Planisware
Get innovation to market

ACCORD DE TRAITEMENT DES DONNÉES PERSONNELLES

Cet Accord de traitement des Données Personnelles (« **DPA** ») fait partie des CG signées entre Planisware et le Client (ci-après le « **Contrat** »). L'objectif du DPA est de refléter l'accord sur le traitement des Données Personnelles, conformément aux exigences des lois et réglementations applicables en la matière. Planisware et le Client seront ci-après désignés séparément par « **Partie** » ou conjointement par « **Parties** ».

1. DÉFINITIONS

Sauf indication contraire dans le DPA, les termes en majuscules ont la signification indiquée dans le Contrat.

« **Responsable de Traitement** »	désigne l'entité qui détermine les finalités et les moyens du traitement des Données Personnelles. Pour les besoins du DPA, le Client est le Responsable de Traitement.
«**Sous-Traitant**»	désigne l'entité qui traite les Données Personnelles pour le compte du Responsable de Traitement. Pour les besoins du DPA, Planisware est le Sous-Traitant.
« **Droit Applicable** »	désigne toutes les lois et règlements obligatoires applicables au traitement des données à caractère personnel dans le cadre des CG Planisware, y compris mais sans s'y limiter au Règlement général sur la protection des données de l'UE 2016/679 (« **RGPD »**), les lois et règlements de l'Union européenne, de l'Espace Economique Européen et de leurs États membres.
«**Personne Concernée**»	désigne une personne soumise au Droit Applicable et à laquelle se rapportent des Données Personnelles.
«**Données Personnelles**»	désigne les données relatives à une personne physique spécifique transmises à et collectées par Planisware dans le cadre des Services fournis par Planisware au Client, à partir desquelles cette personne est identifiée ou identifiable, tel que défini par le Droit Applicable.
«**Traitement**»	désigne toute opération ou ensemble d'opérations effectués sur des données personnelles, de manière automatisée ou non, telle que la collecte, l'organisation, la conservation, l'extraction, la consultation, l'utilisation, la communication par transmission ou diffusion, la limitation, l'effacement ou la suppression.
«**Documentation de sécurité**»	désigne les informations fournies au Client par Planisware concernant ses mesures techniques et organisationnelles de sécurité des données telles que définies à l'Annexe 2 et qui peuvent être ponctuellement mises à jour par Planisware, conformément à ce DPA.

«**Incident de sécurité**»	désigne une divulgation ou un accès non autorisé à des données personnelles ou une destruction, perte ou altération accidentelle ou illégale de données personnelles.
« **Clauses Contractuelles Type**» ou «**Clauses**»	désigne les Clauses Contractuelles Type pour le transfert de données personnelles vers des pays tiers conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil mis en œuvre par la Décision d'exécution (UE) de la Commission 2021/914 du 4 juin 2021.
«**Sous-Traitant Ultérieur**»	signifie que tout tiers, y compris les Affiliés de Planisware, est engagé par Planisware pour le Traitement des Données Personnelles.

2. TRAITEMENT DES DONNÉES PERSONNELLES

2.1. **Traitement des Données Personnelles par le Client**. Dans le cadre de son utilisation des Services, le Client s'engage à respecter le Droit Applicable. Ainsi, les instructions données par le Client à Planisware concernant le Traitement des Données Personnelles doivent être conformes au Droit Applicable. Lorsque le Client accorde l'accès au Service à des Utilisateurs situés dans des juridictions dont la législation impose des exigences de localisation des données (« **Pays de Localisation des Données** »), ou lorsqu'il télécharge sur le Service les Données Personnelles de toute personne située dans un Pays de Localisation des Données : (i) le Client reconnaît que l'ensemble des Données Personnelles en provenance des Pays de Localisation des Données seront hébergées et stockées dans des datacenters situés dans l'EEE, et pourront être traitées dans les pays listés à l'Annexe 1 ; et (ii) le Client demeure seul responsable du respect de toute exigence de localisation des données prévues par les lois applicables des Pays de Localisation des Données.

2.2. **Traitement des Données Personnelles par Planisware**. Planisware traite et utilise les Données Personnelles pour le compte du Client, sur instructions de ce dernier (y compris par e-mail), et exclusivement dans la mesure requise par le Droit Applicable. Le Client reconnaît qu'en utilisant les Services, il fournit à Planisware les instructions nécessaires au traitement et à l'utilisation des Données Personnelles afin de bénéficier des Services conformément à ce DPA et comme décrit plus en détail à l'Annexe 1. En cas de mise à jour importante des modalités de traitement, Planisware informe immédiatement le Client. Planisware informe immédiatement le Responsable de Traitement si, à son avis, une instruction est contraire au Droit Applicable.

2.3. **Analyse d'impact sur la protection**. A la demande du Client, Planisware apporte son aide raisonnable, ainsi que l'assistance nécessaire pour que le Client satisfasse à son obligation de réalisation d'analyse d'impact relative à la protection des données liées à l'utilisation des Services par le Client, découlant du RGPD, dans la mesure où le Client n'a pas accès aux informations pertinentes et si ces informations sont disponibles auprès de Planisware. Planisware doit fournir une assistance raisonnable au Client en cas de consultation préalable ou de réponse requise à toute demande d'autorité compétente en matière de protection des données.

3. DROITS DES PERSONNES CONCERNÉES

3.1. **Suppression des Données Personnelles**. À la résiliation du Contrat, pour quelque raison que ce soit, Planisware supprime toutes les Données Personnelles traitées conformément au présent DPA, ou anonymise les données des Utilisateurs afin de retirer dès que possible toute Donnée Personnelle. En outre, Planisware demande la suppression/anonymisation correspondante à ses Sous-Traitants, à condition qu'ils puissent conserver les données nécessaires pour démontrer leurs conformités aux exigences légales et réglementaires applicables ainsi qu'à la tenue de registres.

3.2. **Droits des Personnes Concernées**. Le Client est seul responsable de l'information des Personnes Concernées sur le Traitement de leurs Données Personnelles et de la gestion de leurs demandes

d'exercice de droits conformément au Droit Applicable. Planisware doit, dans la mesure où le droit applicable le permet, informer le Client en temps utile si une demande d'une Personne Concernée pour l'accès, la correction, la modification ou la suppression de ses Données Personnelles est reçue. Planisware ne doit répondre à aucune demande de ce type sans en avoir reçu l'instruction par écrit du Client (y compris par e-mail), sauf pour confirmer à la Personne Concernée que la demande concerne le Client. Le Client est responsable de tous les coûts raisonnables résultant de la fourniture d'une telle assistance par Planisware.

3.3. **Plaintes ou avis liés à des Données Personnelles**. Dans le cas où Planisware recevrait une plainte, un avis ou une communication officielle concernant son Traitement des Données Personnelles ou concernant le respect par l'une ou l'autre des Parties du Droit Applicable, dans la mesure où le droit applicable le permet, Planisware doit rapidement informer le Client et lui fournir une coopération et une assistance commercialement raisonnables concernant toute plainte, avis, ou communication de ce type. Le Client est responsable de tous les coûts raisonnables résultant de la fourniture de cette assistance par Planisware.

4. PERSONNEL DE PLANISWARE

4.1. **Confidentialité**. Planisware veille à ce que son personnel soit informé de la nature confidentielle des données impliquées dans le Traitement des Données Personnelles, et ait reçu une formation appropriée sur leurs obligations et ait signé des engagements de confidentialité. Planisware doit veiller à ce que ces obligations de confidentialité survivent à la fin de l'engagement du personnel.

4.2. **Limitation d'accès**. Planisware s'assure que l'accès aux Données Personnelles soit limité au personnel requis pour l'exécution du Contrat.

4.3. **Responsable de la protection des données**. Planisware désigne un responsable de la protection des données, dans la mesure où cette nomination est requise par le Droit Applicable. Toute personne ainsi désignée peut être contactée à dpo@planisware.com. Le Client communique dès que possible après la signature du Contrat les coordonnées de son Délégué à la Protection des Données (DPO).

5. SOUS-TRAITANTS ULTÉRIEURS

5.1. **Nomination des Sous-Traitants Ultérieurs**. Le Client reconnaît et accepte expressément que (i) Planisware a le droit de recourir à ses Affiliés en tant que Sous-Traitants Ultérieurs, et (ii) Planisware ou tout autre Affilié peut respectivement engager un tiers pour traiter les Données Personnelles pour le compte de Planisware, dans le cadre de la fourniture des Services. Planisware ne divulguera des Données Personnelles qu'aux Sous-Traitants Ultérieurs, qui ont conclu avec Planisware des accords écrits imposant des obligations au moins équivalentes à celles de ce DPA. Planisware veille à ce que l'accès aux Données Personnelles soit limité aux Sous-Traitants Ultérieurs qui ont besoin de cet accès dans le cadre de la fourniture des Services au Client. Sur demande écrite du Client, et sous réserve que cette demande ne soit pas formulée plus d'une fois par année civile, Planisware lui communique la liste de ses sous-traitants ultérieurs traitant des Données Personnelles, ainsi que les pays situés hors de l'Espace économique européen dans lesquels ces Données Personnelles sont ou peuvent être traitées. La liste des Sous-Traitants Ultérieurs à la date de signature du DPA figure à l'Annexe 1.

5.2. **Droit d'opposition pour les nouveaux Sous-Traitants Ultérieurs**. Planisware informe le Client par écrit (y compris par e-mail) avant de nommer un nouveau Sous-Traitant Ultérieur. S'il est légalement interdit au Client de consentir à l'utilisation de ce nouveau Sous-Traitant Ultérieur, alors le Client informe Planisware par écrit de cette interdiction dans les dix (10) jours ouvrables suivant la réception de la notification. Planisware déploiera des efforts raisonnables pour (i) mettre à disposition du Client un changement dans les Services concernés, (ii) recommander un changement commercialement raisonnable de la configuration ou de l'utilisation des Services concernés par le Client, afin d'éviter le traitement des Données Personnelles par ledit nouveau Sous-Traitant Ultérieur, ou (iii) collaborer avec le Sous-Traitant Ultérieur afin de s'assurer que tout traitement est effectué de manière raisonnablement satisfaisante pour le Client. Si les

Parties ne parviennent pas à trouver une solution adaptée dans un délai qui ne dépasserait pas soixante (60) jours, le Client peut résilier la partie du Contrat, concernant uniquement les Services qui ne peuvent être fournis par Planisware sans l'utilisation du nouveau Sous-Traitant Ultérieur contesté, en fournissant une notification écrite à Planisware.

5.3. **Responsabilité**. Planisware demeure responsable, dans les limites prévues par les CG de Planisware, des actes et omissions de ses sous-traitants ultérieurs comme si elle exécutait elle-même les Services concernés conformément au présent DPA.

6. SÉCURITÉ; DROITS D'AUDIT

6.1. **Contrôles de la protection des Données Personnelles**. Planisware met en place des mesures techniques et organisationnelles appropriées, telles que décrites dans la Documentation de sécurité, contre les Incidents de Sécurité.

6.2. **Audit**. Planisware répond dans un délai raisonnable à toute question écrite spécifique du Client concernant les mesures techniques et organisationnelles de sécurité des données. Planisware permet au Client d'effectuer un audit sur-site pour vérifier la conformité aux mesures techniques et organisationnelles définies dans la Documentation de sécurité, dans les circonstances suivantes : (i) Suite à la notification par Planisware d'un Incident de sécurité, (ii) le Client croit raisonnablement que Planisware ne respecte pas ses engagements de sécurité en vertu du DPA (et dans ce cas, les droits d'audit du Client ne peuvent pas être exercés pour plus d'une fois par année civile), ou (iii) un tel audit est exigé en vertu du Droit Applicable ou sur instruction d'une autorité compétente en matière de protection des données. Tout audit de ce type doit être effectué conformément à la procédure énoncée à l'article 6.3.

6.3. **Procédure d'audit**. Le Client notifie toute demande d'audit, par écrit avec un préavis d'au moins trois (3) semaines. La portée de l'audit est limitée aux politiques, procédures et contrôles de Planisware relatifs à la protection des Données Personnelles tels que décrits dans la Documentation de sécurité. L'audit se réalisera par échange de documents. Sur réception d'une demande écrite d'audit, et sous réserve de l'accord du Client, Planisware peut satisfaire une telle demande d'audit en fournissant au Client une copie confidentielle du rapport établi par un auditeur indépendant mandaté par Planisware, permettant au Client de vérifier la conformité de Planisware aux mesures techniques et organisationnelles prévues dans la Documentation de sécurité. L'audit est réalisé aux frais exclusifs du Client, par un prestataire tiers choisi d'un commun accord entre les Parties, désigné et rémunéré par le Client et soumis à un accord de confidentialité prévoyant l'obligation de préserver la confidentialité de tous les résultats d'audit, ainsi que les informations confidentielles de Planisware. Avant le début de l'audit, les Parties conviendront mutuellement du calendrier, de la durée de l'audit, ainsi que de sa méthodologie. Il expressément précisé qu'aucune Donnée Personnelle autre que celles traitées au nom du Client ne sera partagée ou divulguée par Planisware dans le cadre d'un audit. Le Client fournit gratuitement à Planisware une copie complète de toutes les conclusions de l'audit. Dans l'hypothèse où après examen de la documentation fournie par Planisware en réponse à une demande d'audit, le Client estime que Planisware n'est pas en conformité avec sa Documentation de sécurité, le Client peut demander un audit sur site, avec un préavis écrit d'au moins trois (3) semaines. Planisware communiquera les tarifs de Services Professionnels alors en vigueur, ainsi que l'estimation du temps nécessaire pour répondre et coopérer avec les auditeurs. Ces coûts sont intégralement supportés par le Client. Planisware coopèrera de bonne foi à l'audit, notamment en mettant à disposition des auditeurs les informations et éléments de sécurité raisonnablement nécessaires à la réalisation de l'audit.

6.4. **Avis de non-conformité**. A l'issue d'un audit, ou après avoir reçu un rapport d'audit de Planisware, le Client doit informer Planisware de la manière dont les obligations de sécurité, de

confidentialité ou de protection des données prévues par ce DPA ou le Droit Applicable ne sont pas respectées. Toute information de ce type sera considérée comme une Information Confidentielle de Planisware. À la suite d'une telle notification, Planisware déploiera tous les efforts commercialement raisonnables afin de mettre en œuvre les modifications nécessaires pour assurer le respect de ces obligations.

7. GESTION ET NOTIFICATION DES INCIDENTS DE SÉCURITÉ

7.1. Planisware maintient des politiques et procédures de gestion des Incidents de sécurité dont des procédures détaillées d'escalade d'Incidents de sécurité telles que décrites dans la Documentation de sécurité. Si Planisware a déterminé qu'un Incident de sécurité s'est produit, elle en informe le Client en temps utile et lui fournit des informations pertinentes sur l'Incident de sécurité, y compris, dans la mesure du possible, le type de Données Client concernées, le volume de Données Client divulgué, les circonstances de l'incident, les mesures d'atténuation, ainsi que les mesures correctives et préventives prises. Le Client est responsable de la notification de ces Incidents de sécurité à l'autorité compétente en matière de protection des données et aux Personnes Concernées lorsque le Droit Applicable l'exige.

8. CONDITIONS SUPPLÉMENTAIRES POUR LE TRANSFERT DE DONNÉES PERSONNELLES DEPUIS L'EEE

8.1. **Clauses Contractuelles Type**. Tout Traitement des Données Personnelles dans des pays qui ne garantissent pas un niveau de protection adéquat tel que déterminé par la décision de la Commission européenne du 4 juin 2021 se fait sur la base des Clauses Contractuelles Type. Ce DPA et les CG de Planisware sont les instructions complètes et finales du Client (« **Exportateur de Données** ») à Planisware (« **Importateur de Données** ») pour le Traitement des Données Personnelles. En cas de contradiction entre les dispositions des Clauses Contractuelles Type et ce DPA ou d'autres accords entre les Parties, les Clauses Contractuelles Type prévaudront. Les termes du DPA ne doivent en aucun cas modifier les Clauses. Dans le cas où elles sont modifiées, remplacées ou abrogées par la Commission européenne ou autrement en vertu du Droit Applicable, les Parties coopéreront de bonne foi afin de signer toute version mise à jour des Clauses Contractuelles Type, ou pour négocier de bonne foi une solution permettant d'effectuer un transfert de Données Personnelles conforme au Droit Applicable.

8.2. **Mesures supplémentaires Schrems II.** En cas de demande de divulgation ou d'accès direct aux Données Personnelles provenant d'une autorité de police ou d'un organisme de sécurité d'État d'un pays n'appartenant à l'EEE) présentant un caractère massif, disproportionné ou indiscriminé, (« **Divulgation Gouvernementale** » Planisware en informe le Client en temps voulu (dans la mesure permise par le droit applicable). Les Parties discuteront de bonne foi sur les mesures supplémentaires à mettre en œuvre et sur l'opportunité de notifier l'autorité de surveillance compétente et/ou de suspendre tout transfert ultérieur de Données Personnelles. Dans l'hypothèse où Planisware supporterait des coûts matériels dans l'exercice d'un recours contre une Divulgation Gouvernementale, y compris des frais juridiques raisonnables, ces coûts seront pris en charge et remboursés par le Client sur présentation de justificatifs.

9. EFFET JURIDIQUE ; TERMINAISON

9.1. Ce DPA prend effet entre le Client et Planisware à la date de la dernière signature et prend fin à l'issue du Contrat, sans aucune action requise par l'une ou l'autre des Parties.

10. CONFLIT

10.1. En cas de contradiction ou d'incohérence entre le DPA et les CG de Planisware, ce DPA prévaudra.

Pièces jointes :

- **Annexe 1** – Description du traitement

- **Annexe 2** – Description des mesures de sécurité
- Le cas échéant, Clauses Contractuelles Type
- **Annexe 3** – Clauses optionnelles : Spécificités régionales

ANNEXE 1 – DESCRIPTION DU TRAITEMENT

Cette annexe fait partie intégrante du DPA (et/ou des Clauses Contractuelles Type, le cas échéant).

RESPONSABLE DE TRAITEMENT

Désigne le Client, aux fins de l'utilisation de la solution de Planisware.

RESPONSABLE INDÉPENDANT

Veuillez noter que Planisware traite certaines Données Personnelles des Clients en tant que Responsable de Traitement Indépendant, dans les situations suivantes :
(a) gestion des comptes, de la facturation et de la relation client ainsi que la correspondance client associée ; (b) la rémunération (par exemple, le calcul des commissions des employés et des incitations aux associés) ; (c) respecter les obligations légales (par exemple les exigences fiscales) (d) détecter, prévenir et protéger les abus, scanner des virus, (e) créer des données statistiques agrégées pour le reporting interne. Planisware effectue ce traitement conformément au Droit Applicable ainsi qu'à sa Politique de confidentialité [https://planisware.com/privacy-policy].

SOUS-TRAITANT

Planisware propose une solution de gestion de projet, permettant la priorisation des projets, l'équilibrage de portefeuille et la planification des capacités, et a signé les GTC avec le Client.

SOUS-TRAITANT ULTÉRIEURS

Conformément à l'article 5.1, Planisware peut conserver ses Affiliés en tant que Sous-Traitants, et chacun de ces Affiliés peut respectivement engager des tiers pour traiter les Données Personnelles en lien avec la fourniture de Services. Les Sous-Traitants Ultérieurs sont les suivants (à l'exception de l'entité signataire Planisware):

NOM	EMPLACEMENT	ACTIVITÉS PERTINENTES AU TRAITEMENT
Planisware S.A	200 avenue de Paris, 92320 Chatillon, France	Fourniture de services de support aux Utilisateurs des Clients
Planisware USA Inc.	555 Montgomery Street, Suite 1300 San Francisco, Californie, 94111 États-Unis	
Planisware Deutschland GmbH	52-58 Leonrodstrasse, 80636 Munich, Allemagne	
Planisware UK Ltd.	11h14 - 11h17, Niveau 11 Tour Bleue, Media City Royaume-Uni, Salford, Angleterre, M50 2ST T	
Planisware Singapore Pte Ltd.	600 North Bridge Rd, #10-01, Singapore 188778	
PLW Tunisie SUARL	56 boulevard de la Corniche Avenue de Beji Caid Essebsi, Lac II, 1053 Tunis, Tunisie	
Planisware MIS SARL	5 rue du Helder, 75009 Paris, France	
Planisware MIS (DMCC Dubaï Branch)	Unité 1902 - La Tour du dôme | JLT-PH1-N1 - Tours des lacs Jumeirah	
Planisware Belgique	Avenue des Volontaires 19 1160 Auderghem	
Planisware Korea LLC	354, Gangnam-daero, Gangnam-gu, Séoul, 11F, SW55	
Planisware Japan KK	10e étage, PMO Kojimachi, 6-2-6 Kojimachi, Chiyoda-ku, Tokyo, 102-0083 Japon	

Planisware Italia S.R.L	Viale Giorgio Ribotta 11, CAP 00144 ROMA	
Planisware Austria GmbH	Karl-Farkas-Gasse 22, 1030 Wien	
Planisware Australia Pty Ltd	Suite 302 13/15 Wentworth Ave Sydney NSW 2000	
Planisware MIS	MirMar Business City, Centre Urbain Nord, 1003 Tunis, Tunisie	Fourniture de services de support aux Utilisateurs ainsi que de services gérés, lorsque cela est applicable

PERSONNES CONCERNEES

Le Responsable de Traitement peut soumettre à Planisware des Données Personnelles, dont l'étendue est déterminée et contrôlée par le Responsable de Traitement à sa seule discrétion, et qui incluent les catégories suivantes de Personnes Concernées :

1. Employés du Responsable de Traitement
2. Prestataires du Responsable de Traitement indépendants
3. Autres Utilisateurs, comme autorisé par le Responsable de Traitement en vertu du Contrat
4. Toute personne dont les Données Personnelles sont traitées par le Responsable de Traitement à travers des projets gérés avec la solution de gestion de projet Planisware.

CATÉGORIES DE DONNÉES

Les Données Personnelles transférées concernent les catégories de données suivantes :

1. Les catégories de Données Personnelles traitées pour accéder aux services :
    - Prénom et nom de famille
    - Identifiant système de l'Utilisateur
    - Email Utilisateur
    - Adresse IP
    - Titres de poste/rôles
2. Activité de l'Utilisateur en lien avec le compte du Client,
3. La communication entre les Utilisateurs et le personnel de Planisware en lien avec les services de Support,
4. Le cas échéant, la communication entre les Utilisateurs et le personnel de Planisware en lien avec les Services Professionnels.

CATÉGORIES PARTICULIERES DE DONNÉES

Le Client ne doit pas utiliser les Services pour traiter des Données Personnelles considérées comme des catégories sensibles de données en vertu du Droit Applicable, sans l'accord préalable du signataire de Planisware à ce DPA.

OPÉRATIONS DE TRAITEMENT

Les Données Personnelles traitées font l'objet des traitements de base suivants :

1. Collecte, hébergement et sauvegarde de Données Personnelles à des fins de :
    - Reconnaissance de l'Utilisateur autorisé du Service
    - Permettre l'administration du compte Client par le Responsable de Traitement
    - Fourniture de services de support aux Utilisateurs
    - Le cas échéant, fourniture de Services Professionnels
2. Suppression ou anonymisation des Données Personnelles sur instruction du Client ou à la fin du Contrat.

Planisware
Get innovation to market

ANNEXE 2 – DESCRIPTION DES MESURES DE SECURITE

La présente annexe fait partie intégrante du DPA (et/ou des Clauses Contractuelles Type, le cas échéant).

DESCRIPTION DES MESURES DE SECURITE TECHNIQUES ET ORGANISATIONNELLES MISES EN ŒUVRE PAR PLANISWARE

En vertu de l'article 32 du RGPD, Planisware met en place et maintient un système documenté de gestion de la confidentialité et de la sécurité des informations (incluant des dispositions concernant la conservation des dossiers et le plan de réponse aux incidents), qui comprend des garanties administratives, organisationnelles, techniques et physiques appropriées ainsi que d'autres mesures de sécurité adaptées à la taille et à la complexité du traitement des données, aux préjudices pouvant résulter d'un Incident de sécurité ainsi qu'à la nature et au périmètre des activités de traitement des Données Personnelles. Planisware peut être amenée à mettre à jour ces mesures de sécurité techniques et organisationnelles, tant qu'elles ne diminuent pas de manière significative la sécurité globale du traitement des Données Personnelles.

1. PSEUDONYMISATION / CHIFFREMENT DES DONNÉES PERSONNELLES

Des mesures sont utilisées pour garantir que les Données Personnelles ne puissent pas être lues, copiées, modifiées ou supprimées sans autorisation lors de leur transmission électronique, et que les entités destinataires de tout transfert de Données Personnelles au moyen d'outils de transmission de données puissent être établies et vérifiées.

2. CAPACITÉ À GARANTIR LA CONFIDENTIALITÉ ET L'INTÉGRITÉ CONTINUES DES SYSTÈMES ET SERVICES DE TRAITEMENT

2.1 Mesures visant à empêcher les personnes non autorisées d'accéder physiquement aux systèmes de traitement des Données Personnelles :

a) Définition des personnes ayant obtenu un accès physique aux systèmes où les Données Personnelles sont traitées ;
b) Contrôle des accès électroniques ;
c) Délivrance des identifiants d'accès ;
d) Mise en œuvre de politiques de gestion des visiteurs ;
e) Dispositif d'alarme ou service de sécurité en dehors des heures de service ;
f) Séparation des locaux en différentes zones de sécurité ;
g) Mise en œuvre d'une politique de gestion des badges d'accès ;
h) Porte d'accès sécurisées (ouvre-porte électronique) ;
i) Mise en œuvre de mesures de sécurité sur site (par exemple, alerte/notification d'intrusion).

2.2 Mesures visant à empêcher les personnes non autorisées d'utiliser des équipements de traitement des données personnelles :

a) Définition des personnes pouvant accéder à des équipements de traitement des Données Personnelles ;
b) La mise en œuvre de politiques de gestion des visiteurs ;
c) Protection par mot de passe des ordinateurs du personnel.

2.3 Mesures garantissant que les personnes habilitées à utiliser un système de traitement des données n'ont accès qu'aux Données Personnelles auxquelles elles sont autorisées à accéder conformément à leurs droits d'accès :

a) Mise en œuvre d'une gestion des droits d'accès aux données et fonctions personnelles respectives ;
b) Exigence d'identification vis-à-vis du système de traitement des données (par exemple via l'ID et l'authentification) ;
c) Mise en œuvre d'une politique sur les règles d'accès et profils utilisateur ;
d) Évaluation des procédures en cas d'incidents dommageables.

2.4 Mesures telles que l'enregistrement des saisies de données, afin de garantir qu'il est possible de vérifier et de déterminer si des données personnelles ont été saisies, modifiées ou retirées des systèmes de traitement des données personnelles et, le cas échéant, par qui.

2.5 Mesures visant à garantir que les Données Personnelles traitées pour le compte d'autrui sont traitées conformément aux instructions du Client (Responsable de Traitement et Exportateur de Données), y compris la formation du personnel Planisware et la documentation des demandes de support Client.

2.6 Mesures visant à s'assurer que les Données Personnelles collectées à différentes fins peuvent être traitées séparément, comme l'utilisation de mécanismes de séparation logique des données personnelles de chaque Client du Sous-Traitant Ultérieur.

3. DISPONIBILITÉ ET RÉSILIENCE DES SYSTÈMES ET SERVICES DE TRAITEMENT

Mesures visant à garantir la protection des Données Personnelles contre la destruction ou la perte accidentelle :

a) Mise en place d'un planning de sauvegarde régulier ;
b) Contrôle de l'état des fournisseurs de données à des fins de sauvegarde des Données Personnelles ;
c) Stockage sécurisé des sauvegardes de Données Personnelles ;
d) Mise en œuvre et contrôle régulier des systèmes d'alimentation d'urgence et des systèmes de protection contre les surtensions.

4. DISPONIBILITÉ D'ACCES EN CAS D'INCIDENT PHYSIQUE OU TECHNIQUE

Mesures visant à garantir que les Données Personnelles puissent être restaurées en temps utile en cas de destruction ou de perte accidentelle :

a) La mise en œuvre d'un plan d'urgence ;
b) Protocole sur le déclenchement de la gestion des crises et/ou des situations d'urgence.

5. PROCÉDURES DE TEST, D'APPRECIATION ET D'ÉVALUATION RÉGULIÈRES DE L'EFFICACITÉ DES MESURES TECHNIQUES ET ORGANISATIONNELLES AFIN DE GARANTIR LA SÉCURITÉ DU TRAITEMENT

a) Examen régulier des certifications liées à la sécurité informatique (par exemple, ISO 27001) ;
b) Surveillance par le responsable de la protection des données de Planisware, si désigné, et audit IT concernant la conformité aux processus et exigences déterminés pour la configuration et le fonctionnement des systèmes.

ANNEXE 3 – [Optionnel] Spécificités régionales

Cette annexe fait partie intégrante du DPA.

Abou Dhabi. Lorsque les Données Personnelles protégées par les lois et règlements d'Abou Dhabi relatifs à la protection des données, sont transférées, soit directement, soit par transfert ultérieur, l'avenant aux Clauses Contractuelles Type de l'UE s'applique : https://assets.adgm.com/download/assets/ADGM+-+Data+Transfer+Addendum+to+the+EU+SCC-pdf.pdf/9e08f13a595b11efb0b3aa2a20d5f45b

Argentine. Lorsque les Données Personnelles protégées par la Loi et le Règlement argentins relatifs à la protection des données sont transférées, directement ou par transfert ultérieur, vers tout autre pays qui n'est pas soumis à une décision d'adéquation, les Clauses Contractuelles Type suivantes s'appliquent : http://www.jus.gob.ar/media/3202473/disp_e2016_60_anexoii.pdf

Californie. Lorsque les Données Personnelles protégées par la California Consumer Privacy Act, telle qu'amendée par la California Privacy Rights Act (« CCPA »), sont traitées par Planisware, Planisware traite les Données Personnelles uniquement à des fins professionnelles et opérationnelles applicables aux instructions du client autorisées par la CCPA pour un fournisseur de services, et non pour ses besoins propres (tels que tous ces termes sont définis dans la CCPA). Planisware ne doit pas utiliser ni traiter des Données Personnelles en dehors du champ des services ou de leur relation avec le Client. Planisware n'utilisera aucune Donnée Personnelle à des fins de marketing direct, ni ne vendra ni ne partagera de Données Personnelles, selon la définition de la CCPA. Planisware ne combinera pas les Données Personnelles reçues du Client avec celles reçues d'autres sources. En cas de mise à jour importante concernant le traitement des Données Personnelles par Planisware, Planisware informera immédiatement le Client de ces mises à jour. Planisware certifie qu'elle comprend et respectera les restrictions ci-dessus.

Dubaï. Lorsque les Données Personnelles protégées par les lois et règlements de Dubaï sur la protection des données sont transférées, directement ou par transfert ultérieur, vers un autre pays qui n'est pas soumis à une décision d'adéquation, les Clauses Contractuelles Type suivantes, disponibles en téléchargement, s'appliquent : https://www.difc.com/business/registrars-and-commissioners/commissioner-of-data-protection/data-export-and-sharing

Turquie. Lorsque les Données Personnelles protégées par les lois et règlements turcs sur la protection des données sont transférées, soit directement, soit par transfert ultérieur, les Clauses Contractuelles Type suivantes s'appliquent : https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/d4577ac6-d2cd-4ff4-839f-4218812c3cdc.pdf

Royaume-Uni. Lorsque les Données Personnelles protégées par les lois et règlements britanniques sur la protection des données sont transférées, directement ou par transfert ultérieur, vers tout autre pays qui n'est pas soumis à une décision d'adéquation, l'avenant britannique aux Clauses Contractuelles Type de l'UE s'applique : https://ico.org.uk/media2/migrated/4019539/international-data-transfer-addendum.pdf

Suisse. Lorsque les Données Personnelles protégées par les lois et règlements suisses sur la protection des données sont transférées, directement ou par transfert ultérieur, vers un autre pays qui n'est pas soumis à une décision d'adéquation, l'avenant suisse aux Clauses Contractuelles Type de l'UE s'applique :
« Lorsque le transfert de données personnelles d'un Exportateur de Données vers un Importateur de Données est soumis au RGPD de l'UE et au FADP (Loi fédérale sur la protection des données du 25 septembre 2020 - modifiée pour la dernière fois le 7 juillet 2025), les dispositions supplémentaires suivantes s'appliquent également afin que les Clauses Contractuelles Type soient appropriées afin d'assurer un niveau adéquat de protection pour ce transfert conformément à l'article 6, paragraphe 2, lettre de la FADP :
Le terme « État membre de l'UE » ne doit pas être interprété de manière à exclure les personnes concernées en Suisse de la possibilité de poursuivre leurs droits dans leur lieu de résidence habituelle (Suisse) conformément à l'article 18(c) des Clauses Contractuelles Type.
Le Commissaire fédéral à la protection des données et à l'information est l'autorité de surveillance compétente en matière de transfert des données personnelles hors de Suisse. »

Arabie Saoudite. Lorsque les Données Personnelles protégées par les lois et règlements saoudiens sur la protection des données sont transférées, soit directement, soit par transfert ultérieur, les Clauses Contractuelles Type suivantes s'appliquent : https://sdaia.gov.sa/Documents/StandardContractualClausesForPersonalDataTransferEN.pdf