|  |  |  |
| --- | --- | --- |
| LOGO_CHRMT | Processus | Référence : PROC/00028 |
| **Clauses Contractuelles types RGPD Client - Prestataire** | Version : 01 |
| Date de publication : 11/07/2022 |
| Date de prochaine révision : 11/07/2026 |

La mise à jour de ce document est garantie sur Intranet – Veillez régulièrement à l’actualisation de vos éditions papier.

Pour toute information sur ce document, merci de contacter les rédacteurs et/ou le service qualité.

# CYCLE DE VIE

|  |  |  |
| --- | --- | --- |
| **Rédacteur(s)** | **Relecteur(s)** | **Valideur(s)** |
| **M. Cyril PIERRÉ**  Ingénieur Sécurité SI | **M. Albert CRUMBACH**  RSSI et DPO | **M. Laurent KARMUSIK**  DSI |
| **11/07/2022 01 Création du document** | | |

# OBJET

Les traitements de données par un sous-traitant doivent respecter le RGPD et être encadrés par un contrat avec le responsable de traitement. Ce contrat peut être totalement ou partiellement fondé sur des clauses contractuelles types (CCT).

# DOMAINE D’APPLICATION

**Que sont des clauses contractuelles types entre responsable de traitement et sous-traitant ?**

Dans le cadre de la relation entre un responsable du traitement (RT) et un ou plusieurs sous-traitants (ST) pour le traitement des données personnelles, l’article 28 du RGPD prévoit une série de dispositions relatives à la mise en place d’un contrat spécifique entre les parties, ainsi que des dispositions obligatoires devant figurer dans ce contrat. Ce dernier peut être fondé, en tout ou en partie, sur des clauses contractuelles types (CCT) qui peuvent être établies par la Commission européenne ou adoptées par une autorité nationale de protection des données.

Le 4 juin 2021, la Commission européenne a publié ses CCT entre les RT et les ST.

**Dans quels cas utiliser les CCT responsable de traitement/sous-traitant ?**

Les CCT permettent d’encadrer la relation entre un RT et son ST en intégrant les dispositions obligatoires de l’article 28 du RGPD.

Elles n’ont pas obligatoirement à être utilisées si le contrat entre un RT et un ST contient tous les éléments visés à l’art. 28 du RGPD devant y figurer. Toutefois, elles fournissent un support utile pour encadrer la sous-traitance conformément aux exigences du RGPD.

**Est-il possible de modifier les CCT ?**

Les CCT de la Commission européenne prévoient que les parties s’engagent à ne pas modifier les clauses, sauf en ce qui concerne l’ajout ou la mise à jour d’informations dans les annexes.

Les parties peuvent toutefois inclure les CCT dans un contrat plus large ou ajouter d’autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les clauses ou qu’elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées.

**Ces clauses contractuelles types permettent-elles de transférer des données en dehors de l’Union européenne ?**

Non, la Commission européenne précise que ses CCT ne peuvent servir aux fins du chapitre V du RGPD. En cas de transfert, il convient d’utiliser les clauses contractuelles types dédiées.

# DEFINITIONS / ABREVIATIONS

* **CCT :** Clauses Contractuelles Types
* **DSI** : Direction du Système d’Information
* **RT**: Responsable du Traitement
* **ST**: Sous-Traitant

# DOCUMENTS ASSOCIES

* **PROC/0649 :** Charte d’utilisation des technologies numériques pour le personnel externe au CHR METZ-THIONVILLE
* **PROC/00024 :** Conformité et prérequis techniques DSI
* **PROC/00025 :** Modèle de Plan d’Assurance Sécurité (PAS)

# REFERENCES

* **RGPD**: Le Règlement Général sur la Protection des données
* [**Site de la CNIL**](https://www.cnil.fr/fr/clauses-contractuelles-types-entre-responsable-de-traitement-et-sous-traitant): Clauses contractuelles types

# DEVELOPPEMENT

Table des matières

[1. Clause 1 - Objet et champ d’application 5](#_Toc256000000)

[2. Clause 2 - Invariabilité des clauses 5](#_Toc256000001)

[3. Clause 3 - Interprétation 5](#_Toc256000002)

[4. Clause 4 - Hiérarchie 5](#_Toc256000003)

[5. Clause 5 - Clause d’amarrage (Facultative) 6](#_Toc256000004)

[6. Clause 6 - Description du ou des traitements 6](#_Toc256000005)

[7. Clause 7 - Obligations des parties 6](#_Toc256000006)

[7.1 Instructions 6](#_Toc256000007)

[7.2 Limitation de la finalité 6](#_Toc256000008)

[7.3 Durée du traitement des données à caractère personnel 6](#_Toc256000009)

[7.4 Sécurité du traitement 6](#_Toc256000010)

[7.5 Données sensibles 7](#_Toc256000011)

[7.6 Documentation et conformité 7](#_Toc256000012)

[7.7 Recours à des sous-traitants ultérieurs 7](#_Toc256000013)

[7.8 Transferts internationaux 8](#_Toc256000014)

[8. Clause 8 - Assistance au Client 8](#_Toc256000015)

[9. Clause 9 - Notification de violations de données à caractère personnel 8](#_Toc256000016)

[9.1 Violation de données en rapport avec des données traitées par le Client 9](#_Toc256000017)

[9.2 Violation de données en rapport avec des données traitées par le Prestataire 9](#_Toc256000018)

[10. Clause 10 - Non-respect des clauses et résiliation 9](#_Toc256000019)

Contrat de PRESTATIONS conclu pour le compte Du CHR METZ-THIONVILLE (RT) par un Sous-traitant (ST)

**ENTRE**

Etablissement **CHR METZ-THIONVILLE**

Adresse Hôpital de Mercy, 1 allée du Château CS 45001

Code postal 57085Ville Metz CEDEX 03

*Ci-après le « Client »*

**ET**

[NOM ET ADRESSE DU SOUS-TRAITANT]

*Ci-après le « Prestataire »*

Ensemble les « Parties »

**ONT CONVENU ENSEMBLE DE CE QUI SUIT :**

**ANNEXE**

**Clauses contractuelles types**

# TITRE I – LES CLAUSES DU CONTRAT

## Clause 1 - Objet et champ d’application

1. a) Les présentes clauses contractuelles types (ci-après les «clauses») ont pour objet de garantir la conformité avec [choisir l’option qui convient] : [OPTION 1] : l’article 28, paragraphes 3 et 4, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données / [OPTION 2]: l’article 29, paragraphes 3 et 4, du règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel par les institutions, organes et organismes de l’Union et à la libre circulation de ces données, et abrogeant le règlement (CE) no 45/2001 et la décision no 1247/2002/CE.
2. b) Les responsables du traitement et les sous-traitants énumérés à l’annexe I ont accepté ces clauses afin de garantir le respect des dispositions de l’article 28, paragraphes 3 et 4, du règlement (UE) 2016/679 et/ou des dispositions de l’article 29, paragraphes 3 et 4, du règlement (UE) 2018/1725.
3. c) Les présentes clauses s’appliquent au traitement des données à caractère personnel tel que décrit à l’annexe II.
4. d) Les annexes I à IV font partie intégrante des clauses.
5. e) Les présentes clauses sont sans préjudice des obligations auxquelles le Client est soumis en vertu du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.
6. f) Les clauses ne suffisent pas à elles seules pour assurer le respect des obligations relatives aux transferts internationaux conformément au chapitre V du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.

## Clause 2 - Invariabilité des clauses

1. a) Les parties s’engagent à ne pas modifier les clauses, sauf en ce qui concerne l’ajout d’informations aux annexes ou la mise à jour des informations qui y figurent.
2. b) Les parties ne sont pour autant pas empêchées d’inclure les clauses contractuelles types définies dans les présentes clauses dans un contrat plus large, ni d’ajouter d’autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les clauses ou qu’elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées.

## Clause 3 - Interprétation

1. a) Lorsque des termes définis respectivement dans le règlement (UE) 2016/679 ou dans le règlement (UE) 2018/1725 figurent dans les clauses, ils s’entendent comme dans le règlement en question.
2. b) Les présentes clauses doivent être lues et interprétées à la lumière des dispositions du règlement (UE) 2016/679 et du règlement (UE) 2018/1725 respectivement.
3. c) Les présentes clauses ne doivent pas être interprétées d’une manière contraire aux droits et obligations prévus par le règlement (UE) 2016/679 / le règlement (UE) 2018/1725 ou d’une manière qui porte atteinte aux libertés ou droits fondamentaux des personnes concernées.

## Clause 4 - Hiérarchie

En cas de contradiction entre les présentes clauses et les dispositions des accords connexes qui existent entre les parties au moment où les présentes clauses sont convenues ou qui sont conclus ultérieurement, les présentes clauses prévaudront.

## Clause 5 - Clause d’amarrage (Facultative)

1. a) Toute entité qui n’est pas partie aux présentes clauses peut, avec l’accord de toutes les parties, y adhérer à tout moment, en qualité soit de responsable du traitement soit de sous-traitant, en complétant les annexes et en signant l’annexe I.
2. b) Une fois que les annexes mentionnées au point a) sont complétées et signées, l’entité adhérente est considérée comme une partie aux présentes clauses et jouit des droits et est soumise aux obligations d’un responsable du traitement ou d’un sous-traitant, conformément à sa désignation à l’annexe I.
3. c) Les présentes clauses ne créent pour la partie adhérente aucun droit ni aucune obligation pour la période précédant l’adhésion.

# TITRE II - OBLIGATIONS DES PARTIES

## Clause 6 - Description du ou des traitements

Les détails des opérations de traitement, et notamment les catégories de données à caractère personnel et les finalités du traitement pour lesquelles les données à caractère personnel sont traitées pour le compte du Client, sont précisés à l’annexe II.

## Clause 7 - Obligations des parties

### 7.1 Instructions

1. a) Le Prestataire ne traite les données à caractère personnel que sur instruction documentée du Client, à moins qu’il ne soit tenu d’y procéder en vertu du droit de l’Union ou du droit de l’État membre auquel il est soumis. Dans ce cas, le Prestataire informe le Client de cette obligation juridique avant le traitement, sauf si la loi le lui interdit pour des motifs importants d’intérêt public. Des instructions peuvent également être données ultérieurement par le Client pendant toute la durée du traitement des données à caractère personnel. Ces instructions doivent toujours être documentées.
2. b) Le Prestataire informe immédiatement le Client si, selon lui, une instruction donnée par le Client constitue une violation du règlement (UE) 2016/679 / du règlement (UE) 2018/1725 ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

### 7.2 Limitation de la finalité

Le Prestataire traite les données à caractère personnel uniquement pour la ou les finalités spécifiques du traitement, telles que définies à l’annexe II, sauf instruction complémentaire du Client.

### 7.3 Durée du traitement des données à caractère personnel

Le traitement par le Prestataire n’a lieu que pendant la durée précisée à l’annexe II.

### 7.4 Sécurité du traitement

1. a) Le Prestataire met au moins en œuvre les mesures techniques et organisationnelles précisées à l’annexe III pour assurer la sécurité des données à caractère personnel. Figure parmi ces mesures la protection des données contre toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel ou l'accès non autorisé à de telles données (violation de données à caractère personnel). Lors de l’évaluation du niveau de sécurité approprié, les parties tiennent dûment compte 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 pour les personnes concernées.
2. b) Le Prestataire n’accorde aux membres de son personnel l’accès aux données à caractère personnel faisant l’objet du traitement que dans la mesure strictement nécessaire à l’exécution, à la gestion et au suivi du contrat. Le Prestataire veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

### 7.5 Données sensibles

Si le traitement porte sur des données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, ou des données relatives aux condamnations pénales et aux infractions («données sensibles»), le Prestataire applique des limitations spécifiques et/ou des garanties supplémentaires.

### 7.6 Documentation et conformité

1. a) Les parties doivent pouvoir démontrer la conformité avec les présentes clauses.
2. b) Le Prestataire traite de manière rapide et adéquate les demandes du Client concernant le traitement des données conformément aux présentes clauses.
3. c) Le Prestataire met à la disposition du Client toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans les présentes clauses et découlant directement du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725. À la demande du Client, le Prestataire permet également la réalisation d’audits des activités de traitement couvertes par les présentes clauses et y contribue, à intervalles raisonnables ou en présence d’indices de non-conformité. Lorsqu’il décide d’un examen ou d’un audit, le Client peut tenir compte des certifications pertinentes en possession du Prestataire.
4. d) Le Client peut décider de procéder lui-même à l’audit ou de mandater un auditeur indépendant. Les audits peuvent également comprendre des inspections dans les locaux ou les installations physiques du Prestataire et sont, le cas échéant, effectués moyennant un préavis raisonnable.
5. e) Les parties mettent à la disposition de l’autorité de contrôle compétente/des autorités de contrôle compétentes, dès que celles-ci en font la demande, les informations énoncées dans la présente clause, y compris les résultats de tout audit.

### 7.7 Recours à des sous-traitants ultérieurs

1. a) OPTION 1 : AUTORISATION SPÉCIFIQUE PRÉALABLE : le Prestataire n’est pas autorisé à sous-traiter à un sous- traitant ultérieur les opérations de traitement qu’il effectue pour le compte du Client en vertu des présentes clauses sans l’autorisation écrite spécifique préalable du Client. Le Prestataire soumet la demande d’autorisation spécifique au moins [PRÉCISER LA DURÉE] avant le recrutement du sous-traitant ultérieur en question, ainsi que les informations nécessaires pour permettre au Client de prendre une décision au sujet de l’autorisation. La liste des sous-traitants ultérieurs autorisés par le Client figure à l’annexe IV, que les parties tiennent à jour.
2. OPTION 2 : AUTORISATION ÉCRITE GÉNÉRALE : le Prestataire dispose de l’autorisation générale du Client pour ce qui est du recrutement de sous-traitants ultérieurs sur la base d’une liste convenue. Le Prestataire informe spécifiquement par écrit le Client de tout projet de modification de cette liste par l’ajout ou le remplacement de sous-traitants ultérieurs au moins [PRÉCISER LA DURÉE] à l’avance, donnant ainsi au Client suffisamment de temps pour pouvoir s’opposer à ces changements avant le recrutement du ou des sous- traitants ultérieurs concernés. Le Prestataire fournit au Client les informations nécessaires pour lui permettre d’exercer son droit d’opposition.
3. b) Lorsque le Prestataire recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du Client), il le fait au moyen d’un contrat qui impose au sous-traitant ultérieur, en substance, les mêmes obligations en matière de protection des données que celles imposées au Prestataire en vertu des présentes clauses. Le Prestataire veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses et du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.
4. c) À la demande du Client, le Prestataire lui fournit une copie de ce contrat conclu avec le sous- traitant ultérieur et de toute modification qui y est apportée ultérieurement. Dans la mesure nécessaire à la protection des secrets d’affaires ou d’autres informations confidentielles, y compris les données à caractère personnel, le sous- traitant peut expurger le texte du contrat avant d’en diffuser une copie.
5. d) Le Prestataire demeure pleinement responsable, à l’égard du Client, de l’exécution des obligations du sous-traitant ultérieur conformément au contrat conclu avec le sous-traitant ultérieur. Le Prestataire informe le Client de tout manquement du sous-traitant ultérieur à ses obligations contractuelles.
6. e) Le Prestataire convient avec le sous-traitant ultérieur d’une clause du tiers bénéficiaire selon laquelle — dans le cas où le Prestataire a matériellement disparu, a cessé d’exister en droit ou est devenu insolvable — le Client a le droit de résilier le contrat conclu avec le sous-traitant ultérieur et de donner instruction au sous-traitant ultérieur d’effacer ou de renvoyer les données à caractère personnel.

### 7.8 Transferts internationaux

1. a) Tout transfert de données vers un pays tiers ou une organisation internationale par le Prestataire n’est effectué que sur la base d’instructions documentées du Client ou afin de satisfaire à une exigence spécifique du droit de l’Union ou du droit de l’État membre à laquelle le Prestataire est soumis et s’effectue conformément au chapitre V du règlement (UE) 2016/679 ou du règlement (UE) 2018/1725.
2. b) Le Client convient que lorsque le Prestataire recrute un sous-traitant ultérieur conformément à la clause 7.7 pour mener des activités de traitement spécifiques (pour le compte du Client) et que ces activités de traitement impliquent un transfert de données à caractère personnel au sens du chapitre V du règlement (UE) 2016/679, le Prestataire et le sous-traitant ultérieur peuvent garantir le respect du chapitre V du règlement (UE) 2016/679 en utilisant les clauses contractuelles types adoptées par la Commission sur la base de l’article 46, paragraphe 2, du règlement (UE) 2016/679, pour autant que les conditions d’utilisation de ces clauses contractuelles types soient remplies.

## Clause 8 - Assistance au Client

1. a) Le Prestataire informe sans délai le Client de toute demande qu’il a reçue de la part de la personne concernée. Il ne donne pas lui-même suite à cette demande, à moins que le Client des données ne l’y ait autorisé.
2. b) Le Prestataire prête assistance au Client pour ce qui est de remplir l’obligation qui lui incombe de répondre aux demandes des personnes concernées d’exercer leurs droits, en tenant compte de la nature du traitement. Dans l’exécution de ses obligations conformément aux points a) et b), le Prestataire se conforme aux instructions du Client.
3. c) Outre l’obligation incombant au Prestataire d’assister le Client en vertu de la clause 8, point b), le Prestataire aide en outre le Client à garantir le respect des obligations suivantes, compte tenu de la nature du traitement et des informations dont dispose le Prestataire :

1) l’obligation de procéder à une évaluation de l’incidence des opérations de traitement envisagées sur la protection des données à caractère personnel (« analyse d’impact relative à la protection des données ») lorsqu’un type de traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques ;

2) l’obligation de consulter l'autorité de contrôle compétente/les autorités de contrôle compétentes préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le Client ne prenait pas de mesures pour atténuer le risque ;

3) l’obligation de veiller à ce que les données à caractère personnel soient exactes et à jour, en informant sans délai le Client si le Prestataire apprend que les données à caractère personnel qu’il traite sont inexactes ou sont devenues obsolètes ;

4) les obligations prévues à [OPTION 1] l’article 32 du règlement (UE) 2016/679 / [OPTION 2] aux articles 33, 36 à 38 du règlement (UE) 2018/1725.

1. d) Les parties définissent à l’annexe III les mesures techniques et organisationnelles appropriées par lesquelles le sous- traitant est tenu de prêter assistance au Client dans l’application de la présente clause, ainsi que la portée et l’étendue de l’assistance requise.

## Clause 9 - Notification de violations de données à caractère personnel

En cas de violation de données à caractère personnel, le Prestataire coopère avec le Client et lui prête assistance aux fins de la mise en conformité avec les obligations qui lui incombent en vertu des articles 33 et 34 du règlement (UE) 2016/679 ou des articles 34 et 35 du règlement (UE) 2018/1725, selon celui qui est applicable, en tenant compte de la nature du traitement et des informations dont dispose le Prestataire.

### 9.1 Violation de données en rapport avec des données traitées par le Client

1. En cas de violation de données à caractère personnel en rapport avec des données traitées par le Client, le Prestataire prête assistance au Client :
2. a) aux fins de la notification de la violation de données à caractère personnel à l’autorité de contrôle compétente/aux autorités de contrôle compétentes, dans les meilleurs délais après que le Client en a eu connaissance, le cas échéant (sauf si la violation de données à caractère personnel est peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques) ;
3. b) aux fins de l’obtention des informations suivantes qui, conformément à [OPTION 1] l’article 33, paragraphe 3, du règlement (UE) 2016/679 / [OPTION 2] l’article 34, paragraphe 3, du règlement (UE) 2018/1725, doivent figurer dans la notification du Client, et inclure, au moins :

1)la nature des 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 ;

2)les conséquences probables de la violation de données à caractère personnel ;

3)les mesures prises ou les mesures que le Client 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.

1. Lorsque, et dans la mesure où, il n’est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu’elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais ;
2. c) aux fins de la satisfaction, conformément à [OPTION 1] l’article 34 du règlement (UE) 2016/679 / [OPTION 2] l’article 35 du règlement (UE) 2018/1725, de l’obligation de communiquer dans les meilleurs délais la violation de données à caractère personnel à la personne concernée, lorsque la violation de données à caractère personnel est susceptible d’engendrer un risque élevé pour les droits et libertés des personnes physiques.

### 9.2 Violation de données en rapport avec des données traitées par le Prestataire

En cas de violation de données à caractère personnel en rapport avec des données traitées par le Prestataire, celui-ci en informe le Client dans les meilleurs délais après en avoir pris connaissance. Cette notification contient au moins :

a) une description de la nature de la violation constatée (y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et d'enregistrements de données à caractère personnel concernés) ;

b) les coordonnées d’un point de contact auprès duquel des informations supplémentaires peuvent être obtenues au sujet de la violation de données à caractère personnel ;

c) ses conséquences probables et les mesures prises ou les mesures qu’il est proposé de prendre pour remédier à la violation, y compris pour en atténuer les éventuelles conséquences négatives.

1. Lorsque, et dans la mesure où, il n’est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu’elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais.
2. Les parties définissent à l’annexe III tous les autres éléments que le Prestataire doit communiquer lorsqu’il prête assistance au Client aux fins de la satisfaction des obligations incombant à ce dernier en vertu [OPTION 1] des articles 33 et 34 du règlement (UE) 2016/679/ [OPTION 2] des articles 34 et 35 du règlement (UE) 2018/1725.

# TITRE III - DISPOSITIONS FINALES

## Clause 10 - Non-respect des clauses et résiliation

a) Sans préjudice des dispositions du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725, en cas de manquement du Prestataire aux obligations qui lui incombent en vertu des présentes clauses, le Client peut donner instruction au Prestataire de suspendre le traitement des données à caractère personnel jusqu’à ce que ce dernier se soit conformé aux présentes clauses ou jusqu’à ce que le contrat soit résilié. Le Prestataire informe rapidement le Client s’il n’est pas en mesure de se conformer aux présentes clauses, pour quelque raison que ce soit.

b) Le Client est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel conformément aux présentes clauses si :

1) le traitement de données à caractère personnel par le Prestataire a été suspendu par le Client conformément au point a) et le respect des présentes clauses n’est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d’un mois à compter de la suspension ;

2) le Prestataire est en violation grave ou persistante des présentes clauses ou des obligations qui lui incombent en vertu du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725 ;

3) le Prestataire ne se conforme pas à une décision contraignante d’une juridiction compétente ou de l’autorité de contrôle compétente/des autorités de contrôle compétentes concernant les obligations qui lui incombent en vertu des présentes clauses ou du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.

c) Le Prestataire est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel en vertu des présentes clauses lorsque, après avoir informé le Client que ses instructions enfreignent les exigences juridiques applicables conformément à la clause 7.1, point b), le Client insiste pour que ses instructions soient suivies.

d) À la suite de la résiliation du contrat, le Prestataire supprime, selon le choix du Client, toutes les données à caractère personnel traitées pour le compte du Client et certifie auprès de celui-ci qu’il a procédé à cette suppression, ou renvoie toutes les données à caractère personnel au Client et détruit les copies existantes, à moins que le droit de l’Union ou le droit national n’impose de les conserver plus longtemps.

Le Prestataire continue de veiller à la conformité aux présentes clauses jusqu’à la suppression ou à la restitution des données.

# ANNEXE I - Liste des parties

**Responsable(s) du traitement** :

1. Nom : CHR METZ-THIONVILLE

Adresse : Hopital de Mercy, 1 allée du Château CS 45001, 57085 Metz CEDEX 03

Nom, fonction et coordonnées de la personne de contact : […]

Signature et date d'adhésion : […]

Coordonnées du DPO : Albert Crumbach - [DPO@chr-metz-thionville.fr](mailto:DPO@chr-metz-thionville.fr)

1. Nom : […]

Adresse : […]

Nom, fonction et coordonnées de la personne de contact : […]

Signature et date d’adhésion : […]

Coordonnées du DPO : […]

**Sous-traitant(s)** : [Identité et coordonnées du ou des sous-traitants et, le cas échéant, du délégué à la protection des données du sous- traitant]

1. Nom : […]

Adresse : […]

Nom, fonction et coordonnées de la personne de contact : […]

Signature et date d’adhésion : […]

Coordonnées du DPO : […]

1. Nom : […]

Adresse : […]

Nom, fonction et coordonnées de la personne de contact : […]

Signature et date d’adhésion : […]

Coordonnées du DPO : […]

# ANNEXE II - Description du traitement

*A compléter soit sous format texte rédigé soit sous forme de tableau*

* **Catégories de personnes concernées** dont les données à caractère personnel sont traitées

................................................................................................................................

* **Catégories de données à caractère personnel traitées**

................................................................................................................................

* **Les données sensibles traitées** (le cas échéant) et les limitations ou garanties appliquées qui tiennent pleinement compte de la nature des données et des risques encourus, tels que, par exemple, la limitation stricte de la finalité, les restrictions des accès (y compris l’accès réservé uniquement au personnel ayant suivi une formation spécialisée), la tenue d’un registre de l’accès aux données, les restrictions applicables aux transferts ultérieurs ou les mesures de sécurité supplémentaires.

................................................................................................................................

* **Nature du traitement**

................................................................................................................................

* **Finalité(s)** pour laquelle (lesquelles) les données à caractère personnel sont traitées pour le compte du Client

................................................................................................................................

* **Durée du traitement**

................................................................................................................................

................................................................................................................................

* **Pour le traitement par les sous-traitants (ultérieurs), préciser également l’objet, la nature et la durée du traitement**.

|  |  |
| --- | --- |
| **Catégories de personnes concernées** dont les données à caractère personnel sont concernées |  |
| **Catégories de données à caractère personnel** interrogé |  |
| **Les données sensibles** susceptibles (le cas échéant) et les limitations ou garanties appliquées qui deviendront compte de la nature des données et des risques encourus, tels que, par exemple, la limitation stricte de la finalité, les restrictions des accès (y compris l 'accès réservé uniquement au personnel ayant suivi une formation spécialisée), la tenue d'un registre de l'accès aux données, les restrictions applicables aux transferts ultérieurs ou les mesures de sécurité supplémentaires. |  |
| **Nature du traitement** |  |
| **Finalité(s)** pour laquelle (lesquelles) les données à caractère personnel sont concernées pour le compte du Client |  |
| **Durée du traitement** |  |
| **Pour le traitement par les sous-traitants (ultérieurs), préciser également l'objet, la nature et la durée du traitement.** |  |
| **Produit/Logiciel/Application concerné (le cas échéant)** |  |

# ANNEXE III - Mesures techniques et organisationnelles, y compris mesures techniques et organisationnelles visant à garantir la sécurité des données

*Les mesures techniques et organisationnelles doivent faire l’objet* ***d’une description concrète****, et non pas générique.*

Description des mesures de sécurité techniques et organisationnelles mises en œuvre par le ou les sous-traitants (y compris toute certification pertinente) visant à garantir un niveau de sécurité approprié, compte tenu de la nature, de la portée, du contexte et de la finalité du traitement, ainsi que des risques pour les droits et libertés des personnes physiques.

Exemples de mesures possibles :

* mesures de pseudonymisation et de chiffrement des données à caractère personnel;
* mesures visant à garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
* mesures assurant de disposer de 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;
* procédures visant à tester, à analyser et à évaluer régulièrement l’efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement;
* mesures d’identification et d’autorisation de l’utilisateur;
* mesures de protection des données pendant la transmission;
* mesures de protection des données pendant le stockage;
* mesures visant à garantir la sécurité physique des sites où les données à caractère personnel sont traitées;
* mesures visant à garantir l’enregistrement des événements;
* mesures visant à assurer la configuration des systèmes, y compris la configuration par défaut;
* mesures de gouvernance et de gestion de l’informatique interne et de la sécurité informatique;
* mesures de certification/assurance des procédés et produits;
* mesures visant à garantir la minimisation des données;
* mesures visant à garantir la qualité des données;
* mesures visant à garantir une conservation limitée des données;
* mesures visant à garantir la responsabilité;
* mesures permettant la portabilité des données et garantissant l’effacement]

Pour les transferts vers des sous-traitants (ultérieurs), décrire également les mesures techniques et organisationnelles spécifiques que doit prendre le sous-traitant (ultérieur) pour être en mesure de prêter assistance au Client.

Description des mesures techniques et organisationnelles spécifiques que le Prestataire doit prendre pour pouvoir prêter assistance au Client.

# ANNEXE IV - Liste de sous-traitants ultérieurs

*La présente annexe doit être complétée en cas d’autorisation spécifique de sous-traitants ultérieurs [clause 7.7, point a), option 1].*

**Le Client a autorisé le recours aux sous-traitants ultérieurs suivants :**

1. Nom : ......................................................................................................................................

Adresse :..................................................................................................................................

Nom, fonction et coordonnées de la personne de contact : …................................................

Description du traitement (y compris une délimitation claire des responsabilités dans le cas où plusieurs sous-traitants ultérieurs sont autorisés) : ..............................................................................................................................................................................................................................................................................................................

1. Nom : ......................................................................................................................................

Adresse :..................................................................................................................................

Nom, fonction et coordonnées de la personne de contact : …................................................

Description du traitement (y compris une délimitation claire des responsabilités dans le cas où plusieurs sous-traitants ultérieurs sont autorisés) : ..............................................................................................................................................................................................................................................................................................................

1. Nom : ......................................................................................................................................

Adresse :..................................................................................................................................

Nom, fonction et coordonnées de la personne de contact : …................................................

Description du traitement (y compris une délimitation claire des responsabilités dans le cas où plusieurs sous-traitants ultérieurs sont autorisés) : ..............................................................................................................................................................................................................................................................................................................

1. Nom : ......................................................................................................................................

Adresse :..................................................................................................................................

Nom, fonction et coordonnées de la personne de contact : …................................................

Description du traitement (y compris une délimitation claire des responsabilités dans le cas où plusieurs sous-traitants ultérieurs sont autorisés) : ..............................................................................................................................................................................................................................................................................................................

1. Nom : ......................................................................................................................................

Adresse :..................................................................................................................................

Nom, fonction et coordonnées de la personne de contact : …................................................

Description du traitement (y compris une délimitation claire des responsabilités dans le cas où plusieurs sous-traitants ultérieurs sont autorisés) : ..............................................................................................................................................................................................................................................................................................................