Conditions générales d'hébergement de données à caractère personnel dans le cadre du règlement général de protection des données entrant en vigueur le 25 Mai 2018

1. Article 1. Contexte et Objet

Le Client, responsable de traitement, a souscrit à un ou plusieurs services d'hébergement auprès de Coreoz dans le cadre d'un contrat particulier.

Le Client héberge des données à caractère personnel sur les serveurs opérés par Coreoz ce qui donne à Coreoz le statut, conformément à la doctrine de la CNIL, de sous-traitant.

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) 2016/679 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 »).

Il est rappelé que dans le cadre de sa relation commerciale avec le Responsable de Traitement, Coreoz se limite à fournir de l'espace d'hébergement et n'intervient jamais directement sur les données à caractère personnel du client, en ce sens qu'en aucun cas Coreoz ne manipulera les données à caractère personnel du client, en dehors de :

- leur stockage,
- leur sauvegarde,
- du monitoring, de la supervision et de la sécurisation, des composants physiques, des middlewares et du système d'exploitation mis à disposition du client.

En sa qualité d'hébergeur, Coreoz n'a pas d'obligation générale de surveillance du contenu qu'il héberge et ignore donc si ses clients hébergent des données à caractère personnel sur ses services.

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

Le sous-traitant est autorisé à héberger et, sous réserve de la souscription à ce service, la sauvegarde, pour le compte du responsable de traitement, les données à caractère personnel qu'il a déclaré dans le cadre du formulaire de déclaration.

La nature des opérations réalisées sur les données est :

- l'hébergement des données
- le monitoring des composants physiques, des middlewares et du système d'exploitation,
- la maintenance des middlewares et du système d'exploitation,
- la sécurisation des middlewares et du système d'exploitation,
- et la sauvegarde des données.

La ou les finalité(s) du traitement est ignorée par le Sous-Traitant, conformément à l'article 6-1-2 de la loi n°2004-575 du 21 juin 2004. Le Responsable du Traitement peut toutefois, sous réserve de la mise en place d'un service distinct, porter à la connaissance les données à caractère personnel qu'il héberge sur les serveurs de Coreoz.

Les données à caractère personnel traitées sont ignorées par le Sous-Traitant, conformément à l'article 6-1-2 de la loi n°2004-575 du 21 juin 2004. Le Responsable du Traitement peut toutefois, sous réserve de la mise en place d'un service distinct, porter à la connaissance les données à caractère personnel qu'il héberge sur les serveurs de Coreoz.

Les catégories de personnes concernées sont ignorées par le Sous-Traitant, conformément à l'article 6-1-2 de la loin°2004-575 du 21 juin 2004. Le Responsable du Traitement peut toutefois, sous réserve de la mise en place d'un service distinct, porter à la connaissance les données à caractère personnel qu'il héberge sur les serveurs de Coreoz.

3. Article 3. Durée du contrat

Les présentes conditions générales d'hébergement de données à caractère personnel entrent en vigueur à compter du 25 mai 2018.

4. Article 4. Obligations du sous-traitant vis-à-vis du responsable de traitement

Le sous-traitant s'engage à :

1. Traiter les données uniquement pour la seule finalité qui fait/font l'objet de la sous-traitance, à savoir héberger les données étant entendu que le sous-traitant n'effectue aucune action sur les données à caractère personnel du responsable du traitement en dehors de leur hébergement sur ses serveurs, qu'il s'agisse des serveurs de production et/ ou des serveurs de sauvegarde.

2. traiter les données conformément aux services souscrits par le Client. 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 (dans la mesure où le Responsable du Traitement ne rend pas son hébergement accessible à des tiers non autorisé et veille à ce que les mesures de sécurité permettant la confidentialité soient prises, puisque le client a un total accès sur les données à caractère personnel hébergées par Coreoz)

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.

5. Article 5. Sous-traitance

1. Cadre général de la 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 15 jours 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.

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 sorte 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.

2. Cadre particulier de la sous-traitance « hardware »

Le sous-traitant fait appel à un autre sous-traitant (ci-après, « le sous-traitant ultérieur ») pour effectuer l'hébergement physique des machines.

Le sous-traitant ultérieur héberge physiquement les données du Client.

La raison sociale et les conditions générales RGPD du sous-traitant ultérieur sont précisées dans le contrat particulier conclu avec le Client.

6. Article 6. 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.

7. Article 7. 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).

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 l'adresse indiqué par le Client au moment de la souscription aux services.

8. Article 8. Notification des violations de données à caractère personnel

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance et par email à l'adresse indiquée par le client au moment de la souscription des services.

Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

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.

Le responsable du traitement assume la communication auprès des personnes concernées des violations des données à caractère personnel. Il est rappelé que le sous-traitant n'a pas connaissance des données à caractère personnel qu'il héberge et qu'il n'est donc pas susceptible de déterminer si une violation des données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

9. Article 9. Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations

Le sous-traitant communiquera au responsable de traitement la documentation pertinente pour la réalisation d'analyses d'impact relative à la protection des données par ce dernier, s'agissant uniquement des aspects dont le sous-traitant à la charge, c'est-à-dire, pour le sous-traitant, l'hébergement des données.

Le sous-traitant aide dans la mesure du possible et raisonnablement le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle en fournissant la documentation nécessaire.

10. Article 10. Mesures de sécurité

10.1 Principe

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

- Classification et contrôle du patrimoine informationnel :

Désignation des propriétaires de l'information, de la classification de chaque information, des règles de sécurité associées à chaque classe d'information et de l'inventaire.

- Sécurité du personnel :

Coreoz a élaboré un plan de sensibilisation à la sécurité, destiné à l'ensemble des collaborateurs et adapté à la fonction de chacun.

Par ailleurs, l'équipe sécurité de Coreoz sensibilise l'ensemble du personnel afin que chacun prenne conscience de sa responsabilité dans le processus d'amélioration de la sécurité.

- La politique de sécurité logique de Coreoz est fondée sur un ensemble de principes fondamentaux appliqués au sein de nos prestations. Ces principes étant :
    - Tout ce qui n'est pas explicitement autorisé est interdit,
    - Il n'y a jamais de connexion directe entre le(les) réseau(x) protégés et interne (firewall),
    - Les équipements connectés sur le réseau interne sont « invisibles » d'internet,
    - Les communications privées entre les différents sites à travers un réseau externe (ie. non géré par Coreoz) sont protégées (par exemple via un VPN ou SSH),

10.2 Cadre général

10.2.1 Coreoz s'engage à adopter des Mesures de Sécurité conformes aux dispositions de la Réglementation relative à la Protection des Données et au présente conditions générales RGPD.

10.2.2 Plus particulièrement, Coreoz, compte tenu de la situation actuelle, des coûts de mise en œuvre, et de la nature, de l'objet, du contexte et des finalités du Traitement des Données à Caractère Personnel, ainsi que du risque que le Traitement présente pour les droits et libertés des personnes physiques et de la probabilité et de la gravité de ce risque, s'engage à mettre en œuvre des mesures techniques et opérationnelles adéquates afin de garantir un niveau de sécurité approprié au risque lié au Traitement des Données à Caractère Personnel, y compris, le cas échéant, les mesures prévues à l'article 32, paragraphe 1, du RGPD. Dans tous les cas, Coreoz s'engage :

a) à adopter, à titre d'exigence minimum, l'ensemble des mesures techniques et organisationnelles imposées par la Réglementation relative à la Protection des Données ;

b) à conserver les Données à Caractère Personnel séparément des autres données traitées pour son compte ou celui de tiers, uniquement dans les lieux indiqués par le Client ; et

c) à envoyer à la demande du Client des informations relatives notamment aux mesures physiques, organisationnelles et techniques adoptées pour le Traitement des Données à Caractère Personnel par Coreoz et ses sous-traitants ultérieurs éventuels, ainsi que toute autre information complémentaire éventuellement demandée par le Client en relation avec les mesures physiques, techniques et organisationnelles mises en œuvre en lien avec le Traitement des Données à Caractère Personnel.

10.3 Il est rappelé que dans le cadre de la prestation d'hébergement, le responsable du traitement décide lui-même de la politique de sécurité à laquelle il souscrit et qui peut être plus ou moins étendue selon les options choisies. Les mesures de Coreoz ne se substituent pas aux mesures de sécurité que doit prendre le responsable de traitement pour les traitements de données à caractère personnel afin de s'assurer de la conformité de ses traitements au RGPD.

11. Article 11. Sort des données à l'issue de la relation commerciale

Le sort des données à la fin de la relation contractuelle entre Coreoz et le Client est précisé dans le contrat particulier conclu avec le Client.

12. Article 12. Délégué à la protection des données

Les coordonnées du DPO sont accessibles sur le site internet www.coreoz.com et le client peut écrire à l'adresse :

dpo@coreoz.com

13. Article 13. Documentation

Le sous-traitant met à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations, dans la limite du rôle du sous-traitant, à savoir l'hébergement des données du responsable du traitement.

14. Article 14. Obligations du responsable de traitement vis-à-vis du sous-traitant

Le responsable de traitement s'engage à :

1. Documenter par écrit toute instruction concernant le traitement des données par le sous-traitant.
2. 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 ;
3. Superviser le traitement auprès du sous-traitant conformément au Contrat.

15. Article 15. Portée des conditions générales d'échange de données

Les présentes conditions générales d'hébergement de données à caractère personnel dans le cadre du Règlement général de protection des données entrant en vigueur le 25 mai 2018 et le contrat particulier conclu avec le Client forment un document contractuel unique.

Toutes les stipulations au contrat particulier auxquelles les présentes Conditions Générales d'hébergement de données à caractère personnel ne déroge pas ou non contradictoires avec les termes des Conditions Générales d'hébergement de données à caractère personnel demeurent pleinement applicables entre les parties.

Si l'une des stipulations des conditions générales d'hébergement de données à caractère personnel s'avérait nulle, au regard d'une règle de droit en vigueur ou d'une décision judiciaire devenue définitive, elle serait réputée non écrite, sans pour autant entraîner la nullité des présentes conditions générales d'hébergement de données à caractère personnel ni altérer la validité de ses autres dispositions.