ANNEXE RGPD CCAP

SOMMAIRE

[ANNEXE RGPD CCAP 1](#_Toc143533491)

[1 Définitions (extraits de l’article 4 du RGPD) 2](#_Toc143533492)

[2 Objet 2](#_Toc143533493)

[3 Description du/des traitement(s) de données à caractère personnel 3](#_Toc143533494)

[3.1 Les traitements sous-traités : 3](#_Toc143533495)

[3.2 Les traitements propres au Sous-Traitant : 4](#_Toc143533496)

[4 Obligations du Sous-Traitant vis-à-vis du Responsable de Traitement Mipih 4](#_Toc143533497)

[4.1 Traitement des données : 4](#_Toc143533498)

[4.2 Confidentialité des données : 5](#_Toc143533499)

[4.3 Protection des données : 5](#_Toc143533500)

[4.4 Sous-traitance de troisième niveau (ou plus) ou Sous-traitance « ultérieure » : 5](#_Toc143533501)

[4.5 Assistance au Sous-Traitant Mipih : 6](#_Toc143533502)

[4.6 Notification des violations de données à caractère personnel : 6](#_Toc143533503)

[4.7 Mesures de sécurité techniques et organisationnelles : 7](#_Toc143533504)

[4.8 Réversibilité des données : 7](#_Toc143533505)

[4.9 Délégué à la Protection des Données : 7](#_Toc143533506)

[4.10 Registre des catégories d’activités de traitement : 7](#_Toc143533507)

[5 Obligations du Responsable de Traitement vis-à-vis du Sous-Traitant 8](#_Toc143533508)

[6 Audit 8](#_Toc143533509)

# Définitions (extraits de l’article 4 du RGPD)

Aux fins du **R**èglement **G**énéral de **P**rotection des **D**onnées du 27/04/2016, on entend par :

* **Données à caractère personnel** : toute information se rapportant à une personne physique identifiée ou identifiable directement ou indirectement.
* **Personne concernée** : une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
* **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. Cette définition intègre également le sous-traitant ultérieur à qui le sous-traitant peut faire appel.
* **Traiter/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.
* **Violation de données à caractère personnel** : une 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 transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

# Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles **Titulaire du marché**, en tant que Sous-Traitant, s’engage à effectuer des opérations de traitement de données à caractère personnel pour le seul compte du Mipih Responsable de Traitement dans le cadre du N° de marché.

Ces clauses sont établies entre :

* Le « Responsable de Traitement » Mipih, l’Acheteur, mettant en œuvre des traitements de données à caractère personnel, et ayant souscrit un contrat avec le « Sous-traitant » parmi les catégories de services détaillées par la clause 3.
* Le « Sous-traitant », Titulaire du marché, réalisant pour le compte du Responsable de Traitement des traitements de données à caractère personnel détaillés par la Clause 3.

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, la loi Informatique et Liberté du 6 janvier 1978 et le Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018.

Le Règlement Général sur la Protection des Données impose des obligations spécifiques de confidentialité, de documentation et de sécurité, au Sous-Traitant dont la responsabilité sera susceptible d’être engagée en cas de manquement.

En cas de contradiction entre les présentes dispositions et tout autre document contractuel qui régit ou pourrait régir la relation contractuelle, les présentes clauses prévalent pour tout questionnement concernant les traitements de Données à caractère personnel.

Les champs des clauses suivantes doivent obligatoirement être remplies par l’une et/ou l’autre des Parties :

* Articles 3.1, par le Mipih en tant que RT et à vérifier et corriger par le Titulaire en tant que ST.
* Article 3.2 par le Titulaire en tant que ST, vérification et correction par le Mipih en tant que RT
* Article 4.7 et 4.9 par le Titulaire en tant que ST

# Description du/des traitement(s) de données à caractère personnel

## Les traitements sous-traités :

Le Sous-Traitant est autorisé à traiter pour le compte du Responsable de Traitement, les données à caractère personnel nécessaires pour fournir les seuls services suivants :

\*RT : Lister les services concernés. Exemple : fourniture d’une messagerie.

Les traitements sont effectués pour les finalités suivantes :

\*RT : Lister les finalités des différents traitements mis en œuvre. Exemple : échange de message et pièces jointes, création d’un annuaire, mise à disposition d’un calendrier ou tous traitements mis en œuvre dans le cadre de l’utilisation de l’outil.

Les données traitées pour les finalités susmentionnées sont les suivantes :

\*RT : Lister les données collectées pour chacun des traitements.

Exemple : contenu des messages, identités des destinataires et émetteurs ; identité des personnes dans l’annuaire ; données liées aux habitudes professionnelles, donnée de localisation ou données diverses non sollicitées (ex : RDV personnels) contenues dans le calendrier, etc.

Les catégories de personnes concernées par les traitements sont :

\*RT : Lister les personnes dont les données personnelles sont traitées ex) agents du Mipih, patients, personnes externes au Mipih mais avec lesquelles nous travaillons, etc.

Les données traitées sont conservées pour les durées suivantes :

\*RT mentionner les durées de conservation à faire appliquer au ST ; ST compléter les durées de conservation qui sont appliquées en cas d’absence d’indication faite par le RT.

Exemple : Les données de connexion sont conservées un an puis supprimées (conformément à la législation en vigueur cette durée de conservation ne peut être excédée).

Pour l’exécution du service objet du présent contrat, le Responsable de Traitement met à la disposition du sous-traitant les informations suivantes :

\*RT : Lister les données qui sont mises à disposition du Sous-Traitant dans le cadre de la réalisation de ses obligations contractuelles

Exemple : adresse mail prédéterminée et attribuée à chaque collaborateur, annuaire préexistant, etc.

Ces données ne peuvent être traitées que dans le cadre des services et traitements susmentionnés et conformément aux instructions du Responsable de Traitement.

## Les traitements propres au Sous-Traitant :

En interne, le Sous-Traitant peut être amené à mettre en œuvre des traitements dans ses propres intérêts. Dans le cadre de ce marché, le Titulaire est Responsable de la mise en œuvre des traitements suivants :

\*ST : lister les finalités **et la base légale des traitements**.

Exemple : Accès à la messagerie, Opération de support, de maintenance, la collecte des données de connexion **ou toute opération liée à la gestion d’un outi**l.

L’accès à la messagerie, le support et la maintenance sont des traitements fondés sur l’article 6) §1, b), l’exécution d’une obligation contractuelle. La collecte des données de connexion est quant à elle fondée sur l’article 6, §1, c) l’obligation contractuelle de l’opérateur de messagerie.

Pour ce faire, les données traitées sont les suivantes :

\*ST : lister les données traitées.

Exemple : Données diverses dans le cadre du support, données de connexion, données d’identification pour permettre l’accès à la messagerie, etc.

Les données sont conservées pour les durées suivantes :

\*ST : préciser les durées de conservation appliquées à chaque donnée.

Les catégories de personnes concernées par ce traitement sont les suivantes :

\*ST : lister les personnes concernées par le(s) traitement(s)

Exemple : Les collaborateurs du Mipih et les personnes externes avec lesquelles nous travaillons ; les administrateurs de l’opérateur de messagerie sécurisée, etc.

Les destinataires des données traitées sont les suivants :

\*ST : Lister les destinataires des données, soit toute personne étant susceptible d’avoir accès/de traiter les données.

Exemple : une autorité de contrôle compétente ; un sous-traitant identifié pour la mise en œuvre d’un traitement spécifique, etc.

**NB : préciser l’identité et le contact DPO des sous-traitants ultérieurs.**

Le Sous-Traitant est soumis aux obligations du Responsable de Traitement, au titre du Règlement Général sur la Protection des Données, sur les traitements susmentionnés. Il est notamment tenu à une obligation d’information auprès des personnes concernées des traitements mis en œuvre.

# Obligations du Sous-Traitant vis-à-vis du Responsable de Traitement Mipih

## Traitement des données :

Le Sous-traitant s’engage à :

* Traiter les données pour les seules finalités, mentionnées dans le contrat, faisant l’objet de la sous-traitance, conformément aux instructions expresses et écrites du Responsable de Traitement. Le Sous-Traitant s’interdit de traiter les données pour ses intérêts personnels ou ceux d’un tiers ;
* Traiter les données conformément aux conditions contractuelles définies dans le présent marché ;
* Dans le strict respect de ses obligations légales et réglementaires, le Sous-Traitant peut être amené à traiter les données en dehors des instructions documentées par le Responsable de Traitement et des finalités du contrat. Dans cette hypothèse, le Sous-traitant s’engage à informer préalablement et promptement le Responsable de Traitement de l’existence et des modalités de mise en œuvre de ce traitement.

Mipih en tant que Responsable de Traitement détient seul et de manière exclusive le pouvoir de déterminer les finalités et les moyens du traitement de Données à caractère personnel dans le cadre du contrat de Sous-Traitance.

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.

Si le Sous-Traitant est tenu de procéder à un transfert de données vers un pays tiers ou une organisation internationale, sur le fondement d’une obligation légale à laquelle il est soumis, il doit en informer le Responsable de Traitement de cette obligation juridique avant la mise en en œuvre du traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d’intérêt public.

## Confidentialité des données :

Le Sous-Traitant s’engage à mettre en place toutes les mesures organisationnelles et techniques possibles et conformes à l’état de l’art, pour garantir la confidentialité des données à caractère personne traitées dans le cadre du présent contrat. Il s’engage également à garantir les données contre toute destruction accidentelle ou frauduleuse, perte accidentelle, modification, divulgation ou accès non autorisé.

Le Sous-Traitant s’engage à veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du contrat, notamment son personnel et ses sous-traitants ultérieurs soient soumis à une obligation de confidentialité au moins aussi contraignante que la sienne et reçoivent la formation nécessaire en matière de protection des données à caractère personnel.

## Protection des données :

Le Sous-Traitant s’assure de la sécurité des données, conformément à l’état de l’art, par la mise en œuvre de mesures techniques et organisationnelles listées **à l’article 4.7**.

Le Sous-Traitant s’engage à mettre en œuvre le plus haut niveau de protection dès la conception du traitement.

## Sous-traitance de troisième niveau (ou plus) ou Sous-traitance « ultérieure » :

Le Sous-Traitant n’est pas autorisé à sous-traiter à un sous-traitant ultérieur les opérations de traitement qu’il effectue pour le compte du Responsable de Traitement en vertu des présentes clauses, sans l’autorisation spécifique, écrite et préalable du Responsable de Traitement.

Le Sous-Traitant s’engage à soumettre cette autorisation, pour tout ajout ou changement de sous-traitant ultérieur, au Responsable de Traitement au moins 30 jours avant le début d’exécution de la sous-traitance ultérieure. Cette demande est accompagnée de toutes les informations nécessaires pour permettre au Responsable de Traitement de prendre une décision au sujet de l’autorisation, notamment les activités de traitement sous-traitées, l’identité et les coordonnées du sous-traitant ultérieur et les dates du contrat de sous-traitance, la localisation en Europe ou hors de l’Europe.

En cas de sous-traitance ultérieure, le Sous-Traitant reste pleinement responsable, vis-à-vis du Mipih du bon déroulement des travaux sous-traitées. Le Sous-Traitant s’engage à faire appliquer les obligations dont il a la charge au titre et selon les conditions de la Charte. Il appartient au sous-traitant de s’assurer que le sous-traitant ultérieur présente les garanties suffisantes, quant à la mise en œuvre de mesures techniques et organisationnelles appropriées, de manière à ce que le sous-traitant ultérieur réponde aux exigences du contrat et celles du Règlement européen sur la protection des données. Ces engagements et ces garanties sont formalisés par un contrat liant le Sous-Traitant au Sous-traitant ultérieur. Si le sous-traitant ultérieur ne remplit pas ses obligations, le Sous-Traitant le notifie au Responsable de Traitement, dans les plus brefs délais, et s’assure de la bonne exécution du contrat.

## Assistance au Sous-Traitant Mipih :

Le Sous-Traitant assiste le Responsable de Traitement dans l’exécution 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, droit de ne pas faire l’objet d’une décision individuelles automatisées (y compris le profilage).

Le Sous-Traitant informe le Responsable de Traitement de toute demande d’exercice de droits qui lui est adressée concernant les traitements de données à caractère personnel mentionnés par la présente, à l’adresse suivante : [dpo@mipih.fr](mailto:dpo@mipih.fr) . A moins que le Responsable de Traitement ne l’y ait expressément, spécifiquement et préalablement autorisé, le Sous-Traitant s’interdit de répondre aux demandes d’exercice de droit pour les Traitements mentionnés à la Clause 3.

Le Sous-Traitant est tenu d’assister, du mieux possible, le Responsable de Traitement dans l’exécution de ses obligations au sein du Règlement Européen sur la Protection des Données. C’est le cas notamment pour la réponse aux demandes d’exercice de droit, la réalisation d’analyse d’impact sur les données à caractère personnel, la notification d’une violation de données auprès de l’autorité compétente et/ou la personne concernée et la consultation préalable de l’autorité de contrôle si nécessaire.

## Notification des violations de données à caractère personnel :

Le Sous-Traitant notifie, par téléphone ou courrier électronique, au Responsable de Traitement toute violation de données à caractère personnel, telle que définie à l’article 1, dans un délai maximum de 48 heures après en avoir pris connaissance. Le Sous-Traitant est tenu de notifier le Responsable de Traitement que ces données soient stockées sur ses systèmes ou supports électroniques ou sur ceux de ses sous-traitants ultérieurs.

La notification décrit de manière en des termes clairs et simples la nature de la violation de Données et contient au moins les informations suivantes :

* Le nom et les coordonnées du DPO ;
* La description de la nature de la violation de Données à caractère personnel ;
* La description des conséquences probables de la violation de Données ;
* La description des mesures prises ou que la Responsable de Traitement propose de prendre pour remédier à la violation de Données, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives ;
* 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 concernées.

Si, et dans la mesure où il n’est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

Cette notification 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.

## Mesures de sécurité techniques et organisationnelles :

Le Sous-Traitant s’engage à mettre en œuvre, documenter et auditer les mesures de sécurité suivantes portant sur les données à caractère personnel et les moyens permettant de garantir la confidentialité, l’intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement.

Conformément à l’article 6, le Responsable de Traitement pourra auditer le Sous-Traitant.

Les mesures mises en œuvre sont les suivantes :

\*Le Sous-Traitant liste les mesures de sécurité appliquées spécifiquement aux traitements.

## Réversibilité des données :

Au terme de l’exécution des présentes obligations contractuelles, le Sous-Traitant s’engage à restituer l’intégralité des données, à caractère personnel ou non, traitées dans le cadre de l’exécution des traitements susmentionnés. Cette restitution se fera dans un format structuré, couramment utilisé et lisible par machine.

Cette restitution est suivie de la destruction complète et immédiate de l’ensemble des données, et de toutes copies existantes, dans le système d’information du Sous-Traitant et de ses préposés. A moins que le droit de l’Union ou le de l’Etat membre auquel le Sous-Traitant dispose expressément le contraire. Le Sous-Traitant justifie par écrit du fait et de la date de la destruction.

Dans le cadre de la destruction des données à caractères personnel de santé, le Titulaire s’engage à respecter du guide pratique « destruction de données lors du transfert de matériels informatiques des Systèmes d’Information de Santé (SIS) du corpus documentaire PGSSI-S de l’ASIP Santé.

## Délégué à la Protection des Données :

En application de l’article 37 du Règlement Européen sur la Protection des données, le Sous-Traitant informe le Responsable de Traitement de la désignation le Cliquez ou appuyez ici pour entrer une date. d’un Délégué à la Protection des Données n° Indiquez le numéro de téléphone du DPO. joignable aux adresses ci-après :

Adresse postale : Indiquez l’adresse postale du Sous-Traitant.

Adresse de messagerie : Indiquez l’adresse de messagerie du DPO du type dpo@XXX.

## Registre des catégories d’activités de traitement :

Le Sous-Traitant déclare tenir par écrit et régulièrement mettre à jour un registre des catégories d’activités de traitement effectuées pour le compte du Responsable de Traitement comprenant :

* Le nom et les coordonnées du Responsable de Traitement, des éventuels sous-traitants et le cas échéant du DPO ;
* Les catégories de traitements effectués pour le compte du Responsable de Traitement ;
* Les transferts de données à caractère personnel vers un pays tiers ou une organisation internationale, y compris l’identification de ce pays tiers ou de cette organisation internationale et, dans le cas de transferts visés à l’article 49 § 1 alinéa 2 du RGPD les documents attestant de l’existence de garanties appropriées ;
* Une description des mesures de sécurité techniques et organisationnelles mises en œuvre.

De manière générale, le Sous-Traitant s’engage à mettre à disposition du Responsable de Traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent Contrat et dues au titre du Règlement Général sur la Protection des Données.

# Obligations du Responsable de Traitement vis-à-vis du Sous-Traitant

Le Responsable de Traitement s’engage à :

* Fournir au Sous-Traitant les données strictement nécessaires à la réalisation des traitements, pour la durée d’exécution du contrat ;
* *Fournir l’information aux personnes concernées par les opérations de traitement au moment de la collecte des données* ;
* Documenter par écrit toute instruction concernant le traitement de données par le Sous-Traitant ;
* 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 ;
* Superviser le traitement, y compris réaliser les audits et les inspections auprès du Sous-Traitant.

# Audit

Conformément à l’article 28 du RGPD, le Sous-Traitant fournira au Responsable de Traitement les documentations raisonnablement exigibles et pertinentes démontrant sa conformité quant aux obligations lui incombant au titre des Clauses Contractuelles de Traitement de Données.

Le Client ou l’un de ses mandataires peut auditer, dans la limite de 2 fois par an, la conformité du sous-traitant au regard des dispositions des Clauses Contractuelles de Traitement de Données en cas de doute raisonnable relatif à un quelconque manquement auxdites dispositions.

L’audit devra être réalisé au cours des heures normales d’ouverture sur le site concerné, il sera soumis aux règles internes du Sous-Traitant précisées en Annexe II, et il ne devra pas perturber de manière excessive les activités de celui-ci. Tous les frais associés aux audits sont à la charge de la personne ayant eu l’initiative de l’audit.

Cet audit est notifié par le Responsable de Traitement par Lettre Recommandée avec Accusé de Réception détaillant les documents demandés et, et le cas échéant, le protocole qui sera déroulé, les méthodes utilisées et données auditées, 30 jours ouvrés avant la date projetée de sa mise en œuvre.

Le Sous-Traitant s’engage à faire preuve de bonne foi notamment à mettre à disposition du Responsable de Traitement la documentation demandée et nécessaire pour permettre la réalisation d’un audit sur pièce ou d’un audit sur place et contribuer, de bonne foi et tout du long, à l’audit.

L’audit est effectué par le Responsable de Traitement ou par un tiers désigné par lui, à la triple condition que ce tiers ne soit pas un concurrent direct ou indirect du Sous-Traitant, qu’il soit soumis au secret professionnel et qu’il ait conclu un accord de confidentialité.

Les résultats d’audit feront l’objet d’un débat contradictoire et d’une validation par les Parties. Les rapports d’audit et toutes données, personnelles ou non, auditées sont considérées comme des informations confidentielles des Parties et sont donc soumises à l’engagement de confidentialité intégré au corpus contractuel du présent marché.