Convention de sous-traitance

Les soussignés :
- Le client, <XXX>, <adresse>, numéro d'entreprise <numéro d'entreprise>, ici valablement représenté par <représentant>, ci-après dénommé le client (ou le responsable du traitement)
- Le fournisseur, <XXX>, <adresse>, numéro d'entreprise <numéro d'entreprise>, ici valablement représenté par <représentant>, ci-après dénommé le fournisseur (ou sous-traitant)

Considérant que :
Le responsable du traitement (client) dispose de données à caractère personnel dont il souhaite confier le traitement au sous-traitant (fournisseur). La présente convention vise à régler l'exécution et l'organisation de ce traitement par le sous-traitant, et à offrir suffisamment de garanties à l'égard de la protection de la vie privée.

Plus précisément, il s'agit des mesures techniques et organisationnelles – telles que mentionnées à l'art. 32 du Règlement général relatif à la protection des données / General Data Protection Regulation (RGPD/GDPR) – qui ont pour but que le traitement satisfasse aux exigences du règlement et que la protection des droits de la personne concernée soit garantie.

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, 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.

Article 1er : Objet de la convention (art. 28, alinéa 3, a)
Le sous-traitant agit exclusivement pour le compte du responsable du traitement, sur la base d'instructions écrites. Cette disposition est littéralement imposée par l'article 28, alinéa 3 du RGPD. Conformément aux instructions du responsable du traitement et aux dispositions de la présente convention, le sous-traitant traitera uniquement des données à caractère personnel en faveur du responsable du traitement selon les dispositions telles que décrites à l'annexe 1.

Article 2 : Respect du Règlement général sur la protection des données
Les parties s'engagent en principe et expressément à respecter les dispositions du *Règlement européen 2016/979 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*.

Article 3 : Mise à disposition des données
Pour permettre au sous-traitant de traiter les données à caractère personnel, ces données doivent être mises à sa disposition de l'une ou l'autre manière. Seules les données à caractère personnel qui sont strictement nécessaires aux fins décrites à l'article 1er peuvent être traitées par le sous-traitant. Le traitement des données concernées, ainsi que le mode de mise à disposition doivent toujours se dérouler d'une façon sécurisée.

Article 4 : Utilisation des données à caractère personnel (art. 28, alinéas 3, 4)
Les données peuvent uniquement être traitées par le sous-traitant aux fins décrites à l'annexe 1 de la présente convention. Cela implique l'obligation de principe de n'utiliser les données qu'en interne. La communication des données à des tiers, d'une quelconque façon (au moyen d'une transmission, d'une diffusion ou d'une quelconque autre manière) est interdite, sauf si cela est imposé par ou en

vertu d'une loi. Le fait de faire appel à des sous-traitants constitue aussi une communication à des tiers. Le sous-traitant doit signaler au responsable du traitement, si possible à l'avance, toute communication légalement obligatoire des données à caractère personnel qui font l'objet de la présente convention.

Il est interdit au sous-traitant de faire une copie des données mises à disposition, sauf en vue d'un back-up, si cela est nécessaire dans l'exécution de la mission telle que décrite dans la présente convention. Le sous-traitant ne conservera les données qu'aussi longtemps que cela est nécessaire pour la prestation du service pour lequel elles sont mises à disposition. Si les données ne sont plus nécessaires après cela, le sous-traitant les détruira ou les restituera au responsable du traitement.

Article 5 : Utilisation de sous-traitants ultérieurs (art. 28 alinéa 4)
Le sous-traitant ne prendra pas d'autre sous-traitant en service sans autorisation écrite préalable, spécifique ou générale, du responsable du traitement. En cas d'autorisation écrite générale, le sous-traitant informera le responsable du traitement au sujet des changements visés en ce qui concerne l'ajout ou le remplacement d'autres sous-traitants, le responsable du traitement se voyant offrir la possibilité de formuler une objection contre ces changements. Il est de la responsabilité du premier sous-traitant de conclure une convention de sous-traitance avec le deuxième (troisième,…) sous-traitant, avec l'obligation d'offrir des garanties suffisantes pour ce qui est de l'application de mesures techniques et organisationnelles adéquates. Lorsque l'autre sous-traitant ne respecte pas ses obligations en matière de protection des données, le premier sous-traitant reste entièrement responsable du respect des obligations de cet autre sous-traitant à l'égard du responsable du traitement.

Article 6 : Sécurisation (art. 32)
Le responsable du traitement et le sous-traitant prennent tous deux des mesures techniques et organisationnelles adéquates pour garantir un niveau de sécurité approprié. Le responsable du traitement veille à ce que le sous-traitant prenne toutes les mesures requises (telles qu'énumérées à l'art. 32 du RGPD). Ces mesures sont décrites à l'annexe 2 de la présente convention.
En particulier, le sous-traitant sécurisera les données à caractère personnel contre la destruction, la perte, l'altération ou 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. Le sous-traitant informera toujours le responsable du traitement au sujet des mesures techniques et organisationnelles qu'il a mises à exécution pour sécuriser les données à caractère personnel contre la destruction, la perte, la falsification et la diffusion non autorisée, ainsi que contre l'accès non autorisé.

Article 7 : Limitation physique d'accès
Le sous-traitant veillera à ce que les endroits où des données à caractère personnel sont traitées au bénéfice du responsable du traitement, ne soient pas accessibles pour les personnes non compétentes. À cette fin, il prendra, entre autres, les mesures organisationnelles nécessaires.

Article 8 : Limitation fonctionnelle d'accès
Le sous-traitant limitera l'accès aux données à caractère personnel traitées aux membres du personnel qui ont besoin des données pour exercer les tâches que le sous-traitant leur confie en exécution de la présente convention. À cette fin, le sous-traitant fournira au responsable du traitement une liste des membres du personnel qui sont impliqués dans le traitement en sa faveur de données à caractère personnel.
Si une énumération de tous les membres du personnel est bien trop fastidieuse, on peut opter pour une énumération des services ou divisions.

Article 9 : Information (art. 29)
Le sous-traitant s'engage à informer les personnes qui, conformément à la présente convention, ont accès aux données, au sujet des dispositions du Règlement général relatif à la protection des données. Le sous-traitant garantit que les personnes habilitées à traiter les données à caractère personnel se sont engagées à respecter la confidentialité ou sont tenues par une obligation légale cohérente de confidentialité.

Article 10 : Application du devoir de notification (art. 13)
Si, dans l'exécution de la présente convention, le sous-traitant obtient directement des données à caractère personnel auprès des personnes concernées et qu'il enregistre ces données, il respectera les dispositions de l'article 13 du règlement général relatif à la protection des données et informera les personnes concernées (au moyen d'une politique de la vie privée, par ex.).
Le cas échéant, il est convenu que le sous-traitant soumette préalablement le contenu et le mode de la notification au responsable du traitement.

Article 11 : Contrôle par le responsable du traitement (art. 28 alinéa 3, h)
Le responsable du traitement a le droit, à tout moment, de contrôler le respect de la présente convention. Sur simple demande du responsable, le sous-traitant est tenu, d'une part, de mettre à disposition toutes les informations qui sont nécessaires pour démontrer le respect des obligations établies et pour permettre des audits, dont des inspections, par le responsable du traitement ou par un contrôleur habilité par le responsable du traitement et, d'autre part, de contribuer à ces audits.

Article 12 : Responsabilité (art. 82, alinéa 2)
Le sous-traitant est uniquement et entièrement responsable des dommages qui découlent du non-respect des dispositions de la présente convention et de ses annexes. Si une personne concernée réclame une indemnité du responsable du traitement
en raison d'une violation des dispositions du RGPD par le sous-traitant ou du présent accord , le sous-traitant interviendra dans la procédure, sur simple demande du responsable, afin de protéger le responsable du traitement.

Article 13 : Obligation après la fin du traitement des données à caractère personnel (art. 28, alinéa 3, g)
Les parties conviennent que le sous-traitant restituera au client, après la fin de la prestation de services de traitement des données, toutes les données à caractère personnel transmises et toutes les copies de celles-ci, ou, si le client préfère cette option, il détruira toutes les données à caractère personnel et déclarera au client que la destruction a eu lieu, sauf si la législation applicable au sous-traitant lui interdit de restituer ou de détruire, en toute sécurité, toutes les données à caractère personnel ou une partie de celles-ci. Dans ce cas, le fournisseur garantit qu'il respectera la confidentialité des données à caractère personnel transmises et qu'il ne traitera pas activement les données à caractère personnel transmises.

Fournisseur	Client
Date :	Date :
Lieu :	Lieu :

Annexe 1 : Finalités
Annexe 2 : Description des mesures techniques et organisationnelles telles que décrites à l'art. 32 du RGPD

Convention de sous-traitance – Annexe 1

(ceci est seulement un exemple)

1. **Objet du traitement**
   Le traitement doit permettre au sous-traitant (c.-à-d. l'entreprise de publipostage) d'envoyer des publications de Febelgra (à savoir le magazine mensuel Factua) aux membres de Febelgra.
2. **Durée du traitement :**
   Le sous-traitant peut traiter les données jusqu'à ce que la convention soit résiliée.
3. **Nature et objet du traitement**
   Le sous-traitant ne peut utiliser les données que pour la personnalisation, l'adressage et l'envoi des impressions, à savoir en imprimant des données à caractère personnel sur l'enveloppe et en envoyant celle-ci ensuite.
4. **Type de données à caractère personnel qui sont traitées**
   Les données de contact (nom de société, personne de contact et adresse) des membres de Febelgra.
5. **Catégories de personnes concernées auprès du sous-traitant**
   Les membres Febelgra.

Convention de sous-traitance – Annexe 2

Dispositions de l'art. 32 du RGPD

Compte tenu de l'état des connaissances, des coûts de mise en œuvre 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 œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

Le sous-traitant est tenu de prendre des mesures qui comprennent entre autres ce qui suit :

- la pseudonymisation et le chiffrement des données à caractère personnel
- 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.

À cette fin, le sous-traitant donne ci-dessous une énumération des mesures de sécurité appliquées.

Description des mesures techniques et organisationnelles possibles (il s'agit d'une liste de contrôle -> il incombe au sous-traitant d'indiquer ce qui est d'application ou non, afin de vérifier s'il est pris suffisamment de mesures, ou que le responsable du traitement exige encore des mesures complémentaires) :

1. Mesures techniques

- La présence d'une anonymisation ou pseudonymisation automatique des données à caractère personnel après que l'objectif du traitement (ou des délais de conservation légalement imposés) a été dépassé.

- La présence d'une gestion des utilisateurs convenablement développée. Cela comprend :
    - L'administration doit elle-même pouvoir ajouter/supprimer des utilisateurs internes (sans intervention du fournisseur)
    - La possibilité d'utiliser une authentification multifacteurs (par ex. l'eID)
    - La possibilité d'instituer une politique des mots de passe (les utilisateurs – citoyens choisissent eux-mêmes leurs données de connexion, celles-ci ne sont pas établies dans le back-end)
    - La possibilité de faire une réinitialisation du mot de passe d'un utilisateur
    - Au moins 2 niveaux de droits (un administrateur et des utilisateurs) selon le niveau d'utilisation et de décision

- Un module "audit log" convenablement développé
    - La possibilité de connexion : quel utilisateur a exécuté quelles actions dans le programme (consultation incl.).

- Peut être consultée par le client (l'administration) sans intervention du fournisseur.
- Connexion des interventions exécutées par le fournisseur, pouvant être consultées par le client sans intervention du fournisseur.
- …

- Possibilité d'extraction (exportation) de données / possibilité de back-up.

Par ailleurs, une **application web** doit disposer :

- d'une sécurisation approfondie exécutée sur la base du top 10 des menaces de l'OWASP
  - avec au moins une protection contre une attaque de force brutale (possibilité de bloquer des utilisateurs après x nombre de tentatives de connexion)

- de mises à jour structurelles sur le plan de la sécurité : - Au serveur (système de pilotage, serveur web, antivirus,…)
  - à la base de données
  - à la plateforme utilisée pour l'application web

Un quelconque **transfert** et une quelconque **conservation de données à caractère personnel**, contenus dans l'application, doivent avoir lieu d'une manière **sécurisée**. S'il s'agit d'une application web, les conditions minimales suivantes s'appliquent :

- Les données à caractère personnel sont mises à disposition via une liaison sécurisée (https, VPN, IPSEC, FTPS).
  - Une liaison sécurisée pour les utilisateurs finaux
  - Une liaison sécurisée avec le Registre national

- Les données à caractère personnel sont conservées dans un centre de données européen (de préférence certifié ISO27001)
- Un back-up des données à caractère personnel est aussi transmis via une liaison sécurisée – si d'application par ex. en cas de travail avec un second centre de données – également via une liaison sécurisée. Par ailleurs, la procédure de back-up du fournisseur est documentée.
- Le stockage de données a lieu de façon verrouillée, au moins pour les mots de passe.

2. Mesures organisationnelles

- Le fournisseur dispose d'un consultant en sécurisation.
- Le fournisseur démontre que ses éventuels membres du personnel sont au courant de la politique de sécurité.
- Le fournisseur garantit le client au moyen d'accords que les données à caractère personnel conservées par le fournisseur ne peuvent être consultées que sur demande du client ou après avertissement pour entretien.
- Le fournisseur démontre via une documentation qu'il est en mesure d'informer les clients en cas d'une fuite de données.
- Une déclaration relative à la vie privée donne la transparence nécessaire (principe de la loi relative à la vie privée).
- Le fournisseur garantit dans un SLA des interruptions maximales et un point de contact en cas d'incidents.