contrat pour traitement de données personnelles

**Entre :** *<Nom organisation>* ayant son siège social à *<adresse organisation>*, ici valablement représentée par *<nom représentant>*.

Ci-après dénommée « *<nom organisation en abrégé> »*, soit *le responsable du traitement*.

**et :** <Nom organisation>, ayant son siège à *<adresse organisation>*, ici valablement représentée par *<nom représentant>*.

Ci-après dénommée « *<nom organisation en abrégé> »,* soit *le sous-traitant*.

**Considérant que :**

Le responsable du traitement dispose de données à caractère personnel;

Le responsable du traitement confie en partie le traitement de ces données personnelles au sous-traitant, et que les parties sont dans ce cadre déjà liées par une convention (« la convention sous-jacente ») ;

Que, dans le contexte du règlement général sur la protection des données (RGPD), la relation doit faire l’objet d’un écrit comme indiqué à l'art. 28 RGPD;

# Article 1 – Objet du contrat (art. 28, alinéa 3, a RGPD)

Le sous-traitant agit exclusivement pour le compte du responsable du traitement et ne consultera ni ne traitera des données à caractère personnel que si, et dans la mesure où, cela est indispensable pour l’exécution du contrat, ceci sur base des instructions documentées du responsable du traitement.

Conformément à ces instructions et aux dispositions de la présente convention, le sous-traitant ne traitera pour le compte du responsable du traitement que des données à caractère personnel aux fins déterminées par le responsable du traitement :

# (…)

# Article 2 : Données à caractère personnel et catégories de personnes concernées

Le sous-traitant traite les données à caractère personnel suivantes des catégories de personnes concernées suivantes :

# (…)

# Article 3 : Confidentialité

Le sous-traitant est tenu de garantir la confidentialité des données à caractère personnel qu’il reçoit du responsable du traitement. Une exception à cette règle n’est possible que lorsqu’une disposition légale ou une injonction l’oblige à les communiquer ou lorsque le transfert de données se fait sur instruction du responsable du traitement.

Toute communication requise légalement de données à caractère personnel doit être préalablement notifiée par le sous-traitant au responsable du traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

La confidentialité reste de mise après le transfert ou l’expiration de la présente convention.

# Article 4 : Utilisation d’autres sous-traitants (art. 28 alinéa 4 RGPD)

Pour l’exécution pratique de la mission, le sous-traitant peut conclure des contrats de sous-traitance avec des tiers.

Le responsable du traitement autorise de façon générale le traitement en sous-traitance de données à caractère personnel par d’autres sous-traitants pour les finalités prévues. Si le sous-traitant sous-traite (partiellement) le traitement de données à caractère personnel au nom du responsable du traitement, le sous-traitant le fait toujours au moyen d’un contrat écrit avec l’autre sous-traitant, imposant à ce dernier des obligations de protection de données identiques ou au moins équivalentes aux obligations qui ont été imposées au sous-traitant-même dans le présent contrat. Si l’autre sous-traitant ne parvient pas à remplir son obligation de protection des données en vertu d’un tel contrat écrit, le sous-traitant restera entièrement responsable vis-à-vis du responsable du traitement pour le respect de ces obligations.

Le sous-traitant tient à jour une liste des contrats de sous-traitance actifs qu’il a conclus avec d’autres sous-traitants et est capable de la fournir au responsable du traitement dans un délai raisonnable sur demande écrite (y compris par e-mail). Le sous-traitant informe de façon structurelle le responsable du traitement en cas de changements dans cette liste.

Le responsable du traitement accepte d’ores et déjà la liste suivante d’autres sous-traitants :

(…)

Le fait que le sous-traitant confie ses engagements en tout ou en partie à des tiers ne le dégage pas de sa responsabilité vis-à-vis du responsable du traitement. Ce dernier ne reconnaît aucune relation contractuelle avec ces tiers.

Toutes les obligations qui sont imposées au sous-traitant le sont également à chacun de ses fournisseurs pour les services qui les concernent. Le sous-traitant imposera en particulier à ses fournisseurs l’obligation de confidentialité qui repose sur lui-même.

# Article 5 : Sécurité (art. 32 RGPD)

Le sous-traitant prend toutes les mesures requises en vertu de l’art. 32 du RGPD. Compte tenu de l'état des connaissances, des coûts de mise en oeuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en oeuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. Lors de l’évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l’altération ou de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d’une autre manière, ou de l’accès non autorisé à de telles données, de manière accidentelle ou illicite.

Les mesures comprennent selon les besoins :

* Des moyens permettant de garantir sur base permanente 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 ;
* La mise en œuvre et l’utilisation de technologies et techniques de sécurisation en conformité avec les meilleures pratiques dans l’industrie (firewall, réseau, anti-malware, politique en matière de mots de passe …) ;
* Pseudonymisation ou cryptage de données à caractère personnel (au moins pour les mots de passe);
* Accords mutuels pour la protection contre les vulnérabilités (patching) ou hacking ;
* L’utilisation de connexions sécurisées et certificats pour sites web et pour le trafic de données (https, SSL, VPN) ;
* La garantie de résilience des applications web contre le top 10 des risques de sécurité repris dans l’OWASP (cross site scripting, SQL injection…) .

# Article 6 : Notification de violation de données

Le sous-traitant s’engage à notifier tout traitement ou accès illicites ou autrement non‑autorisés à des données à caractère personnel ou autres données confidentielles. Le sous-traitant notifie la violation immédiatement, au plus tard dans les 24 heures après la constatation de l’incident. De plus, le sous-traitant prendra toutes les mesures raisonnablement nécessaires pour prévenir ou limiter toute (nouvelle) violation des mesures de sécurité.

Le sous-traitant indiquera au moins et dans la mesure où l'information est déjà disponible, les élément suivants:

* nature de l’incident ;
* date et heure de la constatation ;
* données impactées ;
* mesures directement prises afin de limiter tout dommage supplémentaire ;
* date et heure où l’incident a pris fin ;
* mesures structurelles de prévention pour l’avenir.

Le responsable du traitement notifiera les violations de données soumises à une obligation légale de notification à l’autorité de contrôle compétente dans les délais légaux prévus.

# Article 7 : Aide par rapport aux obligations des art. 32 à 36 RGPD

Le sous-traitant aidera, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant, le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36.

# Article 8 : Sensibilisation et formation du personnel (art. 29)

Le sous-traitant s’engage à informer les personnes ayant accès aux données, conformément au présent contrat, sur les dispositions du Règlement Général sur la Protection des Données. Le sous-traitant garantit que les personnes habilitées au traitement des données à caractère personnel se sont engagées à respecter la confidentialité ou sont liées par une obligation légale adéquate en matière de confidentialité.

Le sous-traitant inclura notamment vis-à-vis de ses employés et de ses collaborateurs indépendants des clauses de confidentialité dans ses contrats de travail, son règlement de travail ou ses contrats de consultance.

# Article 9 : Aide concernant les demandes et les droits des personnes concernées

Le sous-traitant aidera, compte tenu de la nature du traitement, le responsable du traitement par des mesures techniques et organisationnelles appropriées, et dans la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au chapitre III du RGPD.

# Article 10 : Contrôle par le responsable du traitement (art. 28 alinéa 3, h RGPD)

Le responsable du traitement a à tout moment le droit de contrôler le respect de ce contrat. Sur simple demande du responsable, le sous-traitant est tenu de mettre à disposition toutes les informations nécessaires pour démontrer le respect des obligations prévues, de permettre la réalisation d’audits, y compris d’inspections, par le responsable du traitement ou un autre contrôleur qu’il a mandaté, et d’y contribuer.

# Article 11 : Responsabilité

Les parties reconnaissent leur responsabilité et le partage de leur responsabilité envers les personnes concernées, conformément à l'art. 82 RGPD.

La responsabilité entre parties pour fautes contractuelles contre ce contrat de sous-traitance est réglée par les dispositions en matière de responsabilité contenues dans la convention sous-jacente.

# Article 12 : Obligation au terme du traitement de données à caractère personnel (art. 28, alinéa 3, g RGPD)

Les parties conviennent que le sous-traitant doit, au terme de la prestation de services relatifs au traitement de données, renvoyer toutes les données à caractère personnel transmises ainsi que leurs copies au client ou, au choix du client, détruire toutes les données à caractère personnel et déclarer au client que la destruction a eu lieu, à moins que la législation applicable au sous-traitant ne lui interdise de renvoyer ou de détruire en toute sécurité toutes ou partie des données à caractère personnel qui lui ont été transmises. Dans ce cas, le sous-traitant garantit qu’il respectera la confidentialité des données à caractère personnel transmises et qu’il ne les traitera pas activement.

**Article 13 : Durée du contrat**

Le présent contrat entre en vigueur après sa signature par les deux parties. Le contrat est conclu pour la période pendant laquelle la convention sous-jacente est en vigueur. Si cette convention prend fin, le présent contrat prend fin également à l’exception de la clause de confidentialité, qui reste d’application après le transfert ou l’expiration du présent contrat.

Au terme de la prestation des services de traitement, le sous-traitant détruira les données personnelles ou les renverra au responsable du traitement.

Fait à ……………………… le jj/mm/aa en 2 exemplaires.

**Pour le responsable du traitement,** **Pour le sous-traitant,**

Nom : Nom :

Fonction : Fonction :

Signature : Signature :