Conditions d'applications du
Règlement Général sur la Protection des Données

RGPD

I. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer, pour le compte du responsable de traitement, les opérations de traitement de données à caractère personnel définies ci-après. Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/67 9 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après, « le règlement européen sur la protection des données »).

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

Le sous-traitant est autorisé à traiter, pour le compte du responsable de traitement, les données à caractère personnel nécessaires pour fournir des outils et services de Technology Expense Management. La nature des opérations réalisées sur les données est la collecte de données auprès des fournisseurs de technologies (opérateurs, éditeurs), la collecte de données à partir d'agents sur des appareils mobiles ou non, la collecte d'informations auprès du responsable de traitement ou de ses clients (données RH, données comptables, données techniques…), la conversion de données, la mise en base de données, la réalisation d'analyses, de KPI, de tableaux de bords et de rapports à partir de ces données. La finalité du traitement est la bonne gestion des coûts et des ressources techniques du responsable de traitement ou de ses clients. Les données à caractère personnel traitées sont les suivantes : nom, prénom, titre, email, détails d'appels et de sessions data, consommations de data par application, pays d'utilisation de la data, informations sur les appareils (mobiles, laptops) utilisés. Toutes les catégories de personnes sont concernées. Pour l'exécution du service objet du présent contrat, le responsable de traitement met à la disposition du sous-traitant les informations nécessaires suivantes : accès aux données de facturation des fournisseurs, accès aux données RH et organisationnelles, accès aux détails d'appels opérateurs ou PBX, accès aux détails de consommations des appareils mobiles. Ces données sont hébergées, selon le choix et les instructions du responsable de traitement, soit dans l'Union Européenne, soit en dehors de l'Union Européenne. Les données sont alors localisées dans les datacenters de la région choisie.

III. Durée du contrat

La durée du présent contrat est alignée sur la durée du contrat de service souscrit par le responsable de traitement.

IV. Obligations du sous-traitant vis-à-vis du responsable de traitement

Le sous-traitant s'engage à :

1. Traiter les données uniquement pour la ou les seule (s) finalité (s) qui fait/font l'objet de la sous-traitance.

2. Traiter les données conformément aux instructions documentées du responsable de traitement. Si le sous-traitant considère qu'une instruction constitue une violation du règlement européen sur la protection des données 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 responsable de traitement. En outre, si le sous-traitant 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 responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

3. Garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat.

4. Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent contrat :

   (i) s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité,
   (ii) reçoivent la formation nécessaire en matière de protection des données à caractère personnel.

5. 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.

V. Sous-traitance

Le sous-traitant est autorisé à faire appel aux l'entités AWS (hébergement), Azure (hébergement), NTT Europe (hébergement), Oracle (maintenance base de données), StoreData (maintenance baie de stockage), Zendesk (stockage de tickets de support) (ci-après, le « sous-traitant ultérieur ») pour mener les activités de traitement décrites entre parenthèses. En cas de recrutement d'autres sous-traitants ultérieurs : Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial 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 européen sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

VI. Droit d'information des personnes concernées

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

VII. Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement à s'acquitter de son obligation de donner 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). Le sous-traitant doit répondre, au nom et pour le compte du responsable de traitement et dans les délais prévus par le règlement européen sur la protection des données, aux demandes des personnes concernées en cas d'exercice de leurs droits, s'agissant des données faisant l'objet de la sous-traitance prévue par le présent contrat.

VIII. Notification des violations de données à caractère personnel

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans un délai maximum de 72 heures après en avoir pris connaissance et par email. Cette notification est accompagnée de toute la documentation utile permettant au responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente. Après accord du responsable de traitement, le sous-traitant notifie à l'autorité de contrôle compétente, au nom et pour le compte du responsable de traitement, les violations de données à caractère personnel dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. La notification contient au moins :

(i) la description de la nature de la violation de données à caractère personnel 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 à caractère personnel 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 à caractère personnel ;

(iv) la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère

personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives. S'il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

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

Le sous-traitant aide le responsable de traitement pour la réalisation d'analyses d'impact relatives à la protection des données. Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

X. Mesures de sécurité

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité suivantes :

(i) Chiffrage des données lors de la collecte et le transfert vers les serveurs du sous-traitant, données confinées dans l'application « agent » sur les appareils mobile,

(ii) Restriction des accès aux données via l'interface homme-machine réalisée sur la base d'une authentification par email/mot de passe des utilisateurs et sur une gestion des droits d'accès au niveau applicatif, masquage de données personnelles dans l'application, accès aux données restreint aux équipes de support et de maintenance des logiciels, restriction de l'accès aux environnements et données de production s'appuyant sur la gestion des accès physiques et logiques de l'hébergeur et sur la sécurisation des accès aux serveurs,

(ii bis) Architecture redondée pour garantir la disponibilité des services, sauvegarde incrémentale journalière et sauvegarde hebdomadaire complète pour limiter les pertes de données en cas d'incident majeur, tests fonctionnels et techniques pour chaque release majeure du logiciel, supervision applicative et système, gestion centralisée des logs d'accès et des logs applicatifs,

(ii ter) Signature par chaque salarié d'un engagement de confidentialité (avenant au contrat),

(iii) Plan de continuité d'activité pour pallier à un incident majeur de l'hébergeur, hébergement de type Paas (Plateform As A Service) pour mettre en œuvre rapidement de nouveaux serveurs,

(iv) Suivi trimestriel interne du Plan d'Assurance Sécurité.

Dans le cas où le responsable de traitement fournit des données personnelles au sous-traitant sous forme de fichier, le responsable de traitement est responsable de crypter ces données selon la méthode définie avec le sous-traitant.

Le responsable de traitement est responsable de l'exactitude des données fournies par fichier ou saisies dans l'IHM par les administrateurs du responsable de traitement.

Pour la fonctionnalité de diffusion des rapports, le responsable de traitement est responsable de la diffusion des rapports contenant des données à caractère personnel via des emails vers des contacts non utilisateurs des logiciels du sous-traitant.

Dans le cas où le responsable de traitement choisit une authentification sur la base de son système SSO, le Client est responsable de l'authentification des utilisateurs gérés par sa solution et de la sécurité de cette solution.

XI. Sort des données

Au terme de la prestation de services relative au traitement de ces données, le sous-traitant s'engage à détruire ou anonymiser toutes les données à caractère personnel dans un délai maximum de 12 mois. Une fois détruites ou anonymisées, le sous-traitant doit justifier par écrit de la destruction ou l'anonymisation.

XII. Délégué à la protection des données

Le sous-traitant communique au responsable de traitement le nom et les coordonnées de son délégué à la protection des données (DPO), s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données.

XIII. Registre des catégories d'activités de traitement

Le sous-traitant déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement comprenant :

(i) le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;

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

(iii) 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 ;

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

(a) de la pseudonymisation et du chiffrement des données à caractère personnel ;

(b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

(c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

(d) d'une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

XIV. Documentation

Le sous-traitant met à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

XV. Obligations du responsable de traitement vis-à-vis du sous-traitant

Le responsable de traitement s'engage à :

1. Fournir au sous-traitant les données visées à l'article II des présentes clauses
2. Documenter par écrit toute instruction concernant le traitement des données par le sous-traitant
3. Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du sous-traitant
4. Superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant