

Préambule

Les présentes clauses trouvent à s'appliquer pour tout traitement de données à caractère personnel par un sous-traitant pour le compte du responsable du traitement du CHR METZ-THIONVILLE.

On entend par :

- Données à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable directement ou indirectement.

- Traitement : toute opération ou tout ensemble d'opérations effectué à l'aide de procédés automatisés ou non et appliqué à des données ou des ensembles de données à caractère personnel, 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.

- Responsable du traitement : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

- Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Tout partenaire du CHR METZ-THIONVILLE entrant dans le champ d'application des présentes définitions est ainsi amené à se voir appliquer les clauses suivantes. Ceci inclut *de facto* les opérations de maintenance effectuées par des tiers pour le compte du CHR METZ-THIONVILLE, le mainteneur étant amené à réaliser un traitement de données à caractère personnel au sens des précédentes définitions.

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 responsable de traitement les opérations de traitement de données à caractère personnel définies dans le cadre de l'objet principal du contrat.

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 responsable de traitement les données à caractère personnel nécessaires pour fournir le ou les service(s) objets du contrat.

Les opérations réalisées sur les données sont conformes aux stipulations suivantes :

La ou les finalité(s) du traitement, les données à caractère personnel traitées et les catégories de personnes concernées sont conformes à l'objet du contrat.

Pour l'exécution du service objet du présent contrat, le responsable de traitement met à la disposition du sous-traitant les informations nécessaires.

III. Obligations du sous-traitant vis-à-vis du responsable de traitement

Le sous-traitant s'engage à :

1. traiter les données **uniquement pour la ou les seule(s) finalité(s)** qui fait/font l'objet de la sous-traitance
2. traiter les données **conformément aux instructions documentées** du responsable de traitement figurant à l'annexe *Référentiel sécurité système d'information* du présent contrat. 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**

CHR METZ-THIONVILLE

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 conforme à la réglementation de la commande publique ou de 2 mois pour tous les autres types de contrat 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 manière à ce 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.

7. 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.

8. 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 conformément à la loi relative aux droits des malades et à la qualité du système de santé 2002 N°2002-303 4 mars 2002, 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 au responsable de traitement via DPD@chr-metz-thionville.fr.

9. Notification des violations de données à caractère personnel

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans le plus bref délai (maximum 24 heures) après en avoir pris connaissance et par le moyen suivant DPD@chr-metz-thionville.fr. Cette notification

CHR METZ-THIONVILLE

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 et aux personnes concernées.

-Les données à communiquer seront les suivantes :

- 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 responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données.

Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

11. Mesures de sécurité

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité prévues à l'annexe *Référentiel sécurité système d'information* du présent contrat et conformément aux principes de base suivants :

- la pseudonymisation et le chiffrement des données à caractère personnel selon la criticité des données convenue avec le responsable de traitement
- 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 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

Le périmètre de responsabilité du sous-traitant intègre tous les composants et services permettant la réalisation de l'objet du contrat.

CHR METZ-THIONVILLE

Les mesures de sécurité à mettre en œuvre sont décrites à l'annexe *Référentiel sécurité système d'information* du présent contrat applicable au périmètre objet du contrat

12. Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage à :

Respecter les dispositions prévues à l'annexe *Référentiel sécurité système d'information* du présent contrat en conformité avec les réglementations applicables au périmètre de données concernées par le contrat.

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. Délégué à la protection des données

Le sous-traitant communique au responsable de traitement **le nom et les coordonnées de son délégué à la protection des données**, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données.

14. 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 I, 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 :
 - 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;

CHR METZ-THIONVILLE

- 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.

15. Documentation et audit

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

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

Le responsable de traitement s'engage à :

1. Fournir au sous-traitant les données prévues dans le contrat
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

Engagement sur le Règlement Général sur la Protection des Données (RGPD)

CHR METZ-THIONVILLE

ATTESTATION SUR L'HONNEUR RELATIVE AU RESPECT DES OBLIGATIONS INCOMBANT AU SOUS-TRAITANT AU REGARD DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL
--

Je soussigné, représentant dument habilité, du sous-traitant du CHR Metz-Thionville m'engage à respecter les obligations inscrites à l'article 28 du Règlement Général à la Protection des Données (RGPD) et décrites ci-après :

- Prendre les mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et garantisse la protection des droits des personnes ;
- Ne pas sous-traiter tout ou partie des prestations confiées, sans l'autorisation formelle et préalable du CHR Metz-Thionville ;
- Ne traiter que les données régies par le contrat qui nous lie et dans les conditions y afférant ;
- Mettre en place une politique appropriée d'habilitation du personnel intervenant dans le cadre du contrat et veiller à ce que ce personnel s'engage à respecter la confidentialité ;
- Prendre toutes mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté conformément à l'article 32 du RGPD ;
- Permettre la réalisation d'audits y compris des inspections par le CHR Metz-Thionville ou un auditeur qu'il a mandaté et contribuer à ces audits ;
- Supprimer ou renvoyer toutes les données au terme du contrat selon le choix du CHR Metz-Thionville ;
- Notifier au CHR Metz-Thionville toutes violations sur les données traitées dans le cadre du contrat, dans les 4h maximum après en avoir pris connaissance ;
- Tenir un registre de toutes les catégories d'activité de traitement effectuées pour le compte du CHR Metz-Thionville ;
- Tenir à la disposition du CHR Metz-Thionville, sur demande et à tout moment, tous les documents attestant de la mise en place des mesures garantissant le respect des obligations qui vous incombent.

Nom et qualité du signataire

A , le

Signature