CONDITIONS GÉNÉRALES
SUR LA PROTECTION DES DONNÉES A CARACTÈRE PERSONNEL

1 - Préambule

La société CIS ISTA, société anonyme, immatriculée au Registre du commerce et des sociétés d'Evry sous le numéro 582 017 810, dont le siège social est situé 30 avenue Carnot – 91 300 Massy (ci-après le « **Prestataire** ») a conclu avec votre société (ci-après le « **Client** ») un contrat de fourniture de service de pose, location, entretien des compteurs de consommation d'eau ou de chauffage avec télé relève chez les locataires ou propriétaires des immeubles que vous gérez (ci-après les « **Usagers** »), ainsi que de transmission et mise à disposition des données des Usagers via un portail internet (ci-après les « **Services** »). Ce contrat est en cours d'exécution à la date d'entrée en vigueur des présentes (ci-après le « **Contrat** »).

Dans le cadre de l'exécution des Services, le Prestataire est amené à collecter et traiter, pour le compte du Client, des données des Usagers qui constituent des données à caractère personnel au sens de l'article 4 du Règlement (UE) 2016/679 du 27 avril 2016 dit Règlement général sur la protection des données (ci-après le « **Règlement** »).

Conformément aux dispositions de l'article 28 du Règlement, les présentes conditions générales et particulières ont pour objet de définir les conditions dans lesquelles le Prestataire, en sa qualité de sous-traitant, s'engage à effectuer pour le compte du Client, en sa qualité de responsable du traitement, les opérations de collecte et de traitement de données à caractère personnel objets des Services (ci-après les « **Conditions générales** »).

Dans le cadre de leurs relations contractuelles, les parties aux présentes s'engagent à respecter la réglementation en vigueur applicable en matière de traitement de données à caractère personnel et, en particulier, le Règlement.

Les Conditions générales pourront faire l'objet de tout complément afin de prendre en compte les évolutions ultérieures des textes applicables en application du Règlement ou autre disposition législative ou règlementaire applicable, ce que chacune des parties reconnaisse et accepte.

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

Le Prestataire est autorisé à traiter pour le compte du Client les données à caractère personnel nécessaires pour fournir les Services et exécuter les opérations tels que décrits dans le Contrat, et qui sont notamment :

- La relève des compteurs individuels ;
- Les données issues de tous les types de contrats d'entretien ou de maintenance ista ;
- L'exploitation et la transmission des données de comptage ;
- La mise à disposition du Client des données via un portail internet ;
- Les prestations de robinetterie.

Le Client indique au Prestataire que les finalités du traitement sont (i) la gestion de la consommation d'eau ou de chauffage par les Usagers, ainsi que (ii) l'analyse des données de consommation des Usagers.

Les données à caractère personnel traitées dans le cadre des présentes sont les données des Usagers, ainsi que les données des gestionnaires et autres intermédiaires chez le Client et le Prestataire.

Les données collectées et traitées à ce titre sont les suivantes (ci-après les « **Données** ») :

- Données d'identification : nom, prénom, adresse postale, adresse email, numéro de logement, numéro de programme / bâtiment / escalier, numéro de téléphone ;
- Données de consommation : numéro de compteur, index de consommation, clé de répartition ;
- Données de facturation : numéros de carte bancaire, numéros BIC et IBAN en cas de prélèvement SEPA, numéros de référence du contrat, date et heure du paiement, moyen de paiement utilisé, date d'expiration du moyen de paiement, montant du paiement.

3 - Obligations du Prestataire vis-à-vis du Client

Le Prestataire s'engage à respecter les dispositions suivantes :

3.1 – Traitement des Données par le Prestataire

(i) Traiter uniquement les Données à caractère personnel pour les finalités qui font l'objet de la sous-traitance.

(ii) Traiter les Données à caractère personnel conformément aux instructions documentées du Client, figurant dans tout document adressé par le Client au Prestataire, par tout moyen jugé utile. Il est précisé qu'à défaut d'instructions écrites, les parties aux présentes conviennent que toute opération réalisée par le Prestataire au titre de l'exécution du Contrat et conforme aux dispositions de ce dernier, constitue une instruction du Client.

Si le Prestataire considère qu'une instruction constitue une violation du Règlement ou toute autre disposition de la loi française applicable, il s'engage à en informer immédiatement le Client. Le Client reconnaît et accepte que dans une telle hypothèse, le Prestataire pourra, à sa libre discrétion, suspendre l'exécution des instructions litigieuses tant qu'il estime que celle-ci n'est pas conforme au Règlement et/ou à la loi française.

Dans l'hypothèse où le Prestataire serait tenu de procéder à un traitement de Données en vertu d'une disposition impérative résultant du droit communautaire ou du droit français, le Prestataire informera le Client de cette obligation juridique avant le traitement des Données, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

(iii) Garantir la confidentialité des Données traitées dans le cadre des présentes.

(iv) Veiller à ce que les personnes autorisées à traiter les Données en vertu des présentes s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité et reçoivent la formation nécessaire en matière de protection des données à caractère personnel.

(v) 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.

3.2 – Transfert des Données hors Union Européenne

En cas de transfert de tout ou partie des Données vers un pays tiers, hors Union européenne, ou vers une organisation internationale, le Prestataire devra obtenir l'accord préalable écrit du Client, par tout moyen jugé utile.

Le cas échéant, le Prestataire s'engage à coopérer avec le Client afin d'assurer :

- le respect des procédures permettant de se conformer à la règlementation locale ;

- si besoin, la conclusion d'un ou plusieurs contrats permettant d'encadrer les flux transfrontaliers de Données. Le Prestataire s'engage en particulier, si nécessaire, à obtenir la conclusion de tels contrats par ses sous-traitants ultérieurs. Dans ce cadre, les Parties conviennent d'utiliser les clauses contractuelles types publiées par la Commission européenne pour encadrer les flux transfrontaliers de données à caractère personnel.

3.3 – Sous-traitance

Le Prestataire est expressément autorisé par le Client à communiquer aux gardiens des immeubles dont le Client a la charge et dans lesquels le Prestataire est chargé d'exécuter les Services, des données lorsque cela est strictement nécessaire à l'exécution desdits Services, conformément aux dispositions du Contrat et des présentes Conditions Générales. Le Client reconnaît et accepte que le Prestataire n'exerce aucun contrôle d'aucune sorte sur le gardien et ne saurait en aucun cas garantir le respect par ledit gardien des mesures de protection appropriée des Données qui lui sont communiquées. Les Parties conviennent expressément que le gardien doit en conséquence être considéré comme un sous-traitant ultérieur du Client, et que la responsabilité du Prestataire ne pourra en aucun cas être engagée au titre de l'exécution de ses obligations à l'égard de la protection des données par le gardien. Il appartient au seul Client de s'assurer que le gardien présente des 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.

Dans l'hypothèse où le Client estimerait que le gardien ne présente pas les garanties suffisantes pour permettre au Prestataire de lui communiquer des Données dans le cadre de l'exécution des Services, il s'engage à en informer immédiatement et par écrit le Prestataire.

Au titre de la présente clause, il convient de distinguer deux catégories de sous-traitants :

(i) les sous-traitants mandatés par le Prestataire pour exécuter tout ou partie des services qui constituent l'objet même du Contrat, et notamment la relève des compteurs et des appareils de mesure et comptage, l'installation et la maintenance desdits appareils (ci-après les « **Sous-traitants Principaux** » ;

(ii) les sous-traitants mandatés par le Prestataire pour exécuter des prestations connexes aux Services, telles que notamment, les services de télécommunication, les services de messageries, les services de maintenance de sa plateforme en ligne ou de ses serveurs, les services de suppression des Données, ainsi que tous prestataires utilisés pour lui permettre la

mise en place des mesures techniques prévues à l'article 3.8 des présentes et notamment toutes les mesures visant à garantir la confidentialité, la disponibilité, l'intégrité et la résistance du matériel et des logiciels nécessaires aux systèmes de traitement des Données (ci-après les « **Sous-traitants Connexes** »).

Le Sous-traitant ultérieur quel qu'il soit, c'est-à-dire Sous-traitant Principal ou Sous-traitant Connexe, sera tenu de respecter les obligations des présentes Conditions générales pour le compte et selon les instructions du Client. Il appartient au Prestataire de s'assurer que le Sous-traitant ultérieur présente 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. Si le Sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le Prestataire demeure pleinement responsable devant le Client de l'exécution par l'autre sous-traitant de ses obligations.

Le Prestataire peut faire appel à d'autres Sous-traitants sur la base d'un consentement écrit généralement accordé dans le présent.

Le Prestataire doit informer le Client de tout changement pouvant être apporté à la participation ou au remplacement d'autres sous-traitants, en lui communiquant la liste mise à jour des sous-traitants, à l'adresse Internet suivante www.ista.com/fr/confidentialite/sous-traitants

Cette liste sera également mise à disposition sur simple demande aux adresses mails de contacts fournis à nos clients, visibles sur le site Web du prestataire et sur les documents de communication entre le Client et le Prestataire. Notamment :

- istaidf@ista.fr
- istanantes@ista.fr
- istalille@ista.fr
- istarouen@ista.fr
- istastrasbourg@ista.fr
- istadijon@ista.fr
- istanice@ista.fr
- istamarseille@ista.fr
- istabordeaux@ista.fr
- istalyon@ista.fr
- istatours@ista.fr

Le Client pourra ainsi se tenir toujours informé de l'état actuel des sous-traitants répertoriés.

Cette liste sera notifiée au client 1 fois par an.

Le Client pourra émettre toutes observations dans un délai de dix (10) jours calendaires à compter de la notification de la liste modifiée. La sous-traitance ne pourra être effectuée dans l'hypothèse où le Client émettrait une objection pendant le délai ainsi convenu portant sur l'absence de garantie d'un niveau de sécurité suffisant par le Sous-traitant Principal ou du non-respect des dispositions des présentes ou de la législation applicable. Toute autre objection sera étudiée par le Prestataire qui reste libre de poursuivre ou non la sous-traitance.

Néanmoins, le Client reconnaît et accepte que dans l'hypothèse où il recrute directement un sous-traitant ultérieur, sans l'assistance du Prestataire, la responsabilité du Prestataire ne pourra en aucun cas être engagée au titre de l'exécution de ses obligations par ledit sous-traitant. Il appartient au seul Client de s'assurer que le sous-traitant ultérieur qu'il a sélectionné présente des 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.

3.4 – Droit d'information des personnes concernées

Il appartient au Client de fournir l'information aux personnes concernées par les opérations de traitement à tout moment jugé utile et au plus tard au moment de la collecte des Données.

3.5 – Exercice des droits des personnes concernées

Dans la mesure du possible, le Prestataire doit aider le Client à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées, à savoir droit d'accès, de rectification, d'effacement et d'opposition, de limitation du traitement, de portabilité des Données et de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Dans ce cadre, lorsque les personnes concernées exercent auprès du Prestataire lesdites demandes, il doit adresser ces demandes dès réception au Client par courrier électronique à l'adresse de notification renseignée par celui-ci dans le Contrat ou par tout autre moyen jugé utile.

3.6 – Notification des violations de données à caractère personnel

En cas de violation de Données, le Prestataire s'engage à procéder à toutes investigations utiles sur les manquements aux règles de protection, afin d'y remédier dans les plus brefs délais et/ou de diminuer dans la mesure du possible, l'impact de tels manquements auprès des personnes dont les données ont été collectées.

Le Prestataire notifie au Client toute violation de données à caractère personnel dans un délai maximum de 48 heures après en avoir pris connaissance et par email. 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.

La notification doit contenir au moins :

(i) la description de la nature de la violation de Données y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de Données concernés ;

(ii) le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;

(iii) la description des conséquences probables de la violation de Données;

(iv) la description des mesures prises pour remédier à la violation de Données, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

3.7 – Aide du Prestataire dans le cadre du respect par le Client de ses obligations

Le Prestataire aide le Client pour la réalisation si nécessaire d'analyse d'impact relative à la protection des Données et pour la réalisation de la consultation préalable de l'autorité de contrôle le cas échéant, suivant des conditions financières à négocier au regard des services à fournir à cet effet.

3.8 – Mesures de sécurité

Le Prestataire s'engage à mettre en œuvre toutes mesures techniques et organisationnelles appropriées pour protéger les Données pendant toute la durée du Contrat, en fonction de l'état des connaissances, les coûts de mise en œuvre et la nature, la portée et les finalités du traitement, ainsi que les risques que représentent ledit traitement pour les droits et libertés des personnes physiques, afin de garantir un niveau de sécurité adapté.

Le Prestataire s'engage notamment à mettre en œuvre toutes mesures propres à empêcher toute déformation, altération, endommagement, destruction de manière fortuite ou illicite, perte, divulgation et/ou tout accès non autorisé par un tiers.

Dans ce cadre, le Prestataire s'engage à prendre les mesures suivantes :

- Confidentialité (Article 32(1) lettre b RGPD)
    - Contrôle de l'accès aux données
        - mesures de sécurité antieffraction (sécurité des portes, système d'alarme avec service de sécurité)

    - Contrôle de l'accès
        - les personnes autorisées peuvent seulement accéder aux données pour lesquelles un accès leur a été accordé
        - recours à des logiciels de protection antivirus continuellement mis à jour
        - protection des échanges d'emails contre les virus et spams (protection antivirus centrale et système de filtre des spams)
        - systèmes de pare-feu
        - protection par un mot de passe (composé d'au moins 8 chiffres, d'une combinaison de lettres, chiffres, caractères spéciaux, devant être obligatoirement changé après 90 jours)

    - Contrôle de la séparation
        - recours à des logiciels testés
        - séparation de l'environnement de production, de test et de développement

- Intégrité (Article 32(1) lettre. b RGPD)
    - Contrôle du transfert
        - cryptage/ recours à des tunnels VPN pour les transmissions
        - cryptage SSL pour l'accès Internet
        - contrôle du flux de communication du système (systèmes pare-feu centraux, connexions WAN exclusives avec contrôles des accès),

- Contrôle de la saisie
  - il est possible de définir ultérieurement si les données de référence du client ont été saisies, modifiées ou supprimées dans les systèmes de traitement des données ainsi que l'identité des personnes ayant réalisé ces actions (enregistrement),

- Disponibilité et capacité (Article 32(1) lettre b, c RGPD)
  - Contrôle de la disponibilité
    - les données à caractère personnel sont continuellement disponibles et protégées de tout risque de destruction ou perte accidentelle, grâce à une sauvegarde permanente,
    - concept de la sauvegarde des données (sauvegarde régulière : journalière, hebdomadaire, mensuelle), modalités de stockage des sauvegardes (compartiments sécurisés, séparés, résistants au feu),
    - sections spécifiquement protégées du centre de données (séparation structurelle, systèmes séparés de contrôle des accès, parois de protection contre les incendies dans toutes les zones du centre de données,
    - dispositifs de protection anti-incendie au siège et sur les sites,

- Procédures de révision, d'analyse et d'évaluation régulière (Article 32(1) (d) RGPD, Article 25(1) RGPD)
    - les personnes employées sont informées des exigences en matière de protection des données via un règlement intérieur sur l'utilisation des données informatisées
    - Dans l'hypothèse où le responsable de traitement exigerait des mesures spécifiques, les Parties se réuniront alors pour en étudier la faisabilité et convenir des conditions opérationnelles et financières à négocier au regard des mesures impliquées.

En cas de modification des mesures techniques mises en place pour assurer la sécurité et la confidentialité des Données, le Prestataire s'engage à les remplacer par des mesures n'emportant pas de régression du niveau de sécurité.

Le Prestataire s'engage à maintenir ces moyens tout au long de l'exécution du Contrat et, à défaut, à en informer immédiatement le Client.

3.9 – Sort des Données

Le Prestataire reconnaît et accepte qu'il ne peut pas, de son propre chef, corriger, supprimer, ni restreindre le traitement des Données dans le cadre des Services. Il ne peut agir que sur instructions du Client. Dans l'hypothèse où une personne prendrait contact avec le Prestataire pour l'une de ses actions, il s'engage à transmettre sans délai la demande au Client.

Le Prestataire s'engage à ne réaliser aucune copie ni aucun double des Données sans en avoir préalablement informé le Client. Ne sont pas concernées les copies jugées nécessaires à la réalisation des Services et à la garantie d'un traitement approprié des Données.

Au terme de la prestation de services relatifs au traitement des Données ou à la demande expresse du Client, le Prestataire s'engage à restituer les Données, en intégralité, ainsi que toutes les copies desdites Données où à les détruire, sur instruction du Client. Le registre de suppression est tenu à disposition du Client sur simple demande.

Le Client reconnaît et accepte que soient soustraites à l'obligation de destruction et de restitution les Données pour lesquelles le Prestataire a une obligation juridique de conservation.

3.10 – Délégué à la protection des données du Prestataire

Le Prestataire informe le Client avoir nommé un délégué à la protection des données dont les coordonnées sont les suivants :

Adresse postale :
Ista France
Directions des Opérations RGPD
30 avenue Carnot
91300 MASSY

Mail :
DPO_ISTA@ista.fr

3.11 – Registre des catégories d'activité de traitement

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

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

(ii) les catégories de traitements effectués pour le compte du Client ;

(iii) le cas échéant, les transferts de Données 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, les documents attestant de l'existence de garanties appropriées ;

(iv) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :

- la pseudonymisation et le chiffrement des Données;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- des moyens permettant de rétablir la disponibilité des Données et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

3.12 - Documentation

Le Prestataire met à la disposition du Client la documentation nécessaire pour démontrer le respect de toutes ses obligations au titre des présentes Conditions générales, qu'il s'engage à fournir sur simple demande.

La preuve de ces mesures peut être fournie au moyen de certificats valides, de rapports ou d'extraits de rapports délivrés par des autorités indépendantes (telles qu'un auditeur, un chargé d'audit, un délégué à la protection des données, le département de sécurité informatique, les auditeurs chargés de la protection des données, les auditeurs qualité) ou d'une certification adaptée émanant de la sécurité informatique ou de l'audit sur la protection des données.

Le Client se réserve le droit de procéder à toutes vérifications qui lui paraissent utiles pour constater le respect des obligations précitées, et notamment en procédant à un audit auprès du Prestataire ou directement auprès d'un sous-traitant ultérieur.

Le Client est tenu d'informer le Prestataire de toute opération de contrôle au moins deux (2) semaines avant la date dudit contrôle. Les personnes chargées de réalisées cet audit par le Client s'engagent à protéger la confidentialité vis-à-vis du Prestataire. Cette obligation de confidentialité doit satisfaire des exigences élevées de sécurité. Les personnes employées ne peuvent entretenir une quelconque relation avec un concurrent du Prestataire.

Le Prestataire s'engage à répondre aux demandes d'audit du Client effectuées par lui-même ou par un tiers de confiance qu'il aura sélectionné, reconnu en tant qu'auditeur indépendant, c'est-à-dire indépendant du Prestataire, ayant une qualification adéquate, et libre de fournir les détails de ses remarques et conclusion d'audit au Responsable de traitement.

Les audits visés doivent permettre une analyse du respect par le Prestataire de ses obligations visées par les présentes.

3.13 – Services complémentaires

Au titre des présentes, le Prestataire peut être amené à fournir aux Clients, sur demande de ce dernier, des services qui ne sont pas initialement prévus dans le Contrat, relatifs à la protection des Données (ex : audit, soutien dans le cadre d'une enquête menée par des autorités de contrôle).

Ces services supplémentaires doivent être rémunérés en plus de la rémunération prévue pour les Services ne portant pas sur la protection des Données, spécifiés dans le Contrat, en fonction des dépenses réellement engagées dans chaque cas.

4 - Obligations du Client vis-à-vis de la Société

Le Client s'engage à :

- Fournir au Prestataire les informations suivantes, afin de lui permettre d'établir son registre des traitements de sous-traitant :
    - Le nom et les coordonnées du Client ou de tout autre responsable du traitement lorsque le traitement est opéré pour plusieurs responsables de traitement ;

- Les coordonnées du Délégué à la protection des données du Client.

- Fournir à la Société les Données nécessaires à l'exécution des Services ;

- Documenter par écrit toute instruction concernant le traitement des données par la Société.

- Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen ;

- Superviser le traitement.

5 - Coopération en cas de contrôle

En cas de contrôle d'une autorité compétente, les Parties s'engagent à coopérer entre elles et avec l'autorité de contrôle.

Dans le cas où le contrôle mené ne concernerait que les traitements mis en œuvre par le Prestataire en tant que responsable de traitement, le Prestataire fera son affaire du contrôle et s'interdira de communiquer ou de faire état des Données du Client.

Dans le cas où le contrôle mené chez le Prestataire concernerait les traitements mis en œuvre au nom et pour le compte du Client, le Prestataire s'engage à en informer immédiatement le Client et à ne prendre aucun engagement pour elle.

En cas de contrôle d'une autorité compétente chez le Client portant notamment sur les prestations délivrées par le Prestataire, ce dernier s'engage à coopérer avec le Client et à lui fournir toute information dont il pourrait avoir besoin ou qui s'avèrerait nécessaire.

6. – Durée

Les présentes Conditions générales entrent en vigueur à compter du 25 mai 2018 pour une durée identique à celle du Contrat, en ce compris ses reconductions, et dont la date d'échéance reste inchangée.

7 – Acceptation

Le Client reconnaît et accepte que les présentes Conditions générales répondent à l'obligation légale prévue à l'article 28 du RGPD de conclure un acte écrit encadrant les relations entre sous-traitant et responsable du traitement en cas de traitement de données à caractère personnel.

Le Client reconnaît et accepte que les présentes Conditions générales viennent compléter le Contrat et s'appliquent automatiquement à l'issue d'un délai de quinze (15) jours à compter de la date de réception des présentes Conditions générales, sans qu'une signature ou un accord écrit ne soit nécessaire. A défaut de contestation écrite du Client dans ce délai, le Client reconnaît accepter pleinement et expressément lesdites Conditions générales.

Le Client qui n'accepte pas les présentes Conditions générales doit en informer le Prestataire et, à défaut d'accord sur les conditions de la collecte et du traitement des Données, mettre un terme au Contrat.