

ANNEXE n°1- Protection des données personnelles

1. Objet

La présente annexe a pour objet de définir les conditions dans lesquelles le Sous-traitant s'engage à effectuer pour le compte du Responsable de traitements les opérations de traitement de données personnelles dans le cadre du contrat. Cette annexe constitue les instructions documentées devant être communiquées par le Responsable de traitements au Sous-traitant au sens de la Loi. Ces instructions documentées pourront, le cas échéant, être complétées d'instructions spécifiques en matière de sécurité des données personnelles.

2. Définitions

« **Données Personnelles** » désigne toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « **Personne Concernée** »). Est réputée être une « personne physique identifiable » toute personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

« **Traitement** » désigne toute opération ou tout ensemble d'opérations effectué ou non à l'aide de procédés automatisés et appliqué à des données personnelles, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

3. Description du Traitement faisant l'objet de la sous-traitance

Le Sous-traitant est autorisé pendant toute la durée du contrat à traiter pour le compte du Responsable de traitements les Données Personnelles nécessaires pour fournir les services de la plate-forme d'informations et de services www.hospimedia.fr, désignée ci-après « la Plate-forme », dans le cadre des instructions du Responsable de traitements décrites dans le tableau ci-dessous.

Description du traitement	Le Souscripteur, identifié comme Responsable de traitement, communique à Hospimedia, le Sous-traitant, les données personnelles des membres de son personnel désignés comme utilisateurs et destinataires des services hospimedia.fr, ci-après dénommés "Utilisateurs".
Nature des opérations réalisées sur les Données Personnelles	• La création et la gestion de comptes abonnés • L'envoi par email des éditions quotidiennes et exceptionnelles ou l'envoi d'invitations à des événements dont HOSPIMEDIA est partenaire • L'envoi par email de réponses à des demandes d'informations effectuées directement par l'intermédiaire de formulaires sur le site www.hospimedia.fr • L'optimisation de l'utilisation des services Hospimedia • L'accès au champ commentaire des articles parus sur le site hospimedia.fr • La proposition d'articles et invitations adaptées à la fonction de l'utilisateur • L'accès à nos contenus sans identifications systématiques

	La réalisation de statistiques et de mesures d'audience afin d'optimiser la navigation et l'utilisation des services Hospimedia.
Finalité(s) du traitement	Donner l'accès aux utilisateurs à un service d'informations sur le secteur sanitaire et/ou médico-social.
Durée du traitement	Pour le souscripteur Les données sont conservées durant toute la durée du contrat. A l'issue de cette durée, ces données feront l'objet d'un archivage à des fins comptables et probatoires pendant 10 ans et seront détruites si lesdits délais ont expiré. Pour les utilisateurs Les données sont conservées durant toute la durée du contrat. Toutes les données seront supprimées ou anonymisées pour les données de consultation 12 mois après la date de fin contractuelle de l'abonnement de la structure à Hospimedia, sous réserve que tout litige contentieux soit levé.
Données Personnelles	Le souscripteur : - le sexe, - le nom, - le prénom, - la structure (nom de l'établissement ou de l'entreprise) - la fonction, - le téléphone, - l'adresse email L'utilisateur : - le nom, - le prénom, - la fonction, - le téléphone, - l'adresse email
Catégories de personnes concernées	Le souscripteur : la personne qui contractualise un abonnement aux services HOSPIMEDIA pour sa propre utilisation ou au nom de la structure pour laquelle il travaille. L'utilisateur : la personne qui profite de l'abonnement sans en être le souscripteur direct.
Contact du délégué à la protection des données personnelles ou de la personne responsable de la protection des données personnelles chez le Responsable de traitement	Le responsable de traitement s'engage à transmettre à Hospimedia le contact du délégué à la protection des données personnelles ou de la personne responsable de la protection des données personnelles pour son compte.

4. Obligations du Sous-traitant vis-à-vis du Responsable de traitements

Le Sous-traitant garantit au Responsable de traitements le respect des obligations légales et réglementaires lui incombant au titre notamment de la Loi ainsi que le respect de ses obligations au titre de la présente annexe.

Ainsi, le Sous-traitant s'engage à :

1. Traiter les Données Personnelles uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de la sous-traitance visée(s) ci-dessus.
2. Traiter les Données Personnelles conformément aux instructions documentées du Responsable de traitements figurant en article III de la présente Annexe, y compris en ce qui concerne les transferts de Données Personnelles vers un pays tiers ou une organisation internationale. Si le Sous-traitant considère qu'une instruction constitue une violation de la Loi, il en informe immédiatement le Responsable de traitements. En outre, si le Sous-traitant est tenu de procéder à un transfert de Données Personnelles vers un pays tiers ou à une organisation internationale en vertu d'une disposition impérative du droit de l'Union Européenne ou du droit de l'Etat membre auquel il est soumis, il doit informer le Client de cette obligation juridique avant le Traitement des Données Personnelles, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.
3. Garantir la confidentialité des Données Personnelles traitées. Ainsi, le Sous-traitant prendra toute mesure permettant d'empêcher toute utilisation détournée, malveillante ou frauduleuse des Données personnelles.
4. A S'interdire de :
 - Traiter et/ou consulter les Données Personnelles à d'autres fins que l'exécution des services qu'il effectue pour le Responsable de traitements au titre du contrat (même si l'accès à ces données est techniquement possible) ;
 - De divulguer, sous quelque forme que ce soit, tout ou partie des Données Personnelles ;
 - De prendre copie ou stocker, quelles qu'en soient la forme et la finalité, tout ou partie des informations ou Données Personnelles contenues sur les supports ou documents qui lui ont été confiés ou qu'il a recueillis en cours d'exécution du contrat, en dehors des cas couverts ;
5. Veiller à ce que les personnes autorisées à traiter les Données personnelles en vertu du 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 Personnelles.
6. Prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des Données Personnelles dès la conception et de protection des Données Personnelles par défaut.
7. 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 tous les cas, le Sous-traitant informe préalablement et par écrit le Responsable de traitements de tout changement envisagé concernant l'ajout ou le remplacement d'autres Sous-Traitants Ultérieurs. Cette information doit indiquer clairement les activités de Traitement sous-traitées, l'identité et les coordonnées du Sous-Traitant Ultérieur et les dates du contrat de sous-traitance. Le Responsable de traitements dispose d'un délai de 30 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 traitements n'a pas émis d'objection pendant le délai convenu.
Le Sous-traitant s'engage à imposer au Sous-Traitant Ultérieur les obligations du contrat et

de la présente annexe. Il appartient au Sous-traitant de s'assurer que le Sous-Traitant Ulérieur présente des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le Traitement réponde aux exigences de la Loi. Si le Sous-Traitant Ulérieur ne remplit pas ses obligations en matière de protection des Données Personnelles, le Sous-traitant demeure pleinement responsable devant le Responsable de traitements de l'exécution par le Sous-Traitant Ulérieur de ses obligations.

8. Droit d'information des Personnes Concernées

Il appartient au Responsable de traitements de fournir l'information (conforme aux exigences de la Loi) aux Personnes Concernées par les opérations de Traitement au moment de la collecte de leurs Données Personnelles.

9. Exercice des droits des Personnes Concernées

Dans la mesure du possible, le Sous-traitant doit aider le Responsable de traitements à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des Personnes Concernées et notamment les droits suivants : 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 au Responsable de traitements dès réception par courrier électronique à l'adresse électronique convenue entre les Parties. Le Sous-traitant ne pourra répondre à la demande d'une Personne Concernée que sur instruction du Responsable de traitements.

10. Notification des Violations de Données Personnelles

Le Sous-traitant notifie au Responsable de traitements dans un délai maximum de 48 heures après en avoir pris connaissance toute violation de Données Personnelles, soit toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données personnelles transmises, traitées ou conservées de façon non conforme aux instructions du Responsable de traitements et à la Loi, ou l'accès non autorisé à de telles Données Personnelles (ci-après la « **Violation** ») et par le moyen de notification convenu entre les Parties.

Le Sous-traitant communique dans le même temps ou par la suite (mais en tout état de cause promptement) toute documentation utile afin de permettre au Responsable de traitements, si nécessaire, de notifier cette Violation à l'autorité de contrôle compétente (ci-après la « **CNIL** »).

Par dérogation à ce qui précède, le Responsable de traitements peut autoriser le Sous-traitant à notifier à la CNIL, au nom et pour le compte du Responsable de traitements, les Violations de Données Personnelles dans les meilleurs délais et en tout état de cause dans un délai de 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.

Dans tous les cas, la notification contient au moins :

- La description de la nature de la Violation de Données Personnelles y compris, si possible, les catégories et le nombre approximatif de Personnes Concernées par la Violation, les catégories et le nombre approximatif d'enregistrements de Données Personnelles 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 Personnelles ;
- La description des mesures prises ou que le Responsable de traitements propose de prendre pour remédier à la Violation de Données Personnelles, 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.

De même, le Responsable de traitements peut autoriser le Sous-traitant à communiquer, au nom et pour le compte du Responsable de traitements, la Violation de Données Personnelles 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 Personnelles et contient au moins :

- La description de la nature de la Violation de Données Personnelles 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 Personnelles 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 personnelles ;
- La description des mesures prises ou que le Responsable de traitements propose de prendre pour remédier à la Violation de Données Personnelles, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

11. Aide du Sous-traitant dans le cadre du respect par le Responsable de traitements de ses obligations.

Le Sous-traitant aide le Responsable de traitements à respecter les obligations pesant sur lui au regard de la Loi, telles que notamment :

- Ses obligations de notification à la CNIL ou de communication à la Personne Concernée d'une Violation de Données Personnelles ;
- Son obligation de consultation préalable de la CNIL visée à l'article 36 du Règlement Européen.

En outre, si le Responsable de traitements décide ou est contraint de réaliser une analyse d'impact relative à la protection des Données Personnelles, le Sous-traitant s'engage à aider le Responsable de traitements pour la réalisation d'une telle analyse.

En cas de contrôle de la CNIL, les Parties s'engagent à coopérer entre elles et avec la CNIL. Plus particulièrement, dans le cas où le contrôle mené chez le Sous-traitant concernerait les Traitements mis en œuvre au nom et pour le compte du Responsable de traitements, le Sous-traitant s'engage à en informer immédiatement le Responsable de traitements et à ne prendre aucun engagement pour lui.

En cas de contrôle de la CNIL chez le Responsable de traitements portant notamment sur les services délivrés par Sous-traitant, ce dernier s'engage à coopérer avec le Responsable de traitements et à lui fournir toute information dont il pourrait avoir besoin ou qui s'avèrerait nécessaire.

12. Mesures de sécurité

Le Sous-traitant s'engage conformément à la Loi, à prendre toutes précautions utiles notamment au regard de la nature des Données Personnelles et des risques présentés par le Traitement, pour préserver la sécurité et la confidentialité des Données Personnelles transmises, traitées ou conservées et empêcher leur déformation, altération, endommagement, destruction de manière fortuite ou illicite, perte, divulgation et/ou tout

accès à ces Données Personnelles par des tiers non autorisés préalablement de manière accidentelle ou illicite.

Le Sous-traitant met en œuvre toutes les mesures techniques et organisationnelles appropriées pour protéger les Données Personnelles, en prenant en compte l'état des connaissances, les coûts de mise en œuvre et la nature, portée, contexte et les finalités du Traitement ainsi que les risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, afin de garantir un niveau de sécurité adapté au risque.

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

- La pseudonymisation et le chiffrement des Données Personnelles ;
- Les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de Traitement ;
- Les moyens permettant de rétablir la disponibilité des Données Personnelles 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.

13. Sort des Données Personnelles

Au terme des services impliquant un Traitement des Données Personnelles ou au plus tard au terme du contrat, le Sous-traitant s'engage, au choix du Responsable de traitements :

- A détruire toutes les Données Personnelles transmises par le Responsable de traitements dans le cadre du contrat ou,
- A renvoyer au Responsable de traitements toutes les Données Personnelles transmises par le Responsable de traitements dans le cadre du contrat ou,
- A renvoyer au Sous-traitant désigné par le Responsable de traitements les Données Personnelles transmises par le Responsable de traitements dans le cadre du contrat.

Par ailleurs, le Sous-traitant s'engage à détruire les copies existantes des Données Personnelles, à l'issue des durées de conservation établies en article III de la présente Annexe.

14. Registre des catégories d'activités de Traitement

Le Sous-traitant s'engage à tenir un registre de toutes les catégories d'activités de Traitement effectuées pour le compte du Responsable de traitements, conformément aux stipulations de l'article 30 du Règlement Européen.

15. Flux transfrontaliers de Données Personnelles

En cas de transfert de Données Personnelles vers un pays tiers, n'appartenant pas à l'Union Européenne, ou ne répondant pas à la certification Privacy Shield, ou vers une organisation internationale, le Sous-traitant devra obtenir l'accord préalable écrit du Responsable de traitements. Si cet accord est donné, le Sous-traitant s'engage à coopérer avec le Responsable de traitements afin d'assurer :

- Le respect des procédures permettant de se conformer à la Loi, par exemple dans le cas où une autorisation de la part de la CNIL apparaîtrait nécessaire ;
- Si besoin, la conclusion d'un ou plusieurs contrats permettant d'encadrer les flux transfrontières de Données Personnelles. Le Sous-traitant s'engage en particulier, si nécessaire, à signer de tels contrats avec le Responsable de traitements et/ou à obtenir la conclusion de tels contrats par ses Sous-Traitants Ultérieurs. Pour ce faire, il est convenu entre les Parties que les clauses contractuelles types publiées par la Commission Européenne seront utilisées pour encadrer les flux transfrontières de Données Personnelles.

16. Documentation

Le Sous-traitant met à la disposition du Responsable de traitements la documentation nécessaire pour démontrer le respect de toutes ses obligations prévues au titre de la présente annexe et de la Loi et pour permettre la réalisation d'audits, y compris des

inspections, par le Responsable de traitements ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

5. Obligations du Responsable de traitements vis-à-vis du Sous-traitant

Le Responsable de traitements s'engage à :

- Fournir au Sous-traitant les Données Personnelles concernées par le contrat ;
- Documenter par écrit toute instruction concernant le Traitement des Données Personnelles par le Sous-traitant ;
- Veiller, au préalable et pendant toute la durée du Traitement, au respect des obligations prévues par la Loi, le présent contrat et la présente annexe de la part du Sous-traitant ;
- Superviser le Traitement, y compris réaliser les audits et les inspections auprès du Sous-traitant.