Formulaire

**Annexe RGPD - traitement en UE**

***ENTÊTE RÉSERVÉE : MERCI DE NE RIEN INSCRIRE***

*Pour information :*

* ***Le texte apparaissant sous ce format (violet italique souligné en pointillé) n’est là que pour aider à compléter les différentes rubriques, et est à supprimer de la version finale.***
* *Le texte [entre crochets et surligner en jaune] est à remplir par le responsable de traitement, et le co-responsable de traitement si nécessaire*
* *Le texte [entre crochets et surligner en vert] est à compléter par le sous-traitant ou le co-responsable de traitement*

Cette Annexe décrit le cadre d’échange de données entre les parties pour l’exécution de [à compléter par le titre de la prestation / du contrat / de l’étude ou autre].

**Partie I – DESCRIPTION DU TRAITEMENT**

# Les parties

**Responsable de traitement** : [indiquer le nom du responsable de traitement]

Représenté, dans le cadre de ce traitement, par : [responsable de la prestation / du contrat / de l’étude] *Le responsable de traitement est la personne morale ou physique qui définit les finalités et les moyens du traitement (les objectifs, quelles données et comment).*

Correspondant local du traitement : [Indiquer la fonction du correspondant local du traitement]

*Le correspondant local est la personne qui met en place la partie opérationnelle du traitement au niveau de l’établissement, interlocuteur local : métier et/ou DTNIB (fonction de la personne + nom si possible), c’est la ou les personnes qui gèrent ce traitement de données au quotidien.*

Retirer le paragraphe ci-dessous sur la co-responsabilité si non concernée

**Co-responsable de traitement** : [indiquer le nom du co-responsable de traitement]

Représenté, dans le cadre de ce traitement, par : [responsable de la prestation / du contrat / de l’étude]

Correspondant local du traitement : [Indiquer la fonction du correspondant local du traitement]

*Le correspondant local est la personne qui met en place la partie opérationnelle du traitement au niveau de l’établissement, interlocuteur local : métier et/ou DTNIB (fonction de la personne + nom si possible), c’est la ou les personnes qui gèrent ce traitement de données au quotidien.*

*Spécificité pour les contrats passés pour le GHT :*

*Co-responsables de traitement : tous les établissements du GHT Sud Lorraine*

*Représentés par leur Directeur Général*

*Représentés, dans le cadre de ce traitement, par chacun des responsables de la mise en place de la prestation au sein de chaque établissement concerné du GHT : préciser la fonction de ces personnes si connues*

Et / ou

**Sous-traitant du traitement de la donnée** : [indiquer le nom du sous-traitant]

Représenté, dans le cadre de ce traitement, par : [responsable de la prestation / du contrat / de l’étude]

L’interlocuteur privilégié *(*personne à contacter*/responsable de la prestation sur site)* :

# Finalités du traitement

[Décrire les objectifs de la prestation / du projet / de l’étude, sous-traités et/ou co-traités]

# Base légale du traitement

[Indiquer la base légale sur lequel repose le traitement.]

☐ Exécution de mesures contractuelles

☐ Obligation légale

☐ Sauvegarde des intérêts vitaux de la personne concernée ou d’une autre personne physique

☐ Exécution d’une mission d’intérêt public ou relevant de l’exercice de l’autorité publique *(préciser la mission d’intérêt public)*

☐ Intérêt légitimes poursuivis par le responsable de traitement ou par un tiers *(préciser l’intérêt légitime poursuivi)*

☐ Consentement

***NB : Dans la majorité du temps, pour le CHRU, la base légale est l’intérêt légitime poursuivi par l’établissement de mettre en place un outil lui permettant de … (à compléter par le responsable de traitement)***

*Si la base légale varie en fonction des finalités, il est nécessaire d’indiquer, les différentes bases légales pour chacune des finalités sous-traitées.*

*Rappel :*

*Pour être licite un traitement de données doit reposer sur un fondement, c’est-à-dire répondre à l’une des conditions énoncées dans l’article 6 du RGPD. Le traitement est nécessaire :*

* *à l’exécution d’un contrat auquel la personne concernée est partie ou à l’exécution de mesures précontractuelles prises à sa demande =>* ***Contrat***
* *au respect d’une obligation légale s’imposant au responsable de traitement =>* ***Obligation légale***
* *à la sauvegarde de la vie de la personne concernée ou d’une autre personne =>* ***Intérêt vitaux***
* *à l’exécution d’une mission d’intérêt public ou relevant de l’exercice de l’autorité publique dont est investi le responsable du traitement =>* ***Intérêt public***
* *Aux fins des intérêts légitimes poursuivis par le responsable de traitement ou par un tiers, à moins que ne prévalent les intérêts ou libertés et droits fondamentaux de la personne concernée =>* ***Intérêt légitime***
* *En dernier recours, si on n’est dans aucun des cadres listés ci-dessus, la personne concernée doit consentir au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques =>* ***Consentement***

*NB : Si la base légale du traitement est le consentement, celui-ci devra être demandé et donné de façon :*

* *Libre : la personne concernée doit pouvoir être livre de refuser ou de retirer son consentement,*
* *Spécifique : pour une finalité précise et des sous-finalités précises,*
* *Éclairé : la personne concernée doit avoir été informée préalablement de toutes les informations liées au traitement de ses données (qui, quoi, comment, pourquoi, où),*
* *Univoque : le consentement doit être donnée pour un acte positif clair, une seule et unique interprétation possible*

# Activité(s) sous-traitée(s)

[Détailler les activités qui sont confiées au sous-traitant et/ou au co-traitant concernant le traitement de données.]

*Exemples de types d’activité à détailler :*

* *Collecte de données*
* *Consultation*
* *Information des personnes concernées*
* *Analyses de données*
* *Transferts de données*
* *Suppression de données*
* *Réassemblages de données*
* *Tri de données*
* *Enregistrement*
* *Hébergement*
* *Etc…*

*Vous pouvez ajouter cette phrase pour les contrats faisant l’objet d’un CCTP :*

*Les activités confiées au sous-traitant et/ou au co-traitant sont précisées dans le CCTP et/ou les marchés subséquents.*

*Vous pouvez ajouter cette phrase pour les contrats faisant l’objet d’un protocole :*

*Les activités confiées au sous-traitant et/ou au co-traitant sont précisées dans le protocole de l’étude.*

# Données personnelles traitées et catégories de personnes concernées

## Données personnelles traitées

*Ne pas oublier les données des professionnelles nécessaires à la bonne exécution du contrat si concernées.*

*Attention à ne pas être trop précis, ici il est question de catégories de données, cela évitera une mise à jour du document dans le cas d’une légère modification des données d’une même catégorie par la suite.*

*Si nécessaire, les sous-traitants et co-responsables de traitement veilleront à compléter ou corriger les catégories de données indiquées ci-après.*

* Données à caractère personnel

|  |  |
| --- | --- |
| **Type de données** | **Description (inventaires des données concernées)** |
| Relatives à l’identité | [inventaire des données concernées : nom, prénom, etc.] |
| Relatives à la vie personnelle  *(hors données de santé)* | [inventaire des données concernées : habitudes de vie, etc.] |
| Relatives à la vie professionnelle | [inventaire des données concernées : emploi, grade, etc.] |
| Informations économiques | [inventaire des données concernées : salaire, RIB, etc.] |
| Localisation et connexion | [inventaire des données concernées : log, etc.] |
| Enregistrements d’images et de voix  *(hors données de santé)* | [inventaire des données concernées : photo, etc.] |
| Autres données | [inventaire des données concernées] |

*Préciser « non concerné » si nécessaire pour confirmer que ce n’est pas un oubli*

* Données sensibles

|  |  |
| --- | --- |
| **Type de données** | **Description (inventaires des données concernées)** |
| Origine raciale ou ethnique | [inventaire des données concernées : ethnie, etc.] |
| Opinions politiques | [inventaire des données concernées : vote, etc.] |
| Convictions religieuses ou philosophiques | [inventaire des données concernées : religion, etc.] |
| Appartenance syndicale | [inventaire des données concernées : syndicat, etc.] |
| Données génétiques | [inventaire des données concernées : génotype, etc.] |
| Données biométriques | [inventaire des données concernées : empruntes, etc.] |
| Données concernant la vie sexuelle ou l'orientation sexuelle | [inventaire des données concernées : bisexualité, etc.] |
| Données judiciaires | [inventaire des données concernées : incarcération, etc.] |
| Numéro d'identification national (NIR) | [inventaire des données concernées : n°sécu, etc.] |
| Données de santé | [inventaire des données concernées : IRM, maladie, etc.] |
| Aucune |  |

*Préciser « non concerné » si nécessaire pour confirmer que ce n’est pas un oubli*

## Catégories de personnes concernées

☐ Patients mineurs (âge < 15 ans)

☐ Patients mineurs (âge >= 15 ans)

☐ Patients majeurs

☐ Professionnels de l’établissement : *préciser le ou les établissement(s)*

☐ Bénévoles, Intérimaires, prestataires, fournisseurs

☐ Etudiants (internes, stagiaires, etc.)

☐ Pairs (relations dans le cadre d’un processus de santé : par exemple, professionnels de santé en réseau, etc…)

☐ Administrations/ organismes officiels

☐ Autre, merci de préciser :

Précisions sur les catégories de personnes concernées :

[Indiquez, par exemple, si cela concerne uniquement une catégorie particulière de personnes concernées.]

*Exemple : les personnes atteintes de la maladie d’Alzheimer, les personnels intervenants dans la prise en charge des malades d’Alzheimer, etc.*

## Durée de conservation des données

[Préciser la durée de conservation des données par le sous-traitant. Si non connue indiquer les critères utilisés pour déterminer la durée].

[On doit préciser si les données sont supprimées par le sous-traitant ou restituées au RT avant destruction de toutes les données détenues par le sous-traitant.]

*La durée de conservation des données correspond à la durée la plus courte entre la durée du contrat liant les parties et la durée de conservation réglementaire applicable à la donnée.*

A l’échéance du contrat, le sous-traitant restituera les données sans en garder copie ou les détruira, selon les consignes du CHRU, et fournira au CHRU une preuve de destruction. A défaut de fournir la preuve de destruction ou de restitution intégrale des données, le sous-traitant sera réputé les avoir détruites et dégagera le CHRU de toutes responsabilités pouvant faire suite à un mésusage des données, sauf si le sous-traitant démontre que ce mésusage a pour origine la propre négligence du CHRU.

# Co-responsabilité de traitement : répartition des responsabilités

*Retirer le paragraphe 6 si non concerné.*

[Tableau à compléter conjointement par les co-responsables de traitement – Ajouter toutes les précisions utiles]

|  |  |  |  |
| --- | --- | --- | --- |
| **Responsabilités** | **CHRU de Nancy** | **Etablissements du GHT** | **[Identifier la partie]** |
| Déterminer les finalités |  |  |  |
| Déterminer les moyens |  |  |  |
| Collecter les données |  |  |  |
| Garantir le recueil du consentement si concerné |  |  |  |
| Déterminer les durées de conservation des données traitées |  |  |  |
| Informer les personnes concernées |  |  |  |
| Répondre aux demandes de droits d’accès |  |  |  |
| Donner l’instruction de traiter les données au sous-traitant |  |  |  |
| Veiller à la conformité du sous-traitant |  |  |  |
| Réaliser l’AIPD**\*** si nécessaire |  |  |  |
| Etre le point de contact de l’autorité de contrôle |  |  |  |
| Notification de violation des données à l’autorité de contrôle |  |  |  |
| Notification de violation des données aux personnes concernées |  |  |  |
| Autre : |  |  |  |

\*AIPD : Analyse d’Impact sur la Vie Privée

# Mesures de sécurité mises en place par le sous-traitant / co-responsable de traitement

**2 choix possibles. Supprimer le cas qui ne s’applique pas à votre contrat**

**Cas 1 : tous les contrats hors recherche en santé** (le tableau de mesures ci-après est bien à retirer si on retient le cas 1)

En tant que sous-traitant (ou co-responsable de traitement, si concerné) de la donnée, le sous-traitant s’engage à respecter, a minima, les mesures de sécurité techniques et organisationnelles requises dans les Exigences SSI à destination des fournisseurs du CHRU de Nancy, annexées au CCAP du présent contrat.

***Cas 2 : Pour les actes juridiques spécifiques à la recherche***

En tant que sous-traitant (ou co-responsable de traitement, si concerné) de la donnée, le partenaire, s’engage à respecter, a minima, les mesures de sécurité techniques et organisationnelles requises dans les Exigences SSI à destination des partenaires du CHRU de Nancy dans le cadre de la recherche en santé (GUI-0076), listées ci-dessous.

| **Types de mesures** | **Précisions** |
| --- | --- |
| Organisation de la sécurité de l’information | * L’organisme met en œuvre une organisation de sécurité de l’information et alloue les ressources nécessaires à la définition des responsabilités, au cloisonnement des tâches, à la mise en œuvre des actions de sécurité physiques et logiques. * L’organisme s’engage sur les mesures nécessaires à la sécurisation des postes de travail (antivirus à jour, pare-feu, etc.) et des équipements mobiles utilisés par ses personnels et ses sous-traitants afin que ces équipements ne constituent pas un vecteur d’atteinte à la sécurité de l’information ; notamment par une limitation de l’accès aux données (chiffrement des équipements, verrouillage automatique de session, etc.) |
| La sécurité des ressources humaines | * L’organisme s’engage à s’assurer que les personnels affectés aux projets ont les niveaux de connaissances et de compétences techniques requis pour la réalisation des tâches qui leurs sont confiées. * L’organisme veille à faire respecter les règles de sécurité et de confidentialité avant le démarrage des services, en faisant signer un accord de confidentialité ou en prévoyant une clause dans le contrat de travail. * Les obligations de l’accord de confidentialité doivent s’étendre au-delà de la fin de la prestation contractuelle. |
| Gestion des actifs | * L’organisme protège la confidentialité des données sur les médias amovibles et lors des transferts à des tiers autorisés. * Au terme de l’utilisation d’un matériel informatique par l’organisme (notamment en cas de mise au rebut, vente réattribution ou recyclage) utilisé et plus particulièrement pour les matériels de stockage, aucune donnée ne doit rester sur celui-ci qui pourrait entrainer la divulgation d’informations. |
| Contrôle d’accès | * L’organisme établit une politique de contrôle sur la base des enjeux de sécurité et en définissant des profils d’habilitations. * L’organisme met en place des procédures formelles pour contrôler les droits d’accès aux systèmes et services d’information couvrant tout le cycle de vie de l’accès utilisateur, incluant une revue au minimum annuelle des droits et des compte d’accès. * L’organisme met en œuvre :   + les moyens nécessaires pour garantir l’unicité des identités des utilisateurs ;   + une politique de mot de passe utilisateur conforme aux recommandations de l’ANSSI ;   + une limitation du nombre de tentatives d’accès présentant un authentifiant erroné. * L’organisme met en œuvre un dispositif de séparation garantissant l’étanchéité des environnements utilisateurs et des données dans les environnements support et sous toutes leurs formes (stockage, mémoire, transmission, etc.). * L’organisme différencie l’interface d’administration de l’interface permettant l’accès des utilisateurs finaux. |
| Cryptographie | * L’organisme met en œuvre des méthodes de chiffrement basés sur des standards publics éprouvés, à l’état de l’art, permettant à toute donnée d’être transmise de façon sécurisée. |
| Sécurité physique et environnementale | * Des périmètres de sécurité sont définis et utilisés pour protéger les zones contenant l’information sensible. * L’organisme applique des mesures de sécurité physique aux bureaux, aux salles et aux équipements, en particulier pour se protéger des désastres naturels, d’attaques malveillantes ou d’accidents. |
| Sécurité liée à l’exploitation | * L’organisme met en œuvre et contrôle les procédures d’exploitation, en particulier celles relatives à la mise à jour des systèmes, aux applications, aux processus d’administration, de développement et de sécurité des développements, à la séparation des environnements de test, de recette et de production. * L’organisme met en œuvre des systèmes de détection pour faciliter la détection rapide, l’investigation et la résolution des incidents de sécurité ; notamment des solutions de lutte contre les codes malveillants. * L’organisme installe les correctifs logiciels le plus tôt possible sur ses applications et ses systèmes. * Une politique de sauvegarde des données est définie précisant la fréquence et durée de rétention. * Les sauvegardes des données stockées sur les moyens de l’organisme sont sous sa responsabilité. * L’organisme mène des tests de restauration réguliers. * Les données sauvegardées à l’extérieur sont au préalable chiffrées. |
| Sécurité des communications | * L’organisme limite les flux réseau au strict nécessaire en filtrant les flux entrants/sortants sur les équipements (pare-feu, proxy, serveurs, etc.). * L’organisme limite les accès Internet en bloquant les services non nécessaires. * Les réseaux Wi-Fi utilisent un chiffrement à l’état de l’art (WPA2 ou WPA2-PSK) et les autres réseaux ouverts aux invités sont séparés du réseau interne. * L’organisme impose un VPN pour l’accès à distance et s’assure qu’aucune interface d’administration n’est accessible directement depuis Internet. * L’organisme met en œuvre la version la plus récente du protocole TLS sur tous les sites web et rend son utilisation obligatoire pour toutes les pages d’authentification, de formulaire ou sur lesquelles sont affichées ou transmises es données à caractère personnel non publiques. * Les pièces sensibles transmises via la messagerie électronique sont chiffrées et la clé de chiffrement est transmise via un canal distinct (par exemple par SMS). |
| Conformité | * L’organisme a mis en place et maintient un plan et processus de contrôle en matière de sécurité de l’information. |
| Gestion des incidents liés à la sécurité de l’information | * L’organisme s’impose la mise en place d’un processus de gestion des incidents. * L’organisme garde un journal avec la description de l’incident et des données compromises (si connues), les coordonnées du déclarant et de la personne à qui l’incident a été communiqué, les mesures prises pour le résoudre (personnes en charge et les données qui ont pu être récupérées), les éventuelles conséquences (pertes, divulgation, altération) qui en ont résulté |
| Aspects de la sécurité de l’information dans la gestion de la continuité de l’activité | * Des moyens de traitement de l’information doivent être mis en œuvre avec suffisamment de redondances pour répondre aux exigences de disponibilités. |

# Sous-traitant ultérieur et transferts internationaux

## Liste des sous-traitants ultérieurs

*[Le responsable de traitement doit indiquer ici* ***s’il autorise ou non****, le recours à la sous-traitance ultérieure.*

*S’il interdit le recours à la sous-traitance ultérieur, il précise également que la clause n°2.7 de la deuxième partie de la présente annexe ne s’applique pas.*

*Si le responsable de traitement autorise le recours à la sous-traitance ultérieur, il précise ici sous quelle modalité (choix entre option 1 et 2 de la clause n°2.7 de la deuxième partie de la présente annexe).]*

*[Listes exhaustives des sous-traitants ultérieurs. Si pas de sous-traitant ultérieur le préciser pour confirmer que ce n’est pas un oubli.]*

|  |  |  |  |
| --- | --- | --- | --- |
| **Sous-traitant** | **Activités sous-traitées** | **Données sous-traitées** | **Lieu d’hébergement / de transfert** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Mesures de sécurité mises en place pour les transferts internationaux

*[Le responsable de traitement doit indiquer ici* ***s’il autorise ou non****, les transferts internationaux pour la sous-traitance ultérieure.*

*S’il interdit les transferts internationaux, il précise également que la clause n°2.8 de la deuxième partie de la présente annexe ne s’applique pas.]*

*[A compléter obligatoirement en cas de transferts internationaux]*

*Si pas de transferts internationaux le préciser pour confirmer que ce n’est pas un oubli.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sous-traitant** | **Activités transférées** | **Données transférées** | **Lieu d’hébergement / de transfert** | **Garanties mises en place** |
|  |  |  |  | *Clauses contractuelles types et autres mesures complémentaires à détailler* |

# Contact pour la protection des données

## Pour les responsables de traitement

[A compléter obligatoirement en précisant le nom des parties en cas de co-responsabilité de traitement]

*Pour un contrat passé par les établissements du GHT : dpo@chru-nancy.fr*

## Pour le sous-traitant

[A compléter obligatoirement]

*Si le sous-traitant n’a pas désigné de délégué à la protection des données (DPO), un contact doit néanmoins être renseigné.*

# Partie II – OBLIGATIONS DES PARTIES

**Clause 1**

**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 du traitement, sont précisés en première partie de cette annexe RGPD.

**Clause 2**

**Obligations des parties**

1. ***Instructions***
2. Le sous-traitant ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, à moins qu’il ne soit tenu d’y procéder en vertu du droit de l’Union ou du droit de l’Etat membre auquel il est soumis. Dans ce cas, le sous-traitant informe le responsable du 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 donnée ultérieurement par le responsable du traitement pendant toute la durée du traitement des données à caractère personnel. Ces instructions doivent toujours être documentées.
3. Le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction donnée par le responsable du traitement 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 Etats membres relatives à la protection des données.
4. ***Limitation de la finalité***
5. Le sous-traitant traite les données à caractère personnel uniquement pour la ou les finalités spécifiques du traitement, telles que définies au §2 en première partie de la présente annexe RGPD, sauf instruction complémentaire du responsable de traitement.
6. Coresponsabilité de traitement

Le coresponsable de traitement s’engage à traiter les données uniquement pour la ou les seule(s) finalité(s) déterminées dans le présent contrat. En outre, si un coresponsable de traitement est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l’Union ou du droit de l’Etat membre auquel il est soumis, il doit informer le ou les responsable(s) conjoint(s) concerné(s) de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d’intérêt public.

1. ***Durée du traitement des données à caractère personnel***

Le traitement par le sous-traitant n’a lieu que pendant la durée du contrat.

1. ***Sécurité du traitement***
2. Le sous-traitant met au moins en œuvre les mesures techniques et organisationnelles précisées au §6 en première partie de la présente annexe RGPD 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.
3. 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.
4. Coresponsabilité de traitement

Le coresponsable de traitement s’engage à garantir la confidentialité et la sécurité des données à caractère personnel traitées. A ce titre, le coresponsable de traitement s’engage à :

1. ne pas divulguer à des tiers, à titre gratuit ou onéreux, et sous quelque forme que ce soit, les données à caractère personnel traitées ;
2. prendre toutes les mesures pour que lesdites données ne puissent être accessibles à d’autres personnes que les personnels attachés à leur traitement et à leur analyse. Ces derniers seront sensibilisés au caractère stratégique des données confiées et liés au coresponsable de traitement par un engagement de confidentialité ;
3. ne pas procéder à des copies, utilisations ou diffusions de partie ou totalité d’un fichier et/ou d’une donnée à l’exception des copies, utilisations ou diffusions nécessaires aux opérations de traitements réalisées sur les données décrites dans la présente convention ;
4. informer les autres parties concernées de toute réception par lui d’une mise en demeure, réquisition ou requête judiciaire, de toute enquête ou toute autre notification relative à la réalisation des prestations ;
5. assurer le chiffrement des informations présentes sur ses équipements utilisés ou transportés ors de ses locaux, comportant des données à caractère personnel, avec un logiciel de chiffrement à l’état de l’art.
6. ***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.

1. ***Documentation et conformité***
2. Les parties doivent pouvoir démontrer la conformité avec les présentes clauses.
3. Le sous-traitant traite de manière rapide et adéquate les demandes du responsable de traitement concernant le traitement des données conformément aux présentes clauses.
4. Le sous-traitant met à la disposition du responsable du traitement 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. A la demande du responsable du 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 du traitement peut tenir compte des certifications pertinentes en possession du sous-traitant.
5. Le responsable du traitement 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 sous-traitant et sont, le cas échéant, effectués moyennant un préavis raisonnable.
6. 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. ***Recours à des sous-traitants ultérieurs***
8. **OPTION 1** : AUTORISATION SPECIFIQUE PREALABLE : 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 du traitement en vertu des présentes clauses sans l’autorisation écrite spécifique préalable du responsable du traitement. Le sous-traitant soumet la demande d’autorisation spécifique au moins quinze (15) jours avant le recrutement du sous-traitant ultérieur en question, ainsi que les informations nécessaires pour permettre au responsable du traitement de prendre une décision au sujet de l’autorisation. La liste des sous-traitants ultérieurs autorisés par le responsable du traitement figure au §7 en première partie de la présente annexe, que les parties tiennent à jour.

**OPTION 2** : AUTORISATION ECRITE GENERALE : le sous-traitant dispose de l’autorisation générale du responsable du traitement pour ce qui est du recrutement de sous-traitants ultérieurs sur la base d’une liste convenue. Le sous-traitant informe spécifiquement par écrit le responsable du traitement de tout projet de modification de cette liste par l’ajout ou le remplacement de sous-traitants ultérieurs au moins quinze (15) jours à l’avance, donnant ainsi au responsable du traitement suffisamment de temps pour pouvoir s’opposer à ces changements avant le recrutement du ou des sous-traitants ultérieurs concernés. Le sous-traitant fournit au responsable du traitement les informations nécessaires pour lui permettre d’exercer son droit d’opposition.

1. Lorsque le sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement), 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 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 et/ou du règlement (UE) 2018/1725.
2. A la demande du responsable du 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.
3. Le sous-traitant demeure pleinement responsable, à l’égard du responsable du 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 du traitement de tout manquement du sous-traitant ultérieur à ses obligations contractuelles.
4. 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 du 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.
5. Coresponsabilité de traitement
6. Le coresponsable de traitement peut faire appel à un sous-traitant pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit les autres responsables conjoints de tout changement envisagé concernant l’ajout ou le remplacement d’autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l’identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Les autres responsables conjoints du traitement disposent d’un délai minimum de quinze (15) jours à compter de la date de réception de cette information pour présenter leurs objections. Cette sous-traitance ne peut être effectuée que si les autres responsables conjoints de traitement n’ont pas émis d’objection pendant le délai susvisé.
7. Il appartient alors au coresponsable de traitement de s’assurer que le sous-traitant présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manières à ce que le traitement réponde aux exigences du règlement européen sur la protection des données. Si le sous-traitant ne remplit pas ses obligations en matière de protection des données, le coresponsable de traitement demeure pleinement responsable devant les autres responsables conjoints de traitement de l’exécution par le sous-traitant de ses obligations.
8. ***Transferts internationaux***
9. Tout transfert de données vers un pays tiers ou une organisation internationale par le sous-traitant n’est effectuée que sur la base d’instructions documentées du responsable du traitement ou afin de satisfaire à une exigence spécifique du droit de l’Union ou du droit de l’Etat membre à laquelle le sous-traitant est soumis et s’effectuée conformément au chapitre V du règlement (UE) 2016/679 ou du règlement (UE) 2018/1725.
10. Le responsable du traitement convient que lorsque le sous-traitant recrute un sous-traitant ultérieur conformément à la clause2.7 pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement) 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 sous-traitant 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 3**

**Assistance au responsable de traitement**

1. Le sous-traitant informe sans délai le responsable du traitement 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 responsable de traitement des données ne l’y ait autorisé.
2. Le sous-traitant prêt 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.
3. Outre l’obligation incombant au sous-traitant d’assister le responsable du traitement en vertu de la clause 3, 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 :
4. l’obligation de procéder à une évaluation de l’incidence des opérations de traitement envisagées sur la protection des données à caractère personne (« 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 ;
5. 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 ;
6. 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 ;
7. 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.

**Clause 4**

**Notification de violations de données à caractère personnel**

En cas de violation de données à caractère personnel, le sous-traitant coopère avec le responsable du 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 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 sous-traitant.

1. ***Violation de données en rapport avec des données traitées par le responsable du traitement***

En cas de violation de données à caractère personnel en rapport avec des données traitées par e responsable du traitement, le sous-traitant prête assistance au responsable du 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 du 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 et l’article 34, paragraphe 3, du règlement (UE) 2018/1725, doivent figurer dans la notification du responsable du traitement, 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 responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

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 et l’article 35 du règlement (UE) 2015/1725, 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.
2. ***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 du traitement dans les meilleurs délais après en avoir pris connaissance. Cette notification 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.

Les parties définissent en première partie de l’annexe RGPD tous les autres éléments que le sous-traitant doit communiquer lorsqu’il prête assistance au responsable du traitement aux fins de la satisfaction des obligations incombant à ce dernier en vertu des articles 33 et 34 du règlement (UE) 2016/679 et des articles 34 et 35 du règlement (UE) 2018/1725.

**Clause 5**

**Non-respect des clauses et résiliation**

1. Sans préjudice des dispositions du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725, en cas de manquement du sous-traitant aux obligations qui lui incombent en vertu des présentes clauses, le responsable du traitement peut donner instruction au sous-traitant 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 sous-traitant informe rapidement le responsable du traitement s’il n’est pas en mesure de se conformer aux présentes clauses, pour quelque raison que ce soit.
2. Le responsable du traitement 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 sous-traitant a été suspendu par le responsable du traitement 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 sous-traitant 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 sous-traitant 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.
3. Le sous-traitant est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel en vertu de présentes clauses lorsque, après avoir informé le responsable du traitement que ses instructions enfreignent les exigences juridiques applicables conformément à la clause 2.1, point b), le responsable du traitement insiste pour que ses instructions soient suivies.
4. A la suite de la résiliation du contrat, le sous-traitant supprime, selon le choix du responsable du traitement, toutes les données à caractère personnel traitées pour le compte du responsable du traitement et certifie auprès de celui-ci qu’il n’a procédé à cette suppression, ou renvoie toutes les données à caractère personnel au responsable du traitement 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 sous-traitant continue de veiller à la conformité aux présentes clauses jusqu’à la suppression ou à la restitution des données.