métriques que le prestataire peut offrir : la liberté contractuelle est reine en la matière.

Si par exemple le client entend offrir un service web à ses users (consommateurs) via un prestataire SaaS, il serait avisé de demander des engagements de temps maximum de chargement des pages web.

Ces mesures doivent être prises et enregistrées régulièrement afin d'en assurer un suivi optimal, puisque les indicateurs révèle la qualité du service rendu.

NB : Il est primordial d'appliquer une périodicité à l'audit de ces mesures.

Les indicateurs ou métriques

4.1 Indicateurs de capacité

Pour quoi ?

- De l’espace de stockage
- Nombre de comptes utilisateurs et administratifs
- Nombre de connections simultanées
- Nombre d’utilisateurs simultanés
- SaaS, PaaS, Hébergement d’un site…

Définir la **capacité maximum** d’un service ou d’une fonctionnalité

Capacité maximum des ressources

=> espace de stockage, CPU, mémoire, etc.

Les indicateurs ou métriques

4.1 Indicateurs de capacité

Volume d'indexation quotidien ou nombre de calculs virtuels ("SVC")

« Virtual Compute (SVC) » : désigne une unité de capacités dans Cloud Platform qui comprend les ressources suivantes : calcul, mémoire et E/S »

Les indicateurs ou métriques

4.2 Indicateurs de disponibilité

Est-ce qu'un service dont la performance est très fortement dégradée peut encore être considéré comme disponible ?

Les objectifs de disponibilité :

- variation selon la période de l'année, selon la typologie d'utilisation, selon les environnements
- variation selon les environnements (de développement, de test, de production, etc.)

Disponibilité du système sur une période de temps :

- pourcentage ou formule (Disponibilité = Temps de disponibilité total – (Indisponibilité – temps de maintenance)
- donc le pourcentage du temps pendant lequel le service est disponible sur une période donnée, souvent calculé par jour, par semaine ou par mois.

Par exemple,

- un client pourrait stipuler qu'il requiert une disponibilité de 99,99 % entre 8 h et 18 h ou que l'application sera disponible 98% du temps 7 jours par semaine, 19 heures par jour.
- pourcentage de requêtes acceptées ou Nombre de requêtes satisfaites dans un laps de temps défini

Les indicateurs ou métriques

4.2 Exemple Contrat de service SaaS

(service cloud) Les Services Cloud seront disponibles 100 % du temps, tel que mesuré par XX sur chaque trimestre civil de la Durée de l'abonnement, et sous réserve des exclusions énoncées ci-dessous (l'« Engagement de niveau de service »).

Un Service Cloud est considéré comme disponible si le Client est en mesure de se connecter à son compte de Service Cloud et de lancer une recherche à l'aide du Logiciel.

OU

(SaaS) Le FOURNISSEUR fera ses meilleurs efforts pour assurer une accessibilité à la totalité des modules et fonctions du logiciel SaaS et aux Données du CLIENT, 24 heures sur 24, 7 jours sur 7, 365 jours par an, selon un taux de disponibilité de 99 % calculé sur une période d'un (1) mois par application de la formule suivante :

Taux de Disponibilité = 100% x [1 - (t/T)]

- t désigne le nombre de minutes où le Logiciel a été indisponible pendant la période d'un mois considérée,

- T désigne le nombre total de minutes dans le mois.

Les indicateurs ou métriques

4.3 Le taux d’erreur accepté

Le taux d’erreurs pour les principaux livrables, comme les erreurs de service, les sauvegardes incomplètes, les erreurs de codage ou les délais non respectés.

Les indicateurs ou métriques

4.4 Le taux d’erreur accepté + indicateur de disponibilité appliqués au Support

Comment détailler le support fourni à l’utilisateur ?

Délais de prise en charge et de résolution d’un incident base sur sa sévérité : préciser

- heures d’ouverture
- les points de départ
- les délais de réponse/prise en compte GTI : délai dans lequel le fournisseur de services commencera l'enquête sur le problème.
- les délais de résolution/traitement GTR : période au terme de laquelle le problème de service sera résolu et corrigé
- les sévérités (définitions strictes) : bloquante, majeure, mineure

Des délais de réponse plus courts lors des heures ouvrables du client.

Les indicateurs ou métriques

4.5 Le temps de réponse

- par opération
- depuis quel point de connexion le temps de réponse est-il calculé
- temps de réponse moyen - Temps de réponse maximum

Si par exemple le client entend offrir un service web à ses users (consommateurs) via un prestataire SaaS, il aura besoin d'une métrique de temps maximum de chargement des pages web.

Les indicateurs ou métriques

2. Garanties de sécurité : indicateurs de la Fiabilité

Objectifs : comment mesurer la capacité à résister aux défaillances ?

- Niveau de redondance
- Authentification et autorisation – informer l'utilisateur sur les mécanismes de sécurité
- Niveau d'assurance en référence aux standards existants (ISO 29115, IAF…), aux niveaux de certification
- Temps nécessaire pour révoquer un accès
- Protection des identifiants de connexion
- Niveau d'authentification par le prestataire et/ou un tiers
- Cryptologie : informer l'utilisateur sur les moyens de cryptologie mis en œuvre
- Gestion des incidents et reporting : informer l'utilisateur sur le temps de prise en compte et le temps de résolution
- Enregistrement et contrôle des logs : informer l'utilisateur sur les moyens d'analyse des failles de sécurité (paramétrage des fichiers logs, disponibilité des fichiers logs et durée de conservation des logs)

Les indicateurs ou métriques

2. Garanties de sécurité : exemple

Conformité et certifications

XX a obtenu un certain nombre d'attestations de conformité et de certifications d'auditeurs de premier plan dans le cadre de son engagement à respecter les normes de l'industrie dans le monde entier et dans le cadre de ses efforts pour protéger les données de nos clients. Les attestations/certifications de conformité suivantes sont disponibles :

SOC 2 Type II : Cloud Platform fait publier un rapport d'audit annuel SOC 2 Type 2. L'audit SOC 2 évalue les processus de sécurité, de disponibilité, d'intégrité des processus et de confidentialité d'une organisation pour fournir une assurance sur les systèmes qu'une entreprise utilise pour protéger les données des clients. Si vous avez besoin de l'attestation SOC 2 Type 2 pour examen, contactez votre représentant commercial pour en faire la demande.

ISO 27001 : Cloud Platform est certifié ISO/IEC 27001:2013. ISO/IEC 27001:2013 est une norme pour un système de gestion de la sécurité de l'information, spécifiant les politiques et procédures pour tous les contrôles juridiques, physiques et techniques utilisés par une organisation pour minimiser les risques pour l'information. Voir certificate.pdf pour accéder à une version PDF du certificat ISO 27001.

Le suivi des métriques

5. Suivi des métriques

- Mentionner les ressources (humaines, logiciels…) utilisés pour mesurer la disponibilité, la capacité et la performance
- Le paramétrage de mesure des services
- Décrire les processus de production de rapports, le contenu, la fréquence et toutes autres normes pertinentes

Gestion des alertes et incidents

6. La procédure en cas de défaillance

Décrire :

- les points de contact en cas d'urgence chez le fournisseur et le client,
- les moyens de notifications,
- le processus de résolutions, dont les rôles et responsabilités de toutes les parties
- la procédure d'escalade en cas de problème ou d'incident
- la processus de médiation
- les méthodes correctives que le fournisseur appliquera si certains services ne sont pas disponibles (outre des compensations financières)

Gestion des alertes et incidents

Exemple : Contrat de support premium :

Article 4. Conditions d'utilisation du Service

4.1 Procédure de sollicitation Chaque demande ou déclaration d'Incident reçue donne lieu à l'enregistrement par XXcloud d'un ticket (ou « Ticket Incident ») suivant selon le cas, la réception de l'email du Client, la validation du formulaire dans l'Interface de gestion, ou la fin de l'appel téléphonique du Client. Le Client est informé immédiatement par courrier électronique de la création du Ticket Incident et du numéro correspondant. En fonction du niveau de sévérité de l'Incident, tel que défini dans le tableau ci-dessous, XXcloud s'engage à réaliser une première réponse par email et dans l'outil de gestion des tickets dans les délais indiqués sur le Site Internet d'XXcloud. Le Client accède au statut et à l'historique de ses demandes et déclarations d'Incidents sur son Interface de Gestion.

En cas de déclaration d'un Incident, le Client s'engage à communiquer à XXcloud un maximum d'informations concernant le problème rencontré, afin de permettre la bonne réalisation du diagnostic. A l'ouverture d'un Ticket Incident le niveau de sévérité est qualifié par XXcloud lors de sa prise en charge sur la base des éléments fournis par le Client au sein dudit Ticket.

Sanctions en cas de non respect du SLA

7. Les clauses pénales : les pénalités

La clause pénale est définie par l'article 1231-5 du code civil

« *lorsque le contrat stipule que celui qui manquera à l'exécuter paiera une certaine somme à titre de dommages et intérêts, il ne peut être alloué à l'autre partie une somme plus forte ni moindre* ».

Avantages :

- maîtriser la sanction de l'inexécution du service par la fixation à l'avance d'une somme forfaitaire, afin d'éviter une évaluation judiciaire du préjudice causé par cette inexécution
- caractère dissuasif ou incitatif
- résoudre rapidement une inexécution contractuelle

La clause pénale s'applique du seul fait de l'inexécution sans qu'il y ait nécessité de prouver :

- le préjudice du créancier.
- la faute du fournisseur, la pénalité pouvant être appliquée dès constatation de l'inexécution des obligations de l'autre partie.

L'inexécution de l'obligation visée par la clause pénale doit être attribuable au débiteur (force majeure, tiers).

La clause pénale doit être expresse, c'est-à-dire qu'elle doit être prévue par écrit dans le contrat. Il faut dès lors prendre garde à ce que l'obligation sujette à la sanction de la clause pénale soit bien mentionnée dans celle-ci

⇒ décrire ce qui déclenche la clause

- Inexécution totale, partielle
- Inexécution tardive
- Inexécution définitive

Sanctions en cas de non respect du SLA

7. Les clauses pénales : les pénalités

Décrire les conditions de forme du déclenchement de la pénalité (mise en demeure, etc.)

Selon l'article 1231-5 du Code civil son montant doit représenter une somme forfaitaire ni excessive, ni dérisoire. En général, afin de compenser le préjudice. Les fournisseurs accordent :

- un pourcentage mensuels liés aux marges de profit
- une somme prédéfinies et plafonnées.
- réduction du prix
- Crédits
- À l'inverse : bonus en cas d'atteinte continue des objectifs

Comment fixer le montant de la clause pénale ?

La pénalité doit compenser le préjudice subi en cas d'inexécution de l'obligation, et ce, quel que soit le préjudice réellement subi lors de la réalisation de la clause.

Ainsi, il faut établir le prix en fonction du préjudice que causerait l'inexécution de l'obligation.

Le montant ne doit pas représenter un caractère excessif ou dérisoire au risque de se voir réviser par le juge.

Enfin, pour le contrat **d'adhésion**, l'article 1171 du Code civil dispose que toute clause non négociable créant un déséquilibre significatif entre les parties est réputée non écrite.

Sanctions en cas de non respect du SLA

7. Les clauses pénales : les pénalités

Que se passe-t-il si le montant de la clause pénale a été incorrectement fixé ?

=> la révision de la clause pénale disproportionnée par le juge.

Aux termes de l'article 1231-5, le juge peut réviser le montant de la clause pénale s'il considère que celui-ci est excessif ou dérisoire. Le juge peut également réviser ce montant lorsque l'inexécution est partielle, de sorte à faire convenir le montant de la clause pénale au préjudice résultant de cette inexécution partielle. Cela permet de réduire le montant à une somme proportionnelle au préjudice subi.

La disproportion s'apprécie en comparant le montant de la clause avec celui du préjudice subi à la suite de l'inexécution des obligations.

La mise en œuvre des pénalités :

- déduire le coût de l'indisponibilité de son paiement
- dresser une facture

Caractère libératoire : dès lors que le débiteur effectue le paiement de l'indemnité prévue par la clause pénale, le créancier n'est plus en droit de lancer contre lui une action en responsabilité auprès des cours et tribunaux.

Sanctions en cas de non respect du SLA

7. Les clauses pénales : les pénalités

CA Paris, 10/01/2020, 17/02157

=> déséquilibre significatif : revue à la baisse de la pénalité

CA Versailles, 16/01/2020, 18/05075

=> rejet de la requalification en clause pénale : le contrat prévoit paiement jusqu'au terme en cas de résiliation anticipée : rejet de la requalification en clause pénale parce que le caractère forfaitaire fait défaut (lié à la durée)

Sanctions en cas de non respect du SLA

7. Exemples

Le total des pénalités encourues au titre de l'intégralité des retards sur un an est plafonné à 15 % du montant des redevances d'abonnement annuel.

N°	Etat du ticket	Critères	Indemnité si non-atteinte
I01	Prise en compte	Cf Annexe – Engagement de niveau de service.docx	20 €
I02	Correction ou solution de contournement	Priorité 1	40 € par jour supplémentaire
		Priorité 2	20 € par jour supplémentaire
		Priorité 3	10 € par jour supplémentaire
I03	Correction après solution de contournement	Priorité 1	20 € par jour supplémentaire
		Priorité 2	10 € par jour supplémentaire
		Priorité 3	5 € par jour supplémentaire

Sanctions en cas de non respect du SLA

8. Les clauses d’indemnisation

Dommages indirects :

- Lorsque le fournisseur accepte de couvrir les pénalités encourues par le client en cas de défaillance de service.
- Ou s’engage à rembourser son client pour tous les coûts liés à un litige avec des parties tierces résultant d’une panne de service d’une certaine ampleur.

Sanctions en cas de non respect du SLA

9. Autres sanctions

Outre le droit à une compensation en cas de préjudice subi à la suite d'une violation de l'accord de niveau de service par le fournisseur, le client peut **suspendre son obligation et/ou de résilier le contrat.**

Audit et contrôle

- Audit documentaire
- Audit automatique via un outil de suivi commun (dashboard)
- Audit sur site :

Décrire le déroulement de l'audit

- par le fournisseur, par un tiers
- délai de prévenance,
- encadrement, clause de confidentialité,
- objectif et limites,

Prévoir les conséquences des violations des termes du Contrat

- communication des résultats,
- modalités de régularisation (délai de mise en conformité, prix prédéfinis, pénalités, réexamen des besoins réels…).

Audit et contrôle

Exemple : guide contractuel Hébergement

AUDIT DOCUMENTAIRE

Les mesures de protection mises en œuvre par le Prestataire doivent être au moins égales aux normes de sécurité prévues par les bonnes pratiques du secteur numérique, telles que <à compléter : la norme xx (dans sa dernière version) par exemple>. Le Prestataire doit fournir la preuve, lors de la signature du Contrat et des mises à jour annuelles, qu'il maintient des contrôles conformes au cadre de la norme <à compléter> et partager avec le Client le résumé des tests de pénétration indépendants, effectués par des tiers engagés par le Prestataire.

AUDIT OPERATIONNEL

Le Client aura droit, au plus <à compléter> fois au cours d'une période de <mois ou année> consécutifs et à ses frais, de procéder à un audit confidentiel de son propre espace Client et des zones communes du Data Center. Un tel audit se déroulera aux dates et heures convenues entre les Parties. L'audit est réalisé par le Client ou par tout tiers auditeur mandaté par le Client. Le Prestataire pourra refuser l'intervention d'un auditeur tiers considéré comme concurrent direct ou indirect du Prestataire. Le Client doit s'assurer qu'il traite toutes les informations confidentielles du Prestataire auxquelles il aurait accès au cours de l'audit, uniquement aux fins de cet audit, conformément au Contrat. Le Client fera respecter les règles mentionnées ci-avant par l'auditeur tiers qu'il aura diligenté et lui fera signer un accord de confidentialité conforme au Contrat.

Sauf accord contraire, l'audit comprendra deux axes : inspection du Data Center et examen par les auditeurs du Client des registres de fonctionnement des Data Centers préparés par le Prestataire. Ces inspection et examen ont pour unique but de vérifier la conformité du Data Center au Contrat.

Le Client s'engage à ce que (i) ces audits ne portent pas atteinte aux activités des autres clients du Prestataire ; (ii) les auditeurs du Client se conforment aux procédures et mesures de sécurité du Prestataire ; (iii) la conduite de l'audit n'impacte pas l'exécution des services.

Au terme de l'audit et dans les meilleurs délais, le Client s'engage à communiquer le rapport d'audit qui sera discuté, le cas échéant, lors d'une réunion bipartite.

Gestion des changements

Du service fourni

Transparence sur les changements de fonctionnalité, d'interface et les mises à jour logicielles

- Maintenance évolutive : nouvelle version ou évolution automatique du service

Transparence sur les changements de sous-traitant

- Information, accord préalable, délai de mise en œuvre…

NB : Parallèle avec les obligations en matière de traitement des données.

Prévoir un plan pour la révision et l'amélioration périodique et continue des SLA.

Des SLA

Prévoir une procédure pour la révision de l'accord de niveau de service.

En aucun cas, le fournisseur (ou le client) n'est autorisé à le modifier de manière unilatérale.

Questions connexes

1. Politique de sauvegarde, gestion des urgences, récupération après sinistre et continuité des activités

NB : Parallèle : les procédures claires visant à restituer les données à tout moment, y compris le calendrier et le format des données, doivent être convenues et testées.

2. Gestion de la vulnérabilité

Dans quelle mesure les actions correctives sont mises en œuvre : nombre de vulnérabilités corrigées, pourcentage de corrections effectuées dans le délai prescrit, pourcentage de vulnérabilités identifiées?

Exigence du client :

Audit de sécurité

NB : résultats de l'analyse des risques au regard de la protection des données personnelles

Questions connexes

3. Garanties concernant la protection des données en cas d'incidents de sécurité et violations de données à caractère personnel

- Détailler les formes et les canaux de notification convenus (ajout à ce qui est déjà prévu dans les clauses).
- Prévoir des contrôles et audits, y compris scientifiques du client chez le fournisseur
- Le fournisseur doit consigner les opérations concernant les données à caractère personnel et les mettre à la disposition du client.
- Le fournisseur doit coopérer d'une manière efficace et efficiente.

4. Résiliation du service et réversibilité

- Définir le calendrier de la transmission, y compris la restitution des données ou l'exportation vers un nouveau fournisseur de services, la suppression définitive.
- Le fournisseur doit techniquement garantir des mécanismes d'élimination sécurisés, comme la destruction, la démagnétisation ou l'écrasement, et fournir une attestation de destruction (y compris les sauvegardes).
- Définir les vérifications possibles via l'inspection des locaux et des enregistrements.

Check List

- Quels sont les services ?
- Quels sont les services de performance ou de fiabilité inclus ?
- Quels sont les services de performance ou de fiabilité non-inclus ?
- Quel est le niveau de qualité du service ? (différentes offres ?)
- Quel est le coût pour fournir le niveau de service ?
- Comment sera fourni le service de performance ou de fiabilité ?
- Comment est contrôlé, suivi et quantifié la performance, la fiabilité ?
- Quand seront revus les services ?
- Quelles sont les heures d'ouverture du service de performance (heures régulières et l'assistance à l'extérieur des heures ouvrables) ?
- Quand les maintenances planifiées auront-elles lieu ?

Check list

- ❖ Type de service concerné par le SLA
- ❖ Le niveau de performance ou de fiabilité souhaité :
- Un service fiable ou performant sera celui qui subira le moins de perturbations dans un laps de temps déterminé et qui sera disponible à (presque) tout moment.
- Un service avec une bonne réactivité effectuera l'action souhaitée rapidement après la demande du client.
- ❖ Les indicateurs retenus
- ❖ Les processus de surveillance : préciser comment les niveaux de performance ou de fiabilité sont supervisés et surveillés. Ce processus implique la collecte de différents types de statistiques, la fréquence à laquelle ces statistiques seront collectées et la manière dont les clients y accéderont.
- ❖ Les étapes de signalement des problèmes : préciser les coordonnées auxquelles signaler le problème et l'ordre dans lequel les détails du problème doivent être signalés ou préciser comment le fournisseur informe le client.
- ❖ Délai de réponse et de résolution du problème
- ❖ Conséquences pour le fournisseur qui ne respecte pas son engagement

Merci pour votre attention

Olivia Flipo
Docteur en Droit
Avocat à la Cour

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

numeum

Engager
le numérique

numeum.fr