dolomède

Nantes, le 20 avril 2018

Annexe aux Conditions Générales
concernant la protection des données personnelles

Avenant Contrat n° 2016-LDA-2

Entre la société XXX, 75008 Paris, dénommée ici le « le CLIENT responsable de traitement», représentée par Mr XXXx, et DOLOMEDE SARL, représentée par Christine Michas, dénommée ici « le sous-traitant », avenant au contrat 2016-LDA-2 du 7/12/2016, il est convenu ce qui suit :

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 CLIENT 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) 2016/679 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 CLIENT responsable de traitement, les données à caractère personnel nécessaires pour fournir les services suivants :

- l'accès aux outils d'administration de la base données (E-dition , Nouveau Back-Office, accès développeurs et tout autre à venir permettant d'administrer les sites hébergés dans le cadre des conditions particulières du contrat d'hébergement) : données des administrateurs
- l'accès sous condition d'abonnement aux données des sites cités précédemment : données des utilisateurs du site
- le partage des données utilisateurs à des sites externes (import, export ou échanges via API) selon les spécifications du CLIENT

Les opérations réalisées sur les données couvrent un cycle de vie complet d'une donnée : création, modification, suppression et échanges (comme indiqué ci-dessus).
La finalité des traitements est de fournir le meilleur service à l'utilisateur en fonction de son profil, de ses commandes et de ses desiderata.
Les données à caractère personnel traitées pour les sites hébergés sont le nom, le prénom, les adresses nécessaires à la facturation et la livraison, ses caractéristiques professionnelles, ses données d'authentification, son email de contact, ses abonnements.
Les catégories de personnes concernées sont les utilisateurs des sites du CLIENT, les administrateurs et éventuels développeurs.

III. Durée du contrat

Le présent contrat entre en vigueur à compter de ce jour et reste valide jusqu'à la fin du

contrat d'hébergement auquel il est annexé.

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

Le sous-traitant s'engage à :

1. traiter les données uniquement pour les seules finalités qui font l'objet de la sous-traitance
2. traiter les données conformément aux instructions documentées du CLIENT 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 :
    - 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
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

6. **Sous-traitance**

   Le sous-traitant peut faire appel à un autre sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. 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 responsable de traitement dispose d'un délai maximum de 78 heures à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu .

7. **Droit d'information des personnes concernées**

   Le sous-traitant, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de données qu'il réalise. La formulation et le format de l'information doit être convenue avec le responsable de traitement avant la collecte de données. L'échange de données déjà collectées par un tiers (via import/export) ne fait pas partie de cette obligation.

8. Exercice des droits d'information des personnes concernées

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).

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique à contact@IXXX.fr.

9. Notification des violations de données à caractère personnel

Après accord du responsable de traitement, le sous-traitant notifie à l'autorité de contrôle compétente (la CNIL), 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 :

- 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 ;
- 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 ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- 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.

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.

Après accord du CLIENT responsable de traitement, le sous-traitant communique, au nom et pour le compte du responsable de traitement, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins :

- 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 ;
- 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 ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- 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.

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

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

11. Mesures de sécurité

Le sous-traitant a mis en place les mesures suivantes dans le cadre de la plate-forme Doloforge sur laquelle les sites sont hébergés :
- redondance des sauvegardes quotidiennes des données du CLIENT
- protection en profondeur de l'accès à la plate-forme
- surveillance 24/7 de la plate-forme et de ses différents composants

Le sous-traitant recommande au CLIENT de compléter la procédure d'authentification de ses utilisateurs en mettant en place des contrôles plus stricts du contenu des mots de passe ou en procédant au chiffrement des mots de passe par exemple. Le sous-traitant pourra conseiller le CLIENT sur les recommandations de la CNIL dans le cadre des opérations de maintenance à réaliser.

12. Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant
s'engage au choix des parties le moment venu :
- à détruire toutes les données à caractère personnel ou
- à renvoyer toutes les données à caractère personnel au responsable de traitement ou
- à renvoyer les données à caractère personnel au sous-traitant désigné par le responsable de traitement

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

13. 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 :
- 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 ;

- les catégories de traitements effectués pour le compte du responsable du traitement ;
- 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, y compris entre autres, selon les besoins :
    - 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 à caractère personnel 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.

14. Documentation

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

V. Obligations du CLIENT responsable de traitement vis-à-vis du sous-traitant

Le CLIENT responsable de traitement s’engage à :

1. fournir au sous-traitant les données visées au 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

Pour Dolomède
Mme MICHAS – Associée Gérante

Pour le CLIENT
XXXX
« lu et approuvé »