Déclaration d'engagement d'ista Luxembourg S.à r.l. sur le traitement des commandes.

Nous, ista Luxembourg S.à r.l., 23, rue des Bruyères, L-1274 Howald, traitons des données à caractère personnel pour vous sur la base de la relation contractuelle existant entre vous et nous. Afin de garantir que ces données personnelles soient traitées conformément aux règles de protection des données, nous délivrons la déclaration d'engagement suivante concernant le traitement des données commandées conformément à l'article 28 du Règlement général sur la protection des données (RGPD) (ci-après dénommée « déclaration d'engagement ») :

1. Objet et durée de la déclaration d'engagement

(1) Objet
L'objet de la déclaration d'engagement et vos coordonnées résultent de la commande ou du contrat-cadre conclu avec vous, auquel il est fait référence ici (ci-après dénommé « contrat de service »).

(2) Durée
La durée de cette déclaration d'engagement (terme ou période de validité) correspond à la durée du contrat de service, sans préjudice quant à la durée légale prévoyant une durée de conservation des données envisagées par la présente déclaration plus longue.

2. Spécification du contenu de la déclaration d'engagement

(1) Nature et finalité du traitement de données envisagé La nature et la finalité du traitement des données personnelles que nous effectuons pour vous sont spécifiquement décrites dans le contrat de service.
La fourniture du traitement de données convenu contractuellement a lieu exclusivement dans un État membre de l'Union européenne ou dans un autre État signataire de l'Accord sur l'Espace économique européen. Toute externalisation / délocalisation dans un pays tiers nécessite votre consentement préalable et ne peut avoir lieu que si les exigences particulières des articles 44 et suivants du RGPD sont remplies.

(2) Type de données
Les types / catégories de données suivants font l'objet d'un traitement de données à caractère personnel :

- Données d'identification de la personne concernée
- Données de communication (par exemple, téléphone, courrier électronique)
- Données de base du contrat (relation contractuelle, intérêt du produit ou du contrat)
- Historique des clients
- Données de facturation et de paiement des contrats
- Données de planification et de contrôle
- Données sur le locataire / propriétaire de l'appartement (par exemple, nom, adresse, clé de répartition, données de consommation)

(3) Catégories de personnes concernées
Les catégories de personnes concernées par le traitement

- Clients
- Partenaires de service d'ista (releveurs de compteurs, installateurs)
- Employés
- Fournisseurs
- Interlocuteur
- Locataires, propriétaires d'appartements

4. Mesures technico-organisationnelles

(1) Nous mettons en œuvre les mesures techniques et organisationnelles spécifiées à l'annexe 1. Les mesures documentées constituent la base de la déclaration d'engagement. Si un examen / un audit de votre part révèle un besoin d'ajustement, celui-ci doit être mis en œuvre d'un commun accord.

2) Nous devons établir la sécurité conformément à l'article 28, alinéa 3, lettre c), et à l'article 32 du RGPD, en particulier en liaison avec l'article 5, alinéas 1 et 2 du RGPD. Dans l'ensemble, les mesures à prendre sont des mesures de sécurité des données et des mesures visant à assurer un niveau de protection de la confidentialité, de l'intégrité, de la disponibilité et de la résilience des systèmes proportionnel au risque. Pour ce faire, il faut tenir compte de l'état de la technique, des coûts de mise en œuvre et de la nature, de la portée et des finalités du traitement, ainsi que de la probabilité variable d'occurrence et de la gravité du risque pour les droits et libertés des personnes physiques au sens de l'article 32, alinéa 1, du RGPD (détails à l'annexe 1).

(3) Les mesures techniques et organisationnelles sont soumises au progrès technique et au développement ultérieur. À cet égard, nous sommes autorisés à mettre en œuvre d'autres mesures alternatives adéquates. Ce faisant, le niveau de sécurité ne doit pas être inférieur au niveau de sécurité des mesures définies. Les changements significatifs doivent être documentés.

4. Correction, limitation et suppression des données

(1) Nous ne pouvons pas de notre propre gré corriger, supprimer ou restreindre le traitement des données que nous traitons en votre nom, mais seulement après avoir reçu des instructions documentées de votre part. Si une personne concernée nous contacte directement à ce sujet, nous vous transmettrons cette demande sans délai.

(2) Dans la mesure où l'étendue des services l'inclut, nous devons pouvoir assurer immédiatement par nos moyens le concept de suppression, le droit d'être oublié, la correction, la portabilité des données et l'information selon vos instructions documentées.

5. L'assurance qualité et les autres obligations d'ista Luxembourg S.à r.l. en tant que mandataire

Outre le respect des dispositions de la présente déclaration d'engagement, nous avons d'autres obligations légales en vertu des articles 28 à 33 du RGPD ; à cet égard, nous garantissons notamment le respect des exigences suivantes :
a) Nomination écrite d'un délégué à la protection des données qui exerce ses fonctions conformément aux articles 38 et 39 du RGPD.

Coordonnées pour un contact direct :

ista Luxembourg S.à r.l.
Délégué à la protection des données
23, rue des Bruyères
1274 Howald
Courrier électronique : GDPR_DPO@ista.lu

Déclaration d'engagement d'ista Luxembourg S.à r.l. sur le traitement des commandes.

b) Garantie de la confidentialité conformément à l'article 28, alinéa 3, phrase 2, lettre b), à l'article 29 et à l'article 32, alinéa 4 RGPD. Nous n'employons dans l'exécution de ce travail que des employés qui sont tenus à la confidentialité et qui ont été préalablement familiarisés avec la réglementation relative à la protection des données les concernant. Nous et toute personne sous notre autorité qui ait accès à des données à caractère personnel ne pouvons traiter les données que conformément à vos instructions, qui s'appliquent également aux pouvoirs accordés dans le cadre de la présente déclaration d'engagement, à moins que la loi ne nous oblige à traiter ces données.

c) Mise en œuvre et respect de toutes les mesures techniques et organisationnelles requises pour la présente déclaration d'engagement conformément à l'art. 28, al. 3, phrase 2, let. c, et à l'art. 32 du RGPD (détails dans l'annexe 1)

d) Vous et nous coopérerons avec l'autorité de contrôle sur demande dans l'exercice de vos missions.

e) Votre information immédiate sur les actions et mesures de contrôle prises par l'autorité de contrôle, dans la mesure où elle concerne cette déclaration d'engagement. Cela s'applique également si une autorité compétente enquête dans le cadre d'une infraction administrative ou d'une procédure pénale concernant le traitement de données à caractère personnel en rapport avec le traitement de commandes chez nous.

f) Si vous faites l'objet d'une inspection de l'autorité de contrôle, d'une infraction administrative ou d'une procédure pénale, d'une action en responsabilité d'une personne concernée ou d'un tiers ou de toute autre action en rapport avec le traitement de votre commande chez nous, nous devons vous soutenir dans chaque cas.

g) Nous contrôlons régulièrement les processus internes ainsi que les mesures techniques et organisationnelles afin de nous assurer que le traitement dans notre domaine de compétence soit effectué conformément aux exigences de la loi applicable en matière de protection des données et que la protection des droits de la personne concernée soit garantie.

h) Vérifiabilité des mesures techniques et organisationnelles prises à votre égard dans le cadre de vos pouvoirs de contrôle conformément à la clause 7 de la présente déclaration d'engagement.

6. Sous-traitance

(1) Aux fins de la présente disposition, on entend par relations de sous-traitance les services qui sont directement liés à la fourniture du service principal. Cela n'inclut pas les services auxiliaires que nous utilisons (par exemple, services de télécommunications, services postaux/transports, services de maintenance et d'utilisation ou élimination des supports de données et autres mesures visant à garantir la confidentialité, la disponibilité, l'intégrité et la résilience du matériel et des logiciels des systèmes de traitement des données).

Toutefois, nous sommes tenus de conclure des accords contractuels appropriés conformément à la loi et de prendre des mesures de contrôle pour garantir la protection et la sécurité des données, même dans le cas de services auxiliaires externalisés.

(2) Nous pouvons utiliser des sous-traitants sur la base du consentement écrit généralement donné ici. Nous vous informerons de tout changement prévu concernant l'implication ou le remplacement de ces sous-traitants en mettant à votre disposition la liste actuelle des sous-traitants sur le site av.ista.de. Vous avez la possibilité de vous informer sur la situation actuelle des sous-traitants à tout moment en fonction des circonstances techniques sur le site web susmentionné, ce qui vous donne la possibilité de vous opposer aux changements.

(3) La transmission de vos données à caractère personnel au sous-traitant et sa première action ne sont autorisées qu'après que toutes les conditions requises pour une sous-traitance aient été remplies.

(4) Si le sous-traitant fournit le service convenu en dehors de l'UE / de l'EEE, nous assurerons la recevabilité en vertu de la loi sur la protection des données par des mesures appropriées. Il en va de même lorsqu'il s'agit de recourir à des prestataires de services au sens de l'alinéa 1, phrase 2.

(5) Toute délocalisation / externalisation ultérieure par le sous-traitant nécessite votre consentement explicite (au moins sous forme de texte) ; toutes les obligations en matière de protection des données que nous assumons en vertu de la présente déclaration d'engagement doivent - dans la mesure où elles sont pertinentes pour la relation de sous-traitance - être également imposées au sous-traitant ultérieur.

7. Vos droits de contrôle

(1) Vous avez le droit de vous convaincre du respect du présent accord par des contrôles ponctuels, qui doivent être annoncés au moins quatre semaines à l'avance, de notre respect du présent accord et de nos activités commerciales. Les personnes que vous employez à cette fin doivent s'engager à garder le secret à notre égard. L'obligation de secret doit répondre à des exigences de sécurité élevées. Les personnes employées ne peuvent avoir aucun lien avec l'un de nos concurrents.

(2) Nous veillerons à ce que vous puissiez vous assurer que nos obligations au titre de l'article 28 du RGPD soient respectées. Nous nous engageons à vous fournir les informations nécessaires sur demande et notamment à vous apporter la preuve de la mise en œuvre des mesures techniques et organisationnelles.

(3) La preuve de ces mesures, qui ne concernent pas seulement l'accord de service / de prestation concret, peut être fournie par des certificats, rapports ou extraits de rapport actuels émanant d'organismes indépendants (par exemple, des auditeurs, des bureaux d'audit, des responsables de la protection des données, des départements de sécurité informatique, des auditeurs de la protection des données, des auditeurs de qualité) ou par une certification appropriée dans le cadre d'audits de sécurité informatique ou de protection des données (par exemple, selon l'Office fédéral pour la sécurité en matière de technologies de l'information (BSI)).

Déclaration d'engagement d'ista Luxembourg S.à r.l. sur le traitement des commandes.

8. Rémunération des services liés à la protection des données

Nous sommes autorisés à facturer les services d'assistance, notamment en vertu des articles 7, 10 et 11 d'exiger une rémunération appropriée en fonction des dépenses de temps et de matériel, dans la mesure où celles-ci ne sont pas incluses dans le contrat de prestation et ne sont pas imputables à notre faute et ne consistent pas exclusivement en l'exécution de nos obligations découlant directement du RGPD ou de la législation fédérale en matière de protection des données (BDSG).

Sauf accord contraire avec vous, la rémunération de nos spécialistes est basée sur un taux horaire de 150,00 euros plus la TVA en vigueur. Nous vous facturerons les frais de matériel et de déplacement au montant réel encouru.

9. Notification en cas de violation par nous

Nous vous aidons à respecter les obligations relatives à la sécurité des données à caractère personnel énoncées aux articles 32 à 36 du RGPD ainsi que les obligations de notification en cas de violation des données, les évaluations d'impact sur la protection des données et les consultations préalables. Il s'agit notamment de :

a) assurer un niveau de protection adéquat par des mesures techniques et organisationnelles qui tiennent compte des circonstances et des finalités du traitement ainsi que de la probabilité et de la gravité prévues d'une éventuelle violation de la sécurité et permettent la détection immédiate des violations pertinentes.

b) l'obligation de vous signaler sans délai les violations de la protection des données à caractère personnel

c) l'obligation de vous assister dans le cadre de votre devoir d'information de la personne concernée et de vous fournir sans délai toutes les informations pertinentes à cet égard

d) notre soutien à l'évaluation de l'impact sur la vie privée

e) notre soutien dans le cadre de vos consultations avec l'autorité de contrôle.

10. Votre pouvoir de donner des instructions

(1) Vous devez nous confirmer immédiatement les instructions verbales (au moins sous forme de texte).

(2) Nous devons vous informer immédiatement si nous pensons qu'une instruction de votre part viole les règles de protection des données. Nous sommes en droit de suspendre l'exécution de l'instruction correspondante jusqu'à ce que vous la confirmiez ou la modifiez.

11. Suppression et restitution des données à caractère personnel

(1) Aucune copie ou duplication des données ne sera faite à votre insu. Sont exclues les copies, dans la mesure où elles sont nécessaires pour remplir le contrat de service et pour assurer un traitement correct des données, ainsi que les données qu'il est obligatoire de conserver en vertu d'une disposition légale.

2) Après l'achèvement des travaux à effectuer par nous sur la base du contrat de service ou plus tôt si vous le demandez - au plus tard à la fin du contrat de service – nous vous remettons tous les documents qui sont entrés en notre possession, les résultats de traitement et d'utilisation générés ainsi que les stocks de données qui sont liés au contrat de service ou, avec votre consentement préalable, nous les détruisons conformément aux réglementations sur la protection des données. Il en va de même pour les matériels de test et les rejets. L'enregistrement de la suppression est fourni sur demande.

(3) Sont exclues des obligations d'effacement et de restitution les données pour lesquelles il existe une obligation de conservation en vertu d'une réglementation légale (par exemple, les documents qui servent de preuve du traitement ordonné et correct des données doivent être conservés par nous au-delà de la fin du contrat conformément aux périodes de conservation respectives).

ista Luxembourg S.à r.l.

06/2018/a

Ista Luxembourg S.à r.l. 23, rue des Bruyères 1274 Howald

Tel. 49 52 52 -45 Billing@ista.lu www.ista.lu

Déclaration d'engagement d'ista Luxembourg S.à r.l. sur le traitement des commandes.

Annexe 1 – Mesures techniques et organisationnelles

1. Confidentialité (article 32, alinéa 1, lettre b), du RGPD)

- Mesures de contrôle d'accès
  - Restriction de l'accès physique des personnes non autorisées aux centres de données et aux serveurs des succursales
  - Contrôle de l'autorisation d'accès aux zones sensibles des centres informatiques par le biais du contrôle des cartes d'identité et de la comparaison avec les listes de personnes autorisée
  - Des mesures de sécurité physiques et organisationnelles (lecteurs de cartes à puce, réception pour l'enregistrement) sont mises en œuvre pour les zones non publiques
  - Les visiteurs du siège de la société reçoivent des badges de visite visibles et ne peuvent entrer dans les zones non publiques que s'ils sont accompagnés
  - Tenue d'un répertoire des clés du siège de l'entreprise
  - Mise en œuvre de mesures de protection contre les intrusions (vidéosurveillance, sécurité des portes, système d'alarme avec service de sécurité)
  - Enregistrement des visites au siège et dans les succursales
- Mesures de contrôle d'accès
  - L'accès aux systèmes n'est possible qu'avec des noms d'utilisateur et des mots de passe individuels
  - L'accès aux systèmes n'est possible que pour un cercle défini de personnes autorisées
  - Les droits d'accès sont attribués selon un processus de validation défini
  - Les connexions des utilisateurs et les heures respectives sont enregistrées
- Mesures de contrôle d'accès
  - Les contrôles d'autorisation se font sur la base d'un concept d'autorisation
  - L'attribution des autorisations est basée sur le principe de « need-to-know » (« besoin de connaître »)
  - Les données personnelles ne peuvent être lues, copiées, modifiées ou supprimées que dans le cadre du concept d'autorisation
  - L'utilisation d'un logiciel de protection contre les virus constamment mis à jour est techniquement assurée
  - Le trafic de courrier électronique entrant est contrôlé par un système central de protection contre les virus et de filtrage de spams
  - Protection de l'infrastructure informatique par des pare-feu
  - Protection par mot de passe (au moins huit caractères, combinaison de lettres, de chiffres et de caractères spéciaux, changement forcé après 90 jours)
  - Une séparation des données de base de la facturation et du client mise en œuvre dans le concept d'autorisation
  - Enregistrement des modifications de données
- Mesures de contrôle de séparation
  - Procédures d'essai et de mise en service des produits logiciels
  - Séparation de l'environnement de production, d'essai et de développement
  - Séparation logique du paysage à trois systèmes selon le concept d'autorisation
  - Gestion du changement avec procédure de libération différenciée
- Mesures de pseudonymisation (article 32, alinéa 1, lettre a) du RGPD ; article 25, alinéa 1 du RGPD)
  - Les données à caractère personnel sont traitées de manière à ce que les données des différents systèmes ne puissent être reliées à une personne concernée spécifique sans informations supplémentaires, lorsque cela est possible et approprié

2. Intégrité (art. 32, alinéa 1, lettre b), du RGPD)

- Mesures de contrôle des transferts
  - Cryptage / utilisation de tunnels VPN pour les transmissions
  - Cryptage SSL pour l'accès au Web
  - Régulation du trafic de communication du système (pare-feu central, connexions WAN exclusives avec contrôles d'accès), journalisation (authentification de l'utilisateur, heure)
- Mesures de contrôle des entrées
  - Contrôles de plausibilité mis en œuvre par le système
  - Il est possible de déterminer ultérieurement si et par qui les données de base des clients ont été saisies, modifiées ou supprimées des systèmes informatique (journalisation)
  - Concept d'autorisation

3. Disponibilité et résilience (art. 32, alinéa 1, lettres b) et c) du RGPD)

- Les données personnelles sont constamment disponibles et protégées contre la destruction ou la perte accidentelle par des sauvegardes régulières
- Concept de sauvegarde des données (sauvegardes régulières : quotidiennes, hebdomadaires, mensuelles), modalités de stockage des sauvegardes (Safe, compartiments coupe-feu séparés)
- Sections du centre de calcul spécialement protégées (séparation structurelle, systèmes de contrôle d'accès séparés, murs de protection contre l'incendie pour toutes les zones du centre de calcul, alimentation électrique via deux connexions géographiquement séparées, deux systèmes d'alerte précoce contre l'incendie séparés avec connexion au centre de contrôle des pompiers)
- Équipements de protection contre l'incendie au siège de l'entreprise et dans les succursales
- Alimentation électrique ininterrompue
- Lignes d'alimentation électrique redondantes
- Systèmes de suivi et de rapport

4. Procédures d'examen, d'appréciation et d'évaluation périodiques (art. 32, al. 1, let. d, du RGPD ; art. 25, al. 1, du RGPD)

- Concept de protection des données / sécurité des données
- Gestion de la réponse aux incidents (Incident-Response-Management)
- Paramètres par défaut favorables à la protection des données (article 25, alinéa 2, du RGPD)
- Contrôle de la commande
- Traitement uniquement selon les instructions documentées du client
- Les instructions sont transmises entre les personnes de contact expressément désignées à cette fin
- Spécifications concrètes pour l'emballage et l'envoi de documents / éléments contenant des données pertinentes
- Les personnes employées sont informées des exigences en matière de protection des données et sont tenues par écrit de respecter la confidentialité conformément aux articles 24, 29 et 32, alinéa 4, du RGPD
- Les sous-traitants sont soigneusement contrôlés quant à leur aptitude à respecter les mesures de sécurité pertinentes et sont tenus par écrit de se conformer aux réglementations applicables en matière de protection des données