Clausier - Gestion des tiers

Contexte

L’objectif de ce clausier de gestion des tiers est de formaliser les droits et obligations réciproques entre les établissements du GHT Centre Manche et les tiers intervenants sur le Système d’Information (SI) ou ayant accès à ses ressources, pour maîtriser les risques de sécurité, juridiques et réglementaires liés à ces relations.

Objectifs cibles :

* Garantir le respect des exigences de sécurité, confidentialité et conformité (cadre RGPD)
* Définir les responsabilités, devoirs, obligations et droits de chaque partie
* Encadrer la traçabilité et l’auditabilité des actions et accès des tiers
* Faciliter la gestion des incidents, la continuité d’activité et la réversibilité contractuelle

Catégories de tiers concernés

* Prestataires informatiques (infogérance, éditeurs de logiciels, support technique)
* Sous-traitants (maintenance, externalisation de services)
* Intervenants techniques externes (dépannage matériel/logiciel, auditeurs de sécurité)
* Consultants, formateurs, temporaires
* Partenaires, fournisseurs, hébergeurs
* Toute personne extérieure accédant physiquement ou logiquement au SI

**Parties :**

[Contexte 1](#_Toc215558680)

[1 SECTION I - Clauses RGPD 2](#_Toc215558681)

[2 SECTION II – ACCES AU SYSTEME D’INFORMATION 8](#_Toc215558682)

[3 SECTION III - DISPOSITIONS FINALES 12](#_Toc215558683)

[4 ANNEXE I - Liste des parties 13](#_Toc215558684)

[5 ANNEXE II - Description du traitement 14](#_Toc215558685)

[6 ANNEXE III - Mesures techniques et organisationnelles, visant à garantir la sécurité des données 15](#_Toc215558686)

[7 ANNEXE IV - Liste de sous-traitants ultérieurs 16](#_Toc215558687)

# SECTION I - Clauses RGPD

Cette partie est optionnelle mais doit être précisée si elle est applicable

**Application des clauses RGPD dans le cadre de l’exécution des missions entre le GHT Centre Manche et le Tiers.**

## Objet et champ d’application

Les présentes clauses contractuelles types (ci-après les « clauses ») ont pour objet de garantir la conformité avec 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 énumérés à l’annexe I ont accepté ces clauses afin de garantir le respect des dispositions de l’article 28, paragraphes 3 et 4, du règlement (UE) 2016/679Les présentes clauses s’appliquent au traitement des données à caractère personnel tel que décrit à l’annexe II.

Les annexes I à IV font partie intégrante des clauses.

## Invariabilité des clauses

Les parties s’engagent à ne pas modifier les clauses, sauf en ce qui concerne l’ajout d’informations aux annexes ou la mise à jour des informations qui y figurent.

Les parties ne sont pour autant pas empêchées d’inclure les clauses contractuelles types définies dans les présentes clauses dans un contrat plus large, ni d’ajouter d’autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les clauses ou qu’elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées.

## Hiérarchie

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

## Clause d’amarrage (facultative)

Toute entité qui n’est pas partie aux présentes clauses peut, avec l’accord de toutes les parties, y adhérer à tout moment, en qualité soit de responsable du traitement soit de sous-traitant, en complétant les annexes et en signant l’annexe I.

Une fois que les annexes mentionnées au point a) sont complétées et signées, l’entité adhérente est considérée comme une partie aux présentes clauses et jouit des droits et est soumise aux obligations d’un responsable du traitement ou d’un sous-traitant, conformément à sa désignation à l’annexe I.

Les présentes clauses ne créent pour la partie adhérente aucun droit ni aucune obligation pour la période précédant l’adhésion.

## 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 à l’annexe II.

## Obligations des parties

Instructions

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’État 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 données ultérieurement par le responsable du 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 du traitement si, selon lui, une instruction donnée par le responsable du traitement constitue une violation du règlement (UE) 2016/679 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 II, sauf instruction complémentaire du responsable du traitement.

Durée du traitement des données à caractère personnel

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

Sécurité du traitement

Le sous-traitant met au moins en oeuvre les mesures techniques et organisationnelles précisées à l’annexe III pour assurer la sécurité des données à caractère personnel. Figurent 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 oeuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques pour les personnes concernées. 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.

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.

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 du traitement concernant le traitement des données conformément aux présentes clauses.

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. À 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.

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.

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.

Recours à des sous-traitants ultérieurs

AUTORISATION SPÉCIFIQUE PRÉALABLE : 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 ……..……… [PRÉCISER LA DURÉE] 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 à l’annexe IV, que les parties tiennent à jour.

Transferts internationaux

Tout transfert de données vers un pays tiers ou une organisation internationale par le sous-traitant n’est effectué 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’État membre à laquelle le sous-traitant est soumis et s’effectue conformément au chapitre V du règlement (UE) 2016/679.

Le responsable du traitement convient que lorsque le sous-traitant recrute un sous-traitant ultérieur conformément à la clause 7.7 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.

## Assistance au responsable du 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. 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 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 :

1. l’obligation de procéder à une évaluation de l’incidence des opérations de traitement envisagées sur la protection des données à caractère personnel («analyse d’impact relative à la protection des données») lorsqu’un type de traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques;
2. l’obligation de consulter l'autorité de contrôle compétente/les autorités de contrôle compétentes préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque;
3. l’obligation de veiller à ce que les données à caractère personnel soient exactes et à jour, en informant sans délai le responsable du traitement si le sous-traitant apprend que les données à caractère personnel qu’il traite sont inexactes ou sont devenues obsolètes;
4. les obligations prévues à l’article 32 du règlement (UE) 2016/679

Les parties définissent à l’annexe III 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 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 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 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 :

* 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) ;
* 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 ;
* 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 à l’annexe III 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

# SECTION II – ACCES AU SYSTEME D’INFORMATION

Cette partie est optionnelle mais doit être précisée

**Application des règles d’accès au Système d’information (physiquement ou via une connexion) dans le cadre de l’exécution des missions entre le GHT Centre Manche et le Tiers.**

## Interlocuteur pour les accès tiers au SI

L’interlocuteur dans la société tierce mentionné ci-dessous sera le contact principal en cas de question ou de demande d’information.

**Nom :** ..............................................................................................................

**Email :** ............................................................................................................

**Tel :** ................................................................................................................

**Fonction :** ......................................................................................................

## Responsabilité et devoirs du tiers quant à la gestion de ses accès et de ses identifiants (VPN, bastion, badge, etc.)

Le tiers intervenant sur le Système d’Information du GHT Centre manche s’engage à respecter strictement les modalités d’accès qui lui sont confiées. Les moyens peuvent être nominatifs ou génériques (par sociétés tierces) selon le cas d’usage.

Dans le cadre d’identifiant nominatif, le titulaire du compte a expressément interdiction de partager, communiquer ou divulguer ses identifiants personnels d’accès (login, mots de passe, certificats, badges, etc.) à toute autre personne. Il en est alors responsable.

Dans le cadre d’identifiant générique, la société tierce assure la gestion sécurisée et la mise à disposition de cet accès aux seules personnes ayant droit d’en connaitre dans son périmètre d’action.

L’utilisation des moyens d’accès tels que le VPN, le bastion, ou tout autre dispositif sécurisé doit respecter les procédures internes définies par les établissements du GHT Centre Manche, incluant l’obligation d’authentification forte (Multi-Factor Authentication - MFA) conformément aux normes en vigueur et quand cela est spécifié et/ou disponible.

Le tiers doit limiter ses interventions au périmètre fonctionnel strictement autorisé et appliquer le principe de moindre privilège afin de réduire les risques d’accès non autorisés ou d’abus.

Le tiers met en place la traçabilité nécessaire à l’indentification des usages (cas des accès génériques). Cette traçabilité constitue une preuve indispensable en cas d’incident de sécurité, d’audit ou de contrôle réglementaire (exigences ANSSI, NIS2).

En cas de perte, vol, compromission ou suspicion d’utilisation frauduleuse des accès, le tiers est tenu d’en informer immédiatement le responsable de la sécurité ou le service informatique en charge (contact RSSI via l’adresse **rssi@ch-stlo.fr**). Toute violation constatée des règles d’accès engage sa responsabilité contractuelle et peut entraîner des sanctions conformément aux dispositions juridiques en matière de sécurité informatique et de protection des données.

Enfin, le tiers accepte que le RSSI ou un représentant puisse réaliser des contrôles, audits ou vérifications de conformité relatifs à la gestion de ses accès et au respect des obligations de sécurité, et ce, sans préavis.

Dans le cas d’usage de notre bastion, les sessions d’accès aux ressources IT du GHT Centre Manche pourront être filmées.

## Autorisation des accès physiques sur site

Tout accès physique par le tiers dans les locaux contenant des actifs du SI doit être explicitement autorisé et doit se faire dans le strict respect des règles internes de sécurité. Les zones sensibles doivent être limitées à ceux ayant une mission précisément définie et justifiée, et sera tracée dans un registre d’accès avec horaires et motifs.

## Traçabilité et gestion des incidents

Le tiers s’engage coopérer pleinement avec le ou les établissements du GHT Centre Manche pour toute analyse post-incident ou vérification de conformité et accepter les audits visant à vérifier la qualité de la journalisation de ses interventions.

En cas de non-respect de ces obligations, la responsabilité contractuelle du tiers pourra être engagée, sans préjudice des sanctions prévues par la loi.

## Continuité d’activité, réversibilité et restitution des données et équipements en fin de mission

Lorsque les contrats mentionnent le devoir de continuité d’activité, le tiers s’engage à maintenir celle-ci durant toute la durée de sa prestation, en mettant en œuvre les moyens techniques et organisationnels nécessaires pour garantir la disponibilité, l’intégrité et la sécurité des services fournis. En cas d’incident ou de rupture de contrat, le tiers devra respecter les plans de continuité d’activité (PCA) et reprise d’activité (PRA) définis conjointement avec le ou les établissements du GHT du Centre Manche concernés, afin de minimiser toute interruption préjudiciable.

Au terme de la mission, ou en cas de cessation anticipée, le tiers est tenu de restituer l’ensemble des données, documents, équipements et supports fournis ou générés dans un format exploitable, conformément aux modalités définies dans le contrat. Cette restitution doit s’effectuer dans des délais stricts, permettant une transition fluide vers un autre prestataire ou vers l’organisation elle-même sans perte ni altération des informations.

Par ailleurs, le tiers devra garantir la suppression sécurisée des données qui ne sont plus nécessaires, en conformité avec les obligations réglementaires (notamment RGPD), et fournir des preuves de cette destruction sur demande. Un plan de réversibilité détaillé, incluant les modalités techniques et organisationnelles de transfert ou restitution, sera annexé au contrat afin d’organiser cette phase critique.

Cette clause vise à protéger la continuité opérationnelle de l’organisation et à limiter les risques liés à une perte d’accès, un arrêt soudain ou un transfert mal maîtrisé des responsabilités.

## Mise à jour des obligations contractuelles en cas d’évolution réglementaire (ex : NIS2)

Le tiers s’engage à prendre en compte et à se conformer aux évolutions légales, réglementaires et normatives applicables pendant toute la durée de son intervention ou de sa relation avec le ou les établissements du GHT Centre Manche. En cas de modification ou de mise à jour des exigences réglementaires (directive NIS2, ou autres cadres sectoriels), il est convenu que les clauses contractuelles relatives à la sécurité, à la confidentialité, aux modalités d’accès et à la gestion des données feront l’objet d’un avenant ou d’une adaptation contractuelle.

Le tiers s’engage à collaborer activement avec l’organisation pour intégrer ces évolutions dans les meilleurs délais afin d’assurer la conformité continue du partenariat et la maîtrise des risques associés. Cela comprend notamment la mise à jour des mesures techniques et organisationnelles, la fourniture de documents attestant du respect des nouvelles exigences, ainsi que la participation aux audits et contrôles liés à ces modifications.

Cette obligation vise à garantir une résilience juridique et opérationnelle face à un environnement réglementaire en constante évolution, en assurant que tous les engagements contractuels restent pertinents et effectifs pour protéger les intérêts des parties.

## Engagement du tiers à la sensibilisation et formation à la sécurité

Le tiers s’engage à assurer que ses personnels intervenant sur le Système d’Information (SI) du GHT Centre Manche ont bénéficié d’une formation adéquate et régulière en matière de sécurité informatique et de cybersécurité. Cette formation doit couvrir les bonnes pratiques de gestion des accès, la reconnaissance des risques et menaces tels que les tentatives d’hameçonnage (phishing), ainsi que le respect des procédures internes et réglementaires en vigueur.

Conformément aux exigences réglementaires ou aux bonnes pratiques, la formation à la sécurité est une obligation légale qui vise à garantir un niveau élevé de sensibilisation et de compétences pour prévenir les incidents et réagir efficacement en cas d’attaque. Le tiers devra fournir à l’organisation, sur demande, les preuves attestant de la réalisation et de la mise à jour régulière de ces formations.

Par ailleurs, le tiers est tenu de sensibiliser son personnel aux enjeux spécifiques du traitement des données personnelles conformément au RGPD, et d’instaurer une culture de sécurité continue en intégrant ces mesures dans ses pratiques opérationnelles.

Enfin, le non-respect de cet engagement pourra engager la responsabilité du tiers et entraîner des mesures contractuelles ou sanctionnelles adaptées.

SECTION III - DISPOSITIONS FINALES

## Non-respect des clauses et résiliation

Sans préjudice des dispositions du règlement (UE) 2016/679, 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.

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 ;
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.

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 des présentes clauses lorsque, après avoir informé le responsable du traitement que ses instructions enfreignent les exigences juridiques applicables conformément à la clause 7.1, point b), le responsable du traitement insiste pour que ses instructions soient suivies.

À 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 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.

ANNEXE I - Liste des parties

Responsable(s) du traitement :

Pour les établissements du GHT Centre Manche

1. Frédérick MARIE, Directeur du Centre Hospitalier Mémorial France Etats-Unis de Saint-Lô

Domicilié 715 rue Dunant, CS 65509 Saint Lô, 50009 Saint Lô Cedex

Représenté par son Délégué à la Protection des Données : [dpo@ch-stlo.fr](mailto:dpo@ch-stlo.fr)

Signature et date d’adhésion :

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

Représenté par son Responsable de la sécurité du SI : [rssi@ch-stlo.fr](mailto:rssi@ch-stlo.fr)

Signature et date d’adhésion :

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

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

Nom: ...............................................................................................................

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

Nom, fonction et coordonnées de la personne de contact :

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

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

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

Signature et date d’adhésion:

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

ANNEXE II - Description du traitement

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

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

Catégories de données à caractère personnel traitées

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

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

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

Nature du traitement

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

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

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

Durée du traitement

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

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

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

ANNEXE III - Mesures techniques et organisationnelles, visant à garantir la sécurité des données

NOTE EXPLICATIVE :

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

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

* mesures de pseudonymisation et de chiffrement des données à caractère personnel ;
* mesures visant à garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
* mesures assurant de disposer de moyens permettant de rétablir la disponibilité des données à caractère personnel et l’accès à celles-ci dans des délais appropriés en cas d’incident physique ou technique ;
* procédures visant à tester, à analyser et à évaluer régulièrement l’efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ;
* mesures d’identification et d’autorisation de l’utilisateur ;
* mesures de protection des données pendant la transmission ;
* mesures de protection des données pendant le stockage ;
* mesures visant à garantir la sécurité physique des sites où les données à caractère personnel sont traitées ;
* mesures visant à garantir l’enregistrement des événements ;
* mesures visant à assurer la configuration des systèmes, y compris la configuration par défaut ;
* mesures de gouvernance et de gestion de l’informatique interne et de la sécurité informatique ;
* mesures de certification/assurance des procédés et produits ;
* mesures visant à garantir la minimisation des données ;
* mesures visant à garantir la qualité des données ;
* mesures visant à garantir une conservation limitée des données ;
* mesures visant à garantir la responsabilité ;
* mesures permettant la portabilité des données et garantissant l’effacement;
* mesures de sécurité pour la gestion des secrets ;
* mesures de sécurité permettant de garantir l'accès à distance aux SI du GHT Centre Manche, notamment les postes de travail du Prestataire ne doivent en aucun cas permettre un rebond entre le réseau du GHT Centre Manche et un réseau tiers ;
* mesures visant à garantir la sécurité des applications et infrastructures ;
* mesures de sécurité mis en place pour le cycle de développement des logiciels.

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

Description des mesures techniques et organisationnelles spécifiques que le sous-traitant doit prendre pour pouvoir prêter assistance au responsable du traitement.

ANNEXE IV - Liste de sous-traitants ultérieurs

NOTE EXPLICATIVE :

La présente annexe doit être complétée en cas d’autorisation spécifique de sous-traitants ultérieurs [ clause 1.6 ].

Le responsable du traitement a autorisé le recours aux sous-traitants ultérieurs suivants :

Nom: ......................................................................................................................

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

Nom, fonction et coordonnées de la personne de contact :

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

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

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