|  |  |
| --- | --- |
| DIRECTION GENERALE DE LA SANTE | **MARCHÉ PUBLIC**  ACCORD-CADRE DE SERVICES |

|  |  |  |
| --- | --- | --- |
|  |  | Prestations d'assistance médicale, d'évacuations sanitaires (EVASAN), de transport de personnels et d'affrètement pour le compte du ministère chargé de la Santé |

|  |
| --- |
| **Annexe\_RGPD** |

|  |  |  |
| --- | --- | --- |
|  | Consultation n° | PRA039766 |

Sommaire

[Clause 1. Objet et champ d’application 5](#_Toc190789873)

[Clause 2. Invariabilité des clauses 5](#_Toc190789874)

[Clause 3. Interprétation 5](#_Toc190789875)

[Clause 4. Hiérarchie 6](#_Toc190789876)

[Clause 5. Description du ou des traitements 6](#_Toc190789877)

[Clause 6. Obligations des parties 6](#_Toc190789878)

[6.1 Instructions 6](#_Toc190789879)

[6.2 Limitation de la finalité 6](#_Toc190789880)

[6.3 Sécurité du traitement 6](#_Toc190789881)

[6.4 Données sensibles 7](#_Toc190789882)

[6.5 Documentation et conformité 8](#_Toc190789883)

[6.6 Recours à des sous-traitants ultérieurs 8](#_Toc190789884)

[6.7 Application d’un droit extraterritorial d’un pays tiers 9](#_Toc190789885)

[6.8 Hébergement des données 9](#_Toc190789886)

[6.9 Registre de traitement 10](#_Toc190789887)

[Clause 7. Assistance au responsable de traitement 10](#_Toc190789888)

[Clause 8. Notification de violations de données à caractère personnel 11](#_Toc190789889)

[8.1 Violation de données en rapport avec des données traitées par le responsable de traitement 11](#_Toc190789890)

[8.2 Violation de données en rapport avec des données traitées par le sous-traitant 12](#_Toc190789891)

[Clause 9. L’audit du sous-traitant 13](#_Toc190789892)

[Clause 10. Sort des données 13](#_Toc190789893)

[Clause 11. Contrôle de l’autorité compétente 14](#_Toc190789894)

[Annexe 1. Liste des parties et des acteurs 16](#_Toc190789895)

[Annexe 2. Description du traitement 18](#_Toc190789896)

[Annexe 3. Mesures techniques et organisationnelles, y compris mesures techniques et organisationnelles visant à garantir la sécurité des données 21](#_Toc190789897)

[Annexe 4. Procès-verbal de destruction de données à caractère personnel et des informations confidentielles traitées 25](#_Toc190789898)

[Annexe 5. notification d’une violation de données à caractère personnel et des informations confidentielles traitées 26](#_Toc190789899)

**Préambule**

Vu le règlement européen (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 96/46/CE (dit « règlement général sur la protection des données » (RGPD)),

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés,

# Objet et champ d’application

Les présentes clauses contractuelles types (ci-après les « clauses ») ont pour objet de garantir la conformité l’article 28, paragraphes 3 et 4, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données.

Les responsables du traitement et les sous-traitants parties aux présentes clauses les ont acceptées afin de garantir le respect des dispositions de l’article 28, paragraphes 3 et 4, du règlement (UE) 2016/679.

Les présentes clauses s’appliquent au traitement des données à caractère personnel tel que décrit à l’annexe 2.

Les annexes 1 à 5 font partie intégrante des clauses.

Les présentes clauses sont sans préjudice des obligations auxquelles le responsable de traitement est soumis en vertu du règlement (UE) 2016/679.

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.

En cas de contradiction entre les présentes clauses et des dispositions législatives et/ou réglementaires, ces dernières prévaudront.

# Invariabilité des clauses

Les parties s’engagent à modifier les articles, ainsi que les informations aux annexes, uniquement avec l’accord des deux parties.

Les parties ne sont 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.

# Interprétation

Lorsque des termes définis respectivement dans le règlement (UE) 2016/679 figurent dans les clauses, ils s’entendent comme dans le règlement en question.

Les présentes clauses doivent être lues et interprétées à la lumière des dispositions du règlement (UE) 2016/679.

Les présentes clauses ne doivent pas être interprétées d’une manière contraire aux droits et obligations prévus par le règlement (UE) 2016/679 ou d’une manière qui porte atteinte aux libertés ou droits fondamentaux des personnes concernées.

# 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.

# 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 responsable de traitement, sont précisés à l’annexe 2.

# Obligations des parties

## Instructions

Le sous-traitant ne traite les données à caractère personnel que sur instruction documentée du responsable de traitement, 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 sous-traitant informe le responsable de traitement 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 responsable de traitement pendant toute la durée du traitement des données à caractère personnel. Ces instructions doivent toujours être documentées.

Le sous-traitant informe immédiatement le responsable de traitement si, selon lui, une instruction donnée par le responsable de traitement constitue une violation du règlement (UE) 2016/679 1725 ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

## Limitation de la finalité

Le sous-traitant traite les données à caractère personnel uniquement pour la ou les finalités spécifiques du traitement, telles que définies à l’annexe 2, sauf instruction complémentaire du responsable de traitement.

## Sécurité du traitement

Le sous-traitant met au moins en œuvre les mesures techniques et organisationnelles précisées à l’annexe 3 pour assurer la sécurité des données à caractère personnel. Figure parmi ces mesures la protection des données contre toute violation de la sécurité entraînante, 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.

De façon générale, tous les flux doivent être sécurisés par des mesures techniques et organisationnelles adaptées aux risques. Tous les flux contenant des données perçues comme sensibles ou sensibles doivent être chiffrés de bout en bout.

Pour chaque interface d’accès au système, le Sous-Traitant s’engage à déployer des mécanismes d’authentifications adaptés aux risques et à recenser la liste des comptes existants ainsi que les rôles et privilèges qui y sont associés. Ces comptes sont nominatifs et l’utilisation de mots de passe constructeur ou par défaut est formellement interdite. Les entrées en session (date, heure, utilisateur, poste informatique / terminal) sont tracées dans un journal.

Le sous-traitant 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 sous-traitant 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.

Enfin, lorsqu’un environnement de développement, de test ou de recette est déployé, le Sous-Traitant s’engage à ne pas y répliquer les données de l’environnement de production. Les données pouvant être transférées aux environnements de développement, de test ou de recette doivent être limitées aux usages strictement nécessaires et doivent être lorsque possible anonymisées.

Par ailleurs, le sous-traitant a une obligation de confidentialité, qui s’applique sans limitation de durée et s’engage à :

* ne communiquer les informations qu’aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication dans le cadre de la mission, qu’il s’agisse de personnes privées, publiques, physiques ou morales ;
* ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l’exécution de la mission ;
* prendre toutes les mesures conformes aux usages et à l’état de l’art dans le cadre de leurs attributions afin d’éviter l’utilisation détournée ou frauduleuse de ces données ;
* s’assurer que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
* s’assurer, dès qu’une personne ayant disposé de l’accès fourni dans le cadre de la mission quitte cette fonction, que les identifiants fournis soient mis à jour pour lui supprimer les accès ;
* ne pas utiliser les données auxquelles il peut accéder à des fins autres que celles prévues dans le cadre des missions respectives.

## 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 sous-traitant applique des limitations spécifiques et/ou des garanties supplémentaires telles qu’exigées par le Responsable de traitement en annexe 3.

## Documentation et conformité

Les parties doivent pouvoir démontrer la conformité avec les présentes clauses.

Le sous-traitant traite de manière rapide et adéquate les demandes du responsable de traitement concernant le traitement des données conformément aux présentes clauses.

Le sous-traitant met à la disposition du responsable de traitement toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans les présentes clauses et découlant directement du règlement (UE) 2016/679. À la demande du responsable de traitement, le sous-traitant 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 responsable de traitement peut tenir compte des certifications pertinentes en possession du sous-traitant.

Le responsable de traitement peut décider de procéder lui-même à l’audit ou de mandater un auditeur indépendant, selon les conditions définies à la clause 12. Les audits peuvent également comprendre des inspections dans les locaux ou les installations physiques du sous-traitant et sont, le cas échéant, effectués moyennant un préavis de 10 jours.

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.

Le Sous-traitant doit être en mesure de fournir au Responsable de traitement à tout moment une liste des personnes autorisées à accéder aux données.

Les équipements (serveurs, postes de travail, réseau) utilisés dans le cadre de l’exécution des prestations confiées au Sous-traitant doivent être localisés dans des locaux sécurisés au sein de l’Union européenne selon les normes en vigueur.

## Recours à des sous-traitants ultérieurs

Le sous-traitant peut recruter un sous-traitant ultérieur dans les conditions définies à l’article 4.6 du cahier des clauses administratives particulière (CCAP) du présent marché.

Lorsque le sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du responsable de traitement), il le fait au moyen d’un contrat qui impose au sous-traitant ultérieur, les mêmes obligations en matière de protection des données que celles imposées au sous-traitant en vertu des présentes clauses. Le sous-traitant 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, qu’il soit situé sur le territoire de l’Union européenne et qu’il ne soit pas soumis à un droit extraterritorial d’un pays tiers à l’Union européenne.

À la demande du responsable de traitement, le sous-traitant 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.

Le sous-traitant demeure pleinement responsable, à l’égard du responsable de traitement, de l’exécution des obligations du sous-traitant ultérieur conformément au contrat conclu avec le sous-traitant ultérieur. Le sous-traitant informe le responsable de traitement de tout manquement du sous-traitant ultérieur à ses obligations contractuelles.

Le sous-traitant convient avec le sous-traitant ultérieur d’une clause du tiers bénéficiaire selon laquelle — dans le cas où le sous-traitant a matériellement disparu, a cessé d’exister en droit ou est devenu insolvable — le responsable de traitement 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.

## Application d’un droit extraterritorial d’un pays tiers

Par exception à la clause 7.7 deuxième paragraphe, si le sous-traitant recrute un sous-traitant ultérieur situé sur le territoire de l’Union européenne et soumis à un droit extraterritorial d’un pays tiers à l’Union européenne, il s’engage à évaluer si la législation du pays tiers permet de respecter le niveau de protection requis par le droit de l’Union européenne, notamment règlement (EU) 2016/679, ainsi que celles requises par les dispositions législatives et réglementaires en vigueur. Si ce niveau ne peut pas être respecté, le sous-traitant s’engage à prévoir des mesures supplémentaires pour garantir un niveau de protection équivalent à celui prévu le droit de l’Union européenne et par le droit français, et à s’assurer que la législation du pays tiers n'empiétera pas sur ces mesures supplémentaires de manière à les priver d'effectivité.

Lorsque le sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques, il veille à ce que le sous-traitant ultérieur respecte la présente clause.

À la demande du responsable de traitement, le sous-traitant lui fournit l’évaluation de la législation du pays tiers et le cas échéant la liste des mesures supplémentaires qui sont prises par le sous-traitant pour garantir un niveau de protection requis par le droit de l’Union européenne, notamment règlement (EU) 2016/679 et par le droit français.

## Hébergement des données

Le sous-traitant s’engage à traiter et héberger les données uniquement sur le territoire de l’Union européenne et à ce que les équipements (serveurs, postes de travail, réseau) utilisés dans le cadre de l’exécution des prestations confiées au sous-traitant soient localisés dans des locaux sécurisés au sein de l’Union européenne selon les normes en vigueur. Cet engagement s’applique également aux sous-traitants ultérieurs qui sont sous la responsabilité du sous-traitant.

Lorsque le sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques, il veille à ce que ce dernier respecte la présente clause.

Le sous-traitant doit communiquer sur demande du responsable de traitement la liste de tous les lieux de stockage de données (site d’hébergement principal, site(s) de secours, etc.) et adresses à partir desquels les intervenants et le cas échéant les sous-traitants ultérieurs ont accès aux données. Si la faisabilité technique de cette exigence s’avère délicate dans le cadre d’architectures distribuées, il peut être demandé au Sous-traitant d’être en mesure de localiser, a posteriori, et non en permanence, le lieu de stockage des données.

Le sous-traitant s’engage à ne pas transférer, héberger ou traiter les données personnelles en dehors de l’Union européenne, y compris par l’intermédiaire d’un sous-traitant ultérieur, sauf autorisation expresse et préalable du Responsable de traitement.

En conséquence, le sous-traitant garantit que l’ensemble des données personnelles seront exclusivement hébergées et traitées sur des serveurs situés dans un État membre de l’Union européenne.

Lorsque le sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques, il veille à ce que ce dernier respecte strictement cette interdiction de transfert.

Sur demande du Responsable de traitement, le sous-traitant communique la liste exhaustive des lieux d’hébergement des données et des pays à partir desquels les intervenants et ses sous-traitants ont accès aux données.

## Registre de traitement

Conformément à l’article 30, paragraphe 2 du règlement (EU) 2016/679, le Sous-Traitant déclare tenir par écrit un registre de toutes les 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 activités de traitements effectués pour le compte du Responsable de 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 ;
* Une description générale des mesures de sécurité physiques, techniques et organisationnelles.

# Assistance au responsable de traitement

Le sous-traitant informe sans délai le responsable du traitement de toute demande qu’il a reçue de la part de la personne concernée par courriel électronique au Référent RGPD de la DGS, à l’adresse :………………….. Il ne donne pas lui-même suite à cette demande, à moins que le responsable du traitement des données ne l’y ait autorisé. Le Sous-traitant tient un registre de demande d’exercice de droit qu’il envoie de manière hebdomadaire au Responsable de traitement.

Le sous-traitant prête assistance au responsable du traitement 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 sous-traitant se conforme aux instructions du responsable du traitement.

Outre l’obligation incombant au sous-traitant d’assister le responsable du traitement en vertu de la clause 8, point b), le sous-traitant aide en outre le responsable du traitement à garantir le respect des obligations suivantes, compte tenu de la nature du traitement et des informations dont dispose le sous-traitant :

* 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 ;
* 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 responsable du traitement ne prenait pas de mesures pour atténuer le risque ;
* L’obligation de veiller à ce que les données à caractère personnel soient exactes et à jour, en informant sans délai le responsable du traitement si le sous-traitant apprend que les données à caractère personnel qu’il traite sont inexactes ou sont devenues obsolètes ;
* Les obligations prévues à l’article 32 du règlement (UE) 2016/679 ;

Les parties définissent à l’annexe 3 les mesures techniques et organisationnelles appropriées par lesquelles le sous-traitant est tenu de prêter assistance au responsable du traitement dans l’application de la présente clause, ainsi que la portée et l’étendue de l’assistance requise.

# Notification de violations de données à caractère personnel

En cas de violation de données à caractère personnel, le sous-traitant coopère avec le responsable de traitement 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, en tenant compte de la nature du traitement et des informations dont dispose le sous-traitant.

## Violation de données en rapport avec des données traitées par le responsable de traitement

En cas de violation de données à caractère personnel en rapport avec des données traitées par le responsable de traitement, le sous-traitant prête assistance au responsable de traitement :

1. 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 responsable de traitement 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) ;
2. Aux fins de l’obtention des informations suivantes qui, conformément à l’article 33, paragraphe 3, du règlement (UE) 2016/679, doivent figurer dans la notification du responsable de traitement, et inclure, au moins :

* 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 ;
* Les conséquences probables de la violation de données à caractère personnel ;
* Les mesures prises ou les mesures que le responsable de 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.

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 ;

1. Aux fins de la satisfaction, conformément à l’article 34 du règlement (UE) 2016/679 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.

## Violation de données en rapport avec des données traitées par le sous-traitant

En cas de violation de données à caractère personnel en rapport avec des données traitées par le sous-traitant, celui-ci en informe le responsable de traitement dans les meilleurs délais après en avoir pris connaissance (liste des personnes à prévenir en annexe 5). Cette notification se fait au moyen du formulaire en annexe 5 et contient au moins :

1. 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) ;
2. 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 ;
3. 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.

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.

# L’audit du sous-traitant

Le responsable de traitement se réserve le droit de contrôler, ou de faire contrôler par un auditeur tiers, à tout moment, et pendant toute la durée de validité du contrat, les mesures prises par le sous-traitant afin de garantir le respect des présentes.

Afin de faciliter l’audit, de permettre au sous-traitant de réunir la documentation et assurer la disponibilité des personnes concernées, le responsable de traitement s’engage à informer le sous-traitant dix jours avant le début de tout audit. Le sous-traitant ne peut refuser la date de l’audit sans motif légitime. Le responsable de traitement se réserve le droit de réaliser, ou de faire réaliser, un audit sans respecter le délai de prévenance dans l’éventualité d’une violation de données à caractère personnel.

Le sous-traitant s’engage à prendre les mesures nécessaires afin d’assurer le bon déroulement de l’audit. Le sous-traitant autorise et accepte que les audits pourront être réalisés directement par le responsable de traitement ou par un auditeur externe, à visiter les locaux du sous-traitant, à rencontrer et interviewer les personnels du sous-traitant, et accéder aux machines participant à la réalisation des traitements concernés par les présentes. Le sous-traitant met à disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de ses obligations.

Le sous-traitant s’assure de l’applicabilité du présent article, dans les mêmes conditions, aux sous-traitants ultérieurs.

# Sort des données

Au terme du présent contrat, le sous-traitant s’engage, après s’être assuré des modalités relatives à la réversibilité et/ou la transférabilité, à détruire toutes les données à caractère personnel. Cette destruction s’accompagne d’un procès-verbal de destruction transmis au responsable de traitement dans les plus brefs délais.

# Contrôle de l’autorité compétente

En cas de contrôle de l’une ou l’autre des parties, diligenté par l’autorité compétente, les parties s’engagent à se porter assistance et mettre à disposition toutes les informations nécessaires pour démontrer le respect des obligations prévues par la présente convention.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | |  |  | |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Liste des parties et des acteurs

**Responsable de traitement**

Nom : ministère de la Santé – CENTRE DE CRISES SANITAIRES (CCS)

Adresse : 14 avenue Duquesne 75 350 Paris 07 SP

Personnes habilitées à donner des instructions :

Canal à utiliser (préciser : note, téléphone, mail, avenant…) : Courriel.

**Sous-traitant :**

Nom : …

Adresse : …

Personnes habilitées à recevoir les instructions : noms, fonctions, coordonnées

**(Option) Sous-traitant :**

Nom : …

Adresse : …

**Personnes habilitées à recevoir les instructions :** noms, fonctions, coordonnées

|  |  |  |
| --- | --- | --- |
| Responsable de traitement délégué : DGS / CSS |  | Sous-traitant : Nom de l’entité concernée |
| GOUVERNANCE DE LA SOUS-TRAITANCE | | |
|  |  | Prénom Nom : Email :  Téléphone : |
| SUIVI OPERATIONNEL DU TRAITEMENT | | |
| Prénom Nom : Email :  Téléphone : |  | Prénom Nom : Email :  Téléphone : |
| SECURITE DES SYSTEMES D’INFORMATION | | |
| Prénom Nom :  Emai : |  | Prénom Nom :  Email :  Téléphone : |
| PROTECTION DES DONNEES PERSONNELLES (Référente RGPD) | | |
| Prénom Nom :  Email : |  | Prénom Nom : Email :  Téléphone : |
| Autre | | |
| Prénom Nom : Email :  Téléphone : |  | Prénom Nom : Email :  Téléphone : |

### Description du traitement

Dans le cadre des missions objet du présent accord-cadre, le titulaire sera amené à détenir des données personnelles sur les personnes couvertes par ces prestations

Présentation du traitement faisant l’objet de la sous-traitance

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

**Les données portent à la fois sur les patients transportés et leurs accompagnants évacués pour des raisons sanitaires (EVASAN), ainsi que le personnel soignant envoyés dans les zones de crise.**

**De même, afin de permettre le remboursement des frais de mission de l’agent, le titulaire mettra en place des canaux de transmission sécurisée via une plateforme numérique dédiée.**

**Catégories de données à caractère personnel traitées**

Les catégories de données concernées sont les suivantes :

Détail d'un patient / accompagnant / soignants volontaires :

• Numéro

• Nom \*

• Prénom \*

• Date de naissance \*

• Sexe \*

• La commune de naissance est-elle en France ?

Coordonnées du participant :

• Adresse complète

• Code postal – Commune

• Téléphone fixe

• Téléphone portable

• Courriel ;

* Coordonnées bancaires.

**Nature du traitement (opération) : Conforme aux dispositions applicables**

**Finalité(s) pour laquelle (lesquelles) les données à caractère personnel sont traitées pour le compte du responsable du traitement :** organiser le transport des personnels mobilisés et des patients, accompagnés et la prise en charge des frais de mission.

**Durée du traitement :**  Jusqu’à la fin de l’accord-cadre.

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

Description des mesures de sécurité techniques et organisationnelles mises en œuvre par le ou les sous-traitants 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.

1. **Sécurisation des accès aux locaux et protection du matériel critique**

La protection des locaux et des équipements informatiques est essentielle pour garantir la confidentialité et l’intégrité des informations. Des mesures sont mises en place afin de limiter les risques d’accès non autorisés et de vol de matériel.

**Contrôle des accès physiques**

* Restriction des accès : Mise en place d’un contrôle d’accès (badges, serrures sécurisées) pour limiter l’entrée aux seules personnes autorisées ;
* Gestion des visiteurs : Enregistrement obligatoire des visiteurs et accompagnement dans les zones sensibles ;
* Surveillance et dissuasion : Utilisation de dispositifs de vidéosurveillance et d’alarmes pour détecter toute intrusion.

**Protection des équipements et des supports de données**

* Stockage sécurisé : Utilisation d’armoires verrouillées pour protéger les équipements critiques et les supports de stockage ;
* Suivi du matériel : Inventaire régulier des équipements et des supports contenant des données sensibles ;
* Destruction sécurisée : Mise en place de procédures de suppression définitive des supports obsolètes (broyeurs, effacement sécurisé).

1. **Sécurité du Réseau**

La mise en place de mesures de protection réseau vise à garantir l’intégrité et la confidentialité des échanges de données, en limitant les risques d’intrusion et d’interception.

**Contrôle des flux et protection périmétrique**

* Pare-feu et filtrage : Installation d’un pare-feu avec règles restrictives pour bloquer les connexions non autorisées.
* Surveillance des accès : Mise en place d’un système de journalisation permettant de détecter les anomalies et d’analyser les tentatives de connexion.

**Segmentation et isolation des services**

* Séparation des réseaux : Création de VLANs pour cloisonner les services internes, l’IoT et les ressources exposées.
* Protection des interfaces externes : Mise en place d’une DMZ pour sécuriser les services accessibles depuis l’extérieur, avec une configuration adaptée aux besoins métiers.

**Sécurisation des connexions à distance**

* Utilisation d’un VPN : Chiffrement des communications via une solution VPN SSL ou IPsec pour les accès distants.
* Authentification renforcée : Mise en place d’un double facteur d’authentification et de certificats pour les connexions aux ressources sensibles.

1. **Sécurité des Postes et Applications**

La sécurisation des terminaux et des applications est essentielle pour limiter les risques liés aux maliciels, aux vulnérabilités et aux accès non autorisés.

**Protection des équipements et des données**

* Détection et réponse aux menaces : Installation d’une solution EDR (Endpoint Detection and Response) et d’un antivirus/anti-malware régulièrement mis à jour.
* Filtrage des contenus : Mise en place d’une protection centralisée contre les menaces web et les emails malveillants.

**Gestion des mises à jour et des correctifs**

* Mise à jour automatisée : Application régulière des correctifs de sécurité sur les systèmes d’exploitation et les logiciels pour limiter les failles exploitables.

**Sécurisation des accès et des sessions**

* Politique de mots de passe robuste : Utilisation de mots de passe complexes et recours à un gestionnaire d’identifiants sécurisé.
* Authentification renforcée : Mise en place d’une authentification multi-facteurs (MFA) pour les comptes sensibles, notamment administrateurs.
* Verrouillage des sessions inactives : Configuration automatique pour limiter les risques d’accès non autorisés.

1. **Sécurité des Données**

La protection des données sensibles repose sur des mesures visant à garantir leur confidentialité, leur intégrité et leur disponibilité, tout en réduisant les risques de perte ou de fuite.

**Sauvegardes et restauration**

* Application de la règle « 3-2-1 » : Automatisation des sauvegardes sur plusieurs supports (local et cloud) avec vérifications régulières.
* Tests de restauration : Vérification périodique de l’efficacité des procédures de récupération des données.

**Contrôle des accès et anonymisation**

* Principe du moindre privilège : Attribution des droits d’accès strictement nécessaires, avec revue trimestrielle des autorisations.
* Réduction des risques en cas d’incident : Mise en place de l’anonymisation ou de la pseudonymisation des données sensibles lorsque cela est possible.

**Destruction sécurisée des données**

* Effacement définitif : Adoption d’une procédure d’effacement sécurisé et d’un calendrier de suppression automatique des données obsolètes.
* Traçabilité des destructions : Documentation des processus pour garantir leur conformité et leur suivi.

1. **Gouvernance et Conformité : Structurer la Sécurité et Sensibiliser les Équipes**

Une gouvernance efficace de la sécurité repose sur une organisation claire, une documentation actualisée et une culture de sensibilisation pour réduire les risques humains et garantir la conformité aux exigences réglementaires.

**Pilotage et organisation de la sécurité**

* Désignation d’un responsable de la sécurité : Identification d’un référent chargé de coordonner les actions de protection des systèmes d’information.
* Définition d’une politique de sécurité : Élaboration de règles internes adaptées aux risques et aux obligations légales.
* Gestion des incidents : Mise en place d’un processus de déclaration et de traitement des incidents de sécurité, avec une procédure d’escalade claire.

**Sensibilisation et formation continue**

* Intégration de la sécurité dès l’accueil : Formation initiale des nouveaux arrivants sur les bonnes pratiques et les risques numériques.
* Rappels réguliers : Campagnes de sensibilisation sur des thématiques clés (hameçonnage, protection des données, gestion des accès).
* Simulations et exercices : Organisation de tests (ex. : faux e-mails de phishing) pour évaluer et améliorer les réflexes de sécurité des équipes.

1. **Mesures Spécifiques**

* Contrôle d’Accès aux Données
  + Mise en place d’un système de gestion des droits d’accès renforcé, permettant un suivi précis des accès aux données sensibles.
* Sécurisation des Transferts et Stockage
  + Utilisation de protocoles sécurisés pour tous les transferts de données.
* Chiffrement systématique : Toute transmission de données sensibles doit être chiffrée, que ce soit via un canal sécurisé (TLS, VPN) ou au repos (fichiers protégés par chiffrement).

### Procès-verbal de destruction de données à caractère personnel et des informations confidentielles traitées

Je, soussigné, *…………………………………………………*, certifie que l’ensemble des données à caractère personnel et des informations confidentielles auxquelles j’ai eu accès dans le cadre de l’accord-cadre n° **PRA039766**, a été détruit de manière irréversible après l’avoir restitué intégralement à la Direction générale de la Santé (DGS) en date du *Jour/Mois/Année*.

La destruction des données à caractère personnel a été réalisée à la date du *Jour/Mois/Année*.

Fait à

Le

Signature

### Notification d’une violation de données à caractère personnel et des informations confidentielles traitées

1. **Détection de l’incident de sécurité/violation de données**

**PRINCIPE**

Dès que le sous-traitant identifie ou est informé, par l'un de ses employés, par un système de détection, par des systèmes de gestion des événements et des informations de sécurité ou par toute autre source, d'une violation de données ou a des motifs raisonnables de soupçonner une telle violation, il doit immédiatement en informer le responsable désigné au sein de la DGS.

Les exemples ci-après sont des situations qui **déclenchent obligatoirement** l’application du présent mode opératoire :

* Un incident de sécurité est détecté via les outils d’analyse de logs ;
* Compromission d’un mot de passe d’une personne accédant aux données dans les environnements de production contenant des données à caractère personnel (ou tout autre environnement dès lors qu’il contient des données à caractère personnel) ;
* Perte d’un support (ordinateur, téléphone, clé USB, etc.) contenant des données à caractère personnel même si le support est chiffré ;
* Constat d’un accès illégitime à des données à caractère personnel ;
* Perte/suppression des données à caractère personnel ;
* Indisponibilité des données (uniquement liée à des incidents de sécurité) ;
* Constat d’une modification non désirée de données.

|  |
| --- |
| **Quel que soit le jour ou l’heure du constat de l’incident, celui-ci devra être notifié dans les plus brefs délais après en avoir pris connaissance.** |

|  |
| --- |
| **Le cas échéant, la notification de l’incident doit se faire concomitamment à la mise en place des mesures visant à stopper l’incident ou à en diminuer les conséquences probables (mesures de remédiation).** |

1. **Personne à notifier**

|  |
| --- |
| **Dans le cadre de la gestion des violations de données, il est nécessaire de connaître les bons interlocuteurs avec qui échanger et communiquer les bonnes informations. Cela est indispensable afin d’éviter tout manquement qui nuirait à un traitement efficace de la violation.** |

La liste des personnes à contacter au sein de la DGS **quel que soit l’incident** :

* **Référent RGPD – DGS :**

1. **Formulaire de notification de violation de données**

*Partie à copier dans le corps d’un courriel*

|  |  |
| --- | --- |
| **Description l’incident de sécurité/violation de données** | |
| **Date de la violation** | |
| Date et heure du début de la violation/incident |  |
| Date et heure de la fin de la violation/incident |  |
| Date et heure de prise de connaissance de la violation/incident |  |
| Date et heure de notification de la DGS, et personne(s) notifiée(s) |  |
| Raisons du retard dans la notification de la DGS |  |
| Commentaires sur les dates |  |
|  | |
| **Contacts du sous-traitants** | |
| Les coordonnées des personnes en charge du traitement de l’incident et leur rôle[[1]](#footnote-2) |  |
| Les coordonnées du/de la Délégué(e) la Protection des données (DPO) du sous-traitant |  |
| Les coordonnées du Responsable de la Sécurité des Systèmes d’Information (RSSI) du sous-traitant |  |
|  | |
| **Information sur le système d’information concernés** | |
| Nom de l’application ou Système d’information concerné(e) |  |
| Environnement concernés (par exemple : production) et le nom de la base |  |
| Identité de l’organisme responsable de la base |  |
|  | |
| **A propos de la violation/incident** | |
| Toute information sur le statut de l’incident : terminé, en cours, analyse en cours, etc. |  |
| Circonstances détaillez de la découverte de la violation |  |
| La nature de l’incident (exemple : divulgation non autorisée de données, indisponibilité non intentionnelle du SI, extraction de données non autorisés, etc.) |  |
| Origine(s) de l'incident |  |
| Liste des données à caractère personnel concernées et/ou traitées dans l’application ou le SI |  |
| Données sensibles concernées |  |
| Nombre approximatif d'enregistrements concernés par la violation |  |
| Personnes ou catégories de personnes concernées (à qui appartiennent les données, exemple : salariés des entreprises) |  |
| Nombre approximatif de personnes concernées par la violation |  |
| La volumétrie des données impactées ou susceptibles d’être impactées par l’incident |  |
| Descriptif détaillé de la violation de données/incident |  |
|  | |
| **Information sur les mesures de sécurité** | |
| Mesures techniques et organisationnelles mises en œuvre préalablement à la détection de l’incident | *(Possibilité de joindre un document listant de manière détaillez les mesures techniques et organisationnelles de sécurité)* |
| Mesures techniques et organisationnelles mises en œuvre à compter de la détection de l’incident et celles en cours d’implémentation |  |
| L’existence d’une sauvegarde, et le cas échéant si elle est aussi impactée par l’incident |  |
| L’existence d’un Plan de Reprise d’Activité (PRA) et/ou un Plan de Continuité d’Activité (PCA) |  |
| Description de l’incident :   * Détection (qui, quand, comment) * Actions réalisées * Les analyses en cours et celles réalisées |  |
| Mesures techniques et organisationnelles de sécurité mise en place (au moment de la survenance de l’incident) susceptibles de réduire le risque pour les personnes en cas de violation de données |  |
|  | |
| **Autre** | |
| Autres informations jugées pertinentes |  |
| Liste des actions prises depuis la prise de connaissance de la violation/incident | 1 –  2 –  3 – |
| Document transmis à la DGS (date et heure) |  |
|  | |
| **Partie réservée à la DGS** | |
| Nom du PV clôture  (À saisir ultérieurement par la DGS) |  |

1. Dans la mesure du possible et en fonction de la gravité de la violation, toute information sur leurs contraintes personnelles, exemple : M. X doit impérativement aller chercher son enfant à l’école à 17h [↑](#footnote-ref-2)