Planisware

Version : 12 février 2026

ANNEXE I – POLITIQUE DE SUPPORT SAAS

La présente Politique de Support SaaS Planisware (« **Politique de Support** ») décrit l'offre de support technique de Planisware pour les Services SaaS. Cette Politique de Support constitue une annexe aux Conditions Générales de Planisware (« **CG** ») et fait partie du Contrat tel qu'il y est défini. Elle est actualisée à chaque Mise à Niveau majeure du Service, avec des conditions qui ne sont pas moins favorables pour le Client.
Les termes en majuscules sont définis dans la présente Politique de Support ou dans les CG.

1. ACCÈS AU SYSTÈME

Planisware maintient et fournit toutes les infrastructures et composants réseaux nécessaires à la fourniture du Service SaaS au Client, y compris un espace de stockage sur disque afin de permettre une installation et une gestion efficaces du Service SaaS.

Les Utilisateurs doivent se connecter au Service avec un navigateur approuvé, comme indiqué dans la matrice de compatibilité des navigateurs Planisware, qui peut être consultée dans la Documentation sur https://myportal.planisware.com mise à jour ponctuellement. Le Service SaaS est accessible via le protocole Hypertext Transfer Protocol Secure (HTTPS). Le Service SaaS prend en charge les protocoles suivants pour chaque type d'échange de données :

Pour l'échange de fichiers : SFTP/HTTPS

Pour les services web (via HTTPS) : ODATA / SOAP / REST

Planisware, en consultation avec le Client, attribue au Service un nom de domaine et une URL dédiés (par exemple https ://customer_choice.planisware.live). Planisware ne peut être tenue responsable de l'impossibilité d'obtenir une URL particulière du fait de circonstances hors de son contrôle raisonnable (par exemple, si cette URL a déjà été allouée à une autre ressource ou projet).

Planisware fournit une bande passante d'accès suffisante pour que le Client et ses Utilisateurs puissent accéder au Service SaaS à tout moment, sans retards ou interruptions déraisonnables lors du téléchargement, la visualisation ou du chargement des données vers ou depuis le Service SaaS. Planisware n'est pas responsable des problèmes d'accès ou de performance causés par les appareils, le service de connexion internet, le matériel informatique, les logiciels ou les mesures de sécurité des Clients ou des Utilisateurs, susceptibles de restreindre l'accès au Service SaaS.

2. HÉBERGEMENT ET SAUVEGARDES DES DONNÉES CLIENT

Le Service SaaS offre un espace de stockage limité pour les Données Client tel que spécifié dans l'Offre. Le Client peut demander un stockage supplémentaire pour les fichiers et documents soumis à un SOW distinct. Planisware déploie des efforts raisonnables pour informer les Clients lorsque leur utilisation du stockage atteint environ 90 % de la limite applicable.

Planisware effectue des sauvegardes quotidiennes des Données Client. Outre toute restauration de sauvegarde à des fins de reprise après incident, Planisware restaure les sauvegardes dans la base de Données Client, comme indiqué dans la présente Politique de Support.

3. MISES A NIVEAU

Planisware procède périodiquement à des Mises à Niveau. Une « **Mise à Niveau** » signifie une nouvelle version du Service SaaS, soit majeure, soit mineure. Une Mise à Niveau est identifiée par un numéro de version augmenté (y compris les augmentations post-décimales pour les versions mineures).

Planisware fournit au moins une Mise à Niveau par année civile, sans coût supplémentaire pour le Client, à condition que (i) les configurations soient migrées en l'état vers la nouvelle version et (ii) que les nouveaux modules ou fonctionnalités inclus dans une Mise à Niveau soient standards et non configurés, sauf si une telle configuration est convenue mutuellement dans le cadre d'un SOW donnant lieu à des frais supplémentaires. Cette Mise à Niveau annuelle est obligatoire, et le Client ne peut pas demander à continuer d'utiliser une version obsolète du Service SaaS, sous réserve des exceptions ci-dessous.

Les Mises à Niveau peuvent entraîner des modifications de l'apparence et/ou des fonctionnalités du Service SaaS cependant, elles ne diminueront ni n'affecteront matériellement ses fonctions.

Planisware donne au Client un préavis écrit d'au moins vingt (20) jours ouvrables avant toute Mise à Niveau. Lorsqu'il est disponible, Planisware peut fournir au Client l'accès à un environnement amélioré pour tester la Mise à Niveau avant la mise en production, pour une période maximale de vingt (20) jours ouvrables. Durant cette période de test, le Client informe Planisware de toute diminution ou altération significative des fonctions du Service SaaS, et Planisware corrige ces problèmes ainsi signalés. Le Client ne peut refuser une Mise à Niveau que si celle-ci est à l'origine d'un incident de Priorité 1 ou 2 sans solution de contournement, tel que défini dans les règles de gestion des incidents (article 5) ci-dessous, une fois que les incidents de Priorité 1 ou Priorité 2 résolus conformément aux règles de gestion des incidents, le Client doit accepter la Mise à Niveau. Dans le cas où une Mise à Niveau est à l'origine d'un incident de Priorité 3 ou 4, Planisware répond conformément aux règles de gestion des incidents, sauf accord entre les Parties à traiter ces incidents dans le cadre d'un SOW distinct.

Les étapes-clés du cycle de vie des versions sont définies dans la feuille de route produit communiquée au Client (disponibilité générale, fin de vie et fin de support avec les obligations correspondantes de gestion des incidents).

4. RÉSILIATION OU EXPIRATION DE L'ACCORD

À la résiliation ou à l'expiration du Contrat, Planisware doit mettre à disposition du Client sur demande écrite, une sauvegarde de la base de Données Client (pour tout autre format, les Parties devront signer un SOW). Planisware conserve les Données Client pendant un maximum de trente (30) jours après la date de résiliation ou d'expiration et la demande écrite doit être faite dans ce délai. Planisware n'a aucune obligation de conserver les Données Client et peut les supprimer après cette période de trente (30) jours. À la fin du Contrat, la seule obligation de Planisware concernant les Données Client consiste à remettre ladite sauvegarde.

5. ACCORD DE NIVEAUX DE SERVICE (« SLA ») ET GESTION DES INCIDENTS

5.1 Support technique

Planisware fournit un support technique sur le Service SaaS conformément à l'article 5.2 (SLA) et à l'article 5.4 (Règles de Gestion des Incidents). Le support est limité comme suit :

1. Le Support technique n'est accessible qu'à certains Utilisateurs identifiés par le Client (généralement les utilisateurs ayant un profil administratif) et non pas à tous.
2. Le Support n'inclut ni le conseil ni la formation concernant l'utilisation fonctionnelle ou la configuration du Service SaaS.
3. Le SLA ne s'applique qu'à l'utilisation du Service SaaS dans l'environnement de production du Client et uniquement après la date de mise en ligne. Lorsqu'un environnement hors production est disponible (par exemple, environnement de test ou d'entraînement), les SLA ne s'appliquent pas.
4. Le plan de réponse aux incidents prévu par le SLA s'applique uniquement à l'environnement de production du Client. Les incidents dans d'autres environnements hors production (par exemple, environnement de test ou de formation) ne sont pas couverts par les exigences de gestion des incidents définies ci-dessous.
5. Le support est assuré pendant les Heures Ouvrées, selon l'entité signataire de Planisware, comme indiqué dans l'Offre :
   - Planisware S.A (également applicable à Planisware UK et Planisware Belgium) : de 9h à 18h (CET) pendant les jours ouvrables, à l'exception des jours fériés nationaux locaux ;
   - Planisware Deutschland GmbH : de 9h à 18h (CET) pendant les jours ouvrables, à l'exception des jours fériés nationaux allemands et des jours fériés en Bavière ;
   - Planisware USA Inc. : de 9h (EST) à 18h (PST) pendant les jours ouvrables, à l'exception des jours fériés américains ;
   - Planisware Singapore PTE. LTD. : de 9h à 18h (SGT) pendant les jours ouvrables, à l'exception des jours fériés nationaux de Singapour ;
   - Planisware Japon KK : de 9h à 18h (JST) pendant les jours ouvrables, à l'exception des jours fériés nationaux japonais.
6. Les règles de SLA et de Gestion des Incidents ne s'appliquent pas lorsque les problèmes de performance/disponibilité sont causés par les éléments suivants :
   - Congestion globale, ralentissement ou indisponibilité d'internet.
   - Indisponibilité des Services SaaS Internet génériques (par exemple les serveurs DNS) en raison d'attaques de virus ou de pirates.
   - Événement de force majeure tel que décrit dans les CG.
   - Actions ou inactions du Client ou de tiers, indépendantes du contrôle de Planisware.
   - Risques liés à l'équipement du Client ou à du matériel informatique tiers, aux logiciels ou infrastructures réseaux qui ne relèvent pas du contrôle exclusif de Planisware.
   - Configuration(s) créée(s) ou modifiée(s) par le Client ou par un tiers au nom du Client. Planisware traite ces incidents uniquement si le Client le demande et sous réserve d'un SOW modifié ou séparé.

5.2 SLA

Mesure / Nom	Définition	Exigence
Disponibilité	Disponibilité Totale : nombre total de minutes dans un mois moins le Temps d'Indisponibilité Autorisée pour ce mois. Disponibilité Réelle : Le pourcentage de disponibilité totale dans un mois calendaire où le Service SaaS est disponible pour les Utilisateurs dans l'environnement de production du Client accessible via des protocoles internet.	Disponibilité Réelle de 99,5 % par mois (hors Temps d'Arrêt Autorisé)
Indisponibilité Autorisée	Mesure du temps total dans un mois calendaire pendant lequel le Service SaaS n'est pas disponible en raison de : ➢ Maintenance régulière (par exemple, coupure programmée sans notification requise) ➢ Maintenance programmée (par exemple, Mise à Niveau ou autre Temps d'Arrêt ad hoc planifiés avec un préavis suffisant au Client) ➢ Maintenance d'urgence, y compris la réponse aux menaces immédiates de sécurité, ainsi que les mesures préventives ou correctives requises pour respecter les obligations contractuelles de sécurité et de continuité des activités ainsi que la législation applicable. ➢ Circonstances échappant au contrôle raisonnable de Planisware, y compris, mais sans s'y limiter : - Défaillances informatiques (pannes, encombrement ralentissement), télécommunications, fournisseurs d'accès Internet ou installations d'hébergement - Actes gouvernementaux, inondations, incendies, tremblements de terre, actes de terrorisme, grèves ou autres problèmes (autres que ceux impliquant des employés de Planisware) - Retards liés aux matériels, logiciels ou systèmes électriques qui ne sont pas sous la possession ni sous le contrôle de Planisware, et attaques par déni de service - Autres activités dirigées par le Client, - Modifications résultant d'actions gouvernementales, politiques ou autres réglementations ou ordonnances judiciaires, et/ou - Absence de réponse du Client lorsqu'un incident nécessite sa participation pour la résolution - Problèmes de connectivité affectant les Utilisateurs	➢ Maintenance régulière : le dimanche matin (durée maximale de quatre heures chaque week-end, sauf accord contraire entre les parties). ➢ Maintenance programmée : Le Client est informé au moins 5 jours ouvrables à l'avance, Planisware s'efforce à programmer l'interruption afin de minimiser l'impact pour le Client. ➢ Maintenance d'urgence : peut être effectuée sans préavis en cas de menace crédible à la sécurité. Le Client est informé pendant l'intervention ou dès que possible par la suite, selon la gravité de la menace. Cela inclut le temps nécessaire au redémarrage de l'application après la résolution d'un problème d'urgence.
Garantie maximale de perte de données (RPO) en cas de catastrophe	Quantité maximale de perte de données à compter de la survenance d'une catastrophe	Pas plus de 24 heures de perte de données
Retour aux opérations (RTO)	Délai pour rétablir le service après une interruption imprévue, à l'exception de la catastrophe.	Pas plus de 12 heures (standard)
Le Client a demandé une restauration de sauvegarde	Mesure le temps entre la demande de récupération et la récupération	La restauration d'une sauvegarde complète de l'ensemble des Données Client est réalisée dans les 4 heures ouvrées à compter de la demande du Client. Le temps de restauration d'une partie de Données Client dépend de la complexité de la demande. Il peut nécessiter une Indisponibilité Autorisée supplémentaire allant jusqu'à 4 heures et ou, être soumis à une Offre distincte.
Environnement hors production Renouvellement des Données Client	Restauration de la base de Données Client dans un environnement hors production (par exemple, test, formation).	3 jours ouvrables après la demande écrite et limité à 6 demandes par an dans un environnement hors production.

Règles de calcul des délais SLA

Le délai de réponse SLA pour un incident commence à courir dès que celui-ci est enregistré pour la première fois dans le système de gestion de service, que l'enregistrement soit réalisé par le Client ou par le prestataire de services. Il peut être mis en pause en cas de dépendance Client, de retards imputables à un tiers ou d'une période de Maintenance Programmée.

Pause / suspension du délai :

Le compteur du SLA peut être mis en pause dans les cas suivants :

1. En attente d'une action du Client – par exemple, lorsque des informations supplémentaires, une validation (autorisation de passage en environnement test, production...), confirmation (sur l'environnement de test ou de production) ou un accès système sont requis de la part du Client et empêchent le fournisseur de poursuivre.
2. Dépendance tierce – par exemple, lorsque la résolution dépend d'un autre fournisseur ou d'un système externe échappant au contrôle du fournisseur.
3. Maintenance programmée ou Indisponibilité Autorisée – le temps passé pendant ces créneaux sont exclus du calcul du SLA.

5.3 CONFIGURATIONS RÉALISÉES PAR LE CLIENT OU UN TIERS DÉSIGNÉ PAR LE CLIENT

Le SLA ne s'applique pas aux incidents, indisponibilités, problèmes de performance ou régressions post-Mise à Niveau qui, après enquête menée par le Client ou un tiers désigné par ce dernier, ne trouvent pas leur origine dans la performance directe, les responsabilités ou omissions imputables à Planisware. Néanmoins, Planisware peut être tenue d'enquêter et/ou tenter de corriger de telles configurations, sous réserve de la conclusion un SOW dédié. Conformément à l'article 9.1 des CG, la responsabilité de Planisware ne peut être engagée pour les dommages causés au Client et résultant d'un acte ou d'une omission du Client ou d'un tiers (y compris, mais sans s'y limiter, les dommages résultant de la création ou modification de configurations par le Client, le fournisseur ou les sous-traitants).

5.4 RÈGLES DE GESTION DES INCIDENTS

L'équipe de Support de Planisware se rend disponible et répond aux incidents comme indiqué dans le tableau ci-dessous.

Niveau de support	Priorité 1 (P1)	Priorité 2 (P2)	Priorité 3 (P3)	Priorité 4 (P4)
Disponibilité du Support	24h/24, 7 jours par semaine	Aux Heures Ouvrées	Aux Heures Ouvrées	Aux Heures Ouvrées
Première Réponse	Dans l'heure suivant le signalement de l'incident	Dans les 2 heures suivant le signalement de l'incident, pendant les heures ouvrées	Dans les 8 heures suivant le signalement de l'incident pendant les heures ouvrées (accusé de réception uniquement)	Dans les 8 heures suivant le signalement de l'incident pendant les heures ouvrées (accusé de réception uniquement)
Réponses de suivi	Toutes les 2 heures à partir du signalement de l'incident jusqu'à la résolution de l'incident	Tous les jours ouvrés	N/A	N/A
Résolution d'un incident (y compris via une solution temporaire de contournement)	Dans les 8 heures suivant le signalement de l'incident	En moyenne 2 jours ouvrés et maximum 5 jours ouvrés	Dans une version ultérieure	Dans une version ultérieure

*Horaires/jours ouvrés tels que définis à l'article 5.1

Les priorités d'incident sont définies comme suit :

Portée de l'incident	Service SaaS indisponible	Service SaaS disponible et utilisable mais : (1) la performance est dégradée, ce qui empêche d'achever le processus souhaité dans un délai raisonnable. (2) Fonctionnalités majeures* indisponibles ou non fonctionnelles et aucune solution de contournement n'est disponible	Service SaaS disponible et utilisable mais : (1) la performance est légèrement dégradée. (2) Fonctionnalités majeures* indisponibles ou non fonctionnelles, mais une solution de contournement est disponible (3) Fonctionnalités mineures indisponibles ou non fonctionnelles et aucune solution de contournement n'est disponible	Fonctionnalités mineures indisponibles ou non fonctionnelles. Problème d'ordre esthétique ou problème qui n'ayant aucune incidence sur l'utilisabilité du Service SaaS ou la capacité à mener à bien un processus
À l'échelle du système	P1	P2	P3	P4
Impact sur plus de 25 % des Utilisateurs	P2	P2	P3	P4
Utilisateurs multiples sans schéma établi	P3	P3	P3	P4
Utilisateur unique	P3	P4	P4	P4

***« Fonctionnalités majeures »** désigne les fonctions critiques du Service SaaS telles que définies entre les Parties avant la date de lancement du Service dans le SOW. Après la mise en œuvre d'un SOW pour les Services Professionnels prévoyant le développement et la mise en œuvre de toute configuration du Service SaaS, les Parties pourront convenir de l'ajout de nouvelles Fonctionnalités Majeures correspondantes.