ANNEXE A

SOUS-TRAITANCE DES DONNEES A CARACTERE PERSONNEL DU CLIENT (ci-après le "responsable de traitement") PAR INDOOR INFORMATIQUE (ci-après le "sous-traitant")

Cette annexe vise la relation contractuelle dans laquelle INDOOR INFORMATIQUE s'engage à fournir au Client des prestations de service et qui implique notamment la manipulation des données à caractère personnel traitées par le Client. Dans ce contexte, et au sens du RGPD, le Client a le rôle de « responsable de traitement », et INDOOR INFORMATIQUE a le rôle de « sous-traitant ».

Les clauses qui suivent ont pour objet de définir les conditions dans lesquelles le Client, en tant que responsable de traitement, confie à INDOOR INFORMATIQUE, en tant que sous-traitant, des opérations de traitement de données personnelles à effectuer pour son compte.

Cette annexe a pour objet de déterminer les engagements que chaque Partie prend afin de se conformer à l'ensemble des lois et réglementations applicables en matière de protection des données personnelles et notamment avec le Règlement (UE) 2016/679 du Parlement européen du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après le « **RGPD** »).

Cette présente annexe fait partie intégrante des Conditions Générales de Vente qui règlementent la relation d'affaires entre INDOOR INFORMATIQUE et le Client.

1. Description du traitement faisant l'objet de la sous-traitance

Services fournis par INDOOR INFORMATIQUE (selon les prestations commandées par le Client	- Prestation d'installation, de mises à jour, de paramétrage des Produits et Logiciels vendus au Client. - Prestation d'assistance et de support impliquant l'intervention d'un technicien INDOOR INFORMATIQUE sur le site du Client. - Prestations supplémentaires choisies par le Client, telles que : audit, reprise de parcs, déménagement, paramétrage spécifique, intégration.
Nature des opérations réalisées	Toute opération rendue nécessaire pour fournir les prestations commandées par le Client, et en particulier : - l'accès, la consultation, la collecte, la structuration, la modification des données afin de paramétrer, mettre à jour et maintenir les Produits et Logiciels ; - la structuration, l'hébergement et la minimisation de certaines données pour maintenir la base de connaissance des techniciens INDOOR INFORMATIQUE et faciliter les interventions ultérieures chez le Client; - la destruction des données conservées par INDOOR INFORMATIQUE à l'issue de la relation contractuelle avec le Client.
Finalité du traitement	Les finalités du traitement réalisé par le Client doivent être déterminées par lui, à sa seule discrétion, et être communiquées à INDOOR INFORMATIQUE. Les finalités

	devront être déterminées, explicites, légitimes et licites. INDOOR INFORMATIQUE devra être alertée si le Client a considéré que son traitement présentait un risque élevé pour les droits et libertés des personnes physiques.
Catégories de données à caractère personnel traitées	Les catégories de données à caractère personnel traitées dépendent de l'activité et des finalités déterminées par le Client. De façon générale, les catégories suivantes sont couramment utilisées et peuvent donc être considérées comme étant traitées : Identité : civilité, nom ou raison sociale, prénoms, adresse (y compris siège social, lieu de facturation, numéro de téléphone, adresses courriel) Toute autre catégorie de données à caractère personnel traitée par le Client devra être notifiée à INDOOR INFORMATIQUE. En particulier, INDOOR INFORMATIQUE devra être informée lorsque les catégories de données à caractère personnel traitées par le Client concerneront : - des catégories particulières de données au sens de l'article 9 du RGPD, c'est-à-dire des données sensibles. - ou des données relatives aux condamnations pénales et aux infractions au sens de l'article 10 du RGPD ; - ou le numéro d'identification national au sens de l'article 87 du RGPD.
Catégories de personnes concernées :	Les catégories de personnes concernées dépendront de l'activité et des finalités déterminées par le Client et doivent être déterminées par lui, à sa seule discrétion, et être communiquées à INDOOR INFORMATIQUE.
Durée de conservation :	INDOOR INFORMATIQUE met en œuvre des durées de conservation adaptées aux opérations de traitement qu'elle est amenée à effectuer, en fonction des prestations de services fournies au Client et conformément au principe de minimisation. A la fin de ses interventions sur site ou à distance, INDOOR INFORMATIQUE supprime par principe toute copie de données à caractère personnel qu'elle aurait pu avoir à faire, sauf lorsqu'une conservation de celles-ci est nécessaire pour établir un compte-rendu d'intervention. Dans certains cas, INDOOR INFORMATIQUE peut être amenée à conserver des modèles de documents utilisés par le Client (matrice de documents spécifiques qui ne sont pas couramment utilisé sur le marché, exigences particulières du Client) afin de consolider la base de connaissance de ses techniciens et faciliter les interventions ultérieures chez le Client. Autant que possible, INDOOR INFORMATIQUE minimisera les données figurant sur ces modèles de documents, sauf lorsque leur lisibilité est requise pour comprendre et tester le paramétrage souhaité par le Client. Lorsque la relation contractuelle entre le Client et INDOOR INFORMATIQUE cesse, INDOOR INFORMATIQUE supprimera les catégories de données à caractère personnel qu'elle est susceptible d'avoir conservé dans sa base de connaissance Client sur simple notification du Client.

2. Durée de l'accord RGPD

Le présent accord RGPD entre en vigueur à compter de la signature de l'accord de partenariat auquel il est annexé et sera valable pendant toute la durée dudit accord de partenariat.

3. Obligations de INDOOR INFORMATIQUE en tant que sous-traitant

INDOOR INFORMATIQUE s'engage à :

- traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de la sous-traitance ;
- traiter les données conformément aux instructions documentées du Client. Si INDOOR INFORMATIQUE considère qu'une instruction constitue une violation du RGPD ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en informe immédiatement le Client. En outre, si INDOOR INFORMATIQUE est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer le Client de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;
- garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat ;
- veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent contrat :
    - s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
    - reçoivent la formation nécessaire en matière de protection des données à caractère personnel ;
- prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut.

4. Sous-traitant de INDOOR INFORMATIQUE

INDOOR INFORMATIQUE pourra être amenée à faire appel à des sous-traitants ultérieurs pour mener certaines activités de traitement spécifiques.

INDOOR INFORMATIQUE pourra être amenée à modifier ou compléter la liste des sous-traitants ultérieurs auxquels elle fait appel. Dans ce cas, INDOOR INFORMATIQUE informe préalablement et par écrit le Client. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Le Client dispose d'un délai de quinze (15) jours ouvrés à compter de la date de réception de cette information pour présenter ses objections.

Les sous-traitants ultérieurs de INDOOR INFORMATIQUE sont tenus de respecter les mêmes obligations que celles convenues dans le présent accord RGPD. Il appartient à INDOOR INFORMATIQUE de s'assurer que ses sous-traitants ultérieurs présentent les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données.

Si INDOOR INFORMATIQUE souhaite procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu de la règlementation précitée, il doit au préalable s'assurer que le sous-traitant ultérieur prend des garanties adéquates pour encadrer le transfert de données conformément aux exigences du RGPD, telle que (i) l'existence d'une décision d'adéquation de la Commission européenne, (ii) des clauses standards de protection des données adoptées par la Commission européenne, (iii) des codes de conduite approuvés conformément au RGPD,
(iv) des mécanismes de certification approuvés conformément au RGPD, (v) des clauses contractuelles validées par la CNIL.

5. Droit d'information des personnes concernées

Il appartient au Client de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

6. Exercice du droit des personnes

Dans la mesure du possible, INDOOR INFORMATIQUE doit aider le Client suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

7. Notification des violations de données à caractère personnel

INDOOR INFORMATIQUE notifie au Client toute violation de données à caractère personnel dans un délai maximum de 24 heures après en avoir pris connaissance et par courrier électronique. Cette notification est accompagnée de toute documentation utile afin de permettre au Client, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

8. Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations

INDOOR INFORMATIQUE aide le Client pour la réalisation d'analyses d'impact relative à la protection des données. Cette aide se limitera à fournir des informations techniques sur les mesures de sécurité mises en œuvre et ne dégage pas le Client de mener la réalisation de l'analyse d'impact qu'il lui incombe.

INDOOR INFORMATIQUE aide le Client pour la réalisation de la consultation préalable de l'autorité de contrôle. Ces prestations d'assistance seront indemnisées moyennant une facturation supplémentaire raisonnable, compte-tenu de la nécessité de mobiliser des ressources techniques et humaines pour l'exécution de ces prestations.

9. Mesures de sécurité

INDOOR INFORMATIQUE s'engage à mettre en œuvre toutes les mesures de sécurité techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

Il met en œuvre notamment les mesures de sécurité suivantes :

- **Sensibilisation des utilisateurs :**
  - Information et sensibilisation des personnes manipulant les données
  - Rédaction d'une charte informatique et donner à celle-ci une force contraignante
- **Authentification des utilisateurs :**
  - Définition d'un identifiant (login) unique à chaque utilisateur
- **Adoption d'une politique de mot de passe utilisateur conforme aux recommandations de la CNIL**
  - Obligation faite à l'utilisateur de changer son mot de passe après réinitialisation
  - Limitation du nombre de tentatives d'accès à un compte
- **Gestion des habilitations**
  - Définition des profils d'habilitation
  - Suppression des permissions d'accès obsolètes
  - Réalisation d'une revue annuelle des habilitations
- **Traçage des accès et gestion des incidents**
  - Prévision d'un système de journalisation
  - Information des utilisateurs de la mise en place du système de journalisation
  - Protection des équipements de journalisation et des informations journalisées
  - Prévision des procédures pour les notifications de violation de données à caractère personnel
- **Sécurisation des postes de travail**
  - Prévision d'une procédure de verrouillage automatique de session
  - Utilisation des antivirus régulièrement mis à jour
  - Installation d'un « pare-feu » (firewall) logiciel
  - Recueil de l'accord de l'utilisateur avant toute intervention sur son poste
- **Sécurisation de l'informatique mobile**
  - Prévision des moyens de chiffrement des équipements mobiles
  - Sauvegardes ou synchronisations régulières des données
  - Secret exigé pour le déverrouillage des smartphones
- **Protection du réseau informatique interne**
  - Limitation des flux réseau au strict nécessaire
  - Sécurisation des accès distants des appareils informatiques nomades par VPN
  - Mise en œuvre du protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi
- **Sécurisation des serveurs**
  - Limitation de l'accès aux outils et interfaces d'administration aux seules personnes habilitées
  - Installation sans délai des mises à jour critiques
  - Assurance de la disponibilité des données
- **Sauvegarde et prévision de la continuité d'activité**
  - Sauvegardes régulières
  - Stockage des supports de sauvegarde dans un endroit sûr
  - Prévision des moyens de sécurité pour le convoyage des sauvegardes
  - Prévision et tests réguliers de la continuité d'activité
- **Archivage de manière sécurisée**
  - Mise en œuvre des modalités d'accès spécifiques aux données archivées
  - Destruction des archives obsolètes de manière sécurisée
- **Encadrement de la maintenance et de la destruction des données**
  - Enregistrement des interventions de maintenance dans une main courante
  - Encadrement par un responsable de l'organisme des interventions par des tiers
  - Effaçage des données de tout matériel avant sa mise au rebut
- **Gestion de la sous-traitance**
  - Prévision d'une clause spécifique dans les contrats des sous-traitants

- Prévision des conditions de restitution et de destruction des données

- **Protection des locaux**
  - Restriction des accès aux locaux au moyen de portes verrouillées
  - Installation d'alarmes anti-intrusion et vérifications périodiques de celles-ci

10. Sort des données

Au terme des prestations de services relatives au traitement de ces données, INDOOR INFORMATIQUE s'engage à détruire toutes les données à caractère personnel.

11. Registre des catégories d'activités de traitement

INDOOR INFORMATIQUE déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du Client comprenant :

- le nom et les coordonnées du Client pour le compte duquel il agit, des éventuels sous- traitants et, le cas échéant, du délégué à la protection des données ;

- les catégories de traitements effectués;

- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;

- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles.

12. Documentation

INDOOR INFORMATIQUE met à la disposition du Client la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le Client ou un autre auditeur qu'il a mandaté, et contribuer à ces audits. Toute demande d'audit et/ou d'inspection devra être demandée par le Client par lettre recommandée avec accusé de réception au moins 15 jours avant la date envisagée pour sa réalisation ainsi que sur l'identité des auditeurs envisagés. INDOOR INFORMATIQUE confirmera sous 7 jours au Client la possibilité de cette date et faire d'éventuelles réserves objectives (non-concurrence) sur les auditeurs envisagés. Tout audit et/ou inspection ne pourra être réalisée qu'après qu'un accord de confidentialité ait été signé entre INDOOR INFORMATIQUE et l'ensemble des auditeurs.

.A.R.L au capital de 2000 Euros
Code APE 6201Z
R.C.S NANTERRE B 324 103 829
SIRET : 750 364 689 000 26

Indoor Informatique
25 Rue Henri Chapron
92600 Asnières sur Seine
06 79 85 36 11