**Contrat relatif à la protection des données à caractère personnel**

# Objet

Le présent contrat a pour objet de définir les conditions dans lesquelles […] (ci-après « le sous-traitant ») s’engage à effectuer pour le compte du CHU DIJON BOURGOGNE (ci-après « le responsable de traitement ») les opérations de traitement de données à caractère personnel définies ci-après.

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, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après, « le règlement européen sur la protection des données ») et la loi 78/17 du 6 janvier 1978 modifiée (ci-après, « loi informatique et libertés »).

Les termes utilisés dans le présent avenant ont le sens qui leur est donné par le RGPD à l’article Définition, notamment : « Responsable de Traitement », « Sous-traitant », « Données personnelles » (ou « Données »), « Violation de Données », « Traitement » et « Personne concernée ».

# Description du traitement faisant l’objet de la sous-traitance

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel définies par les conditions subséquentes :

• Catégorie(s) des données à caractère personnel traitées :

|  |  |
| --- | --- |
| Type de données | Coche si oui |
| Etat civil, identité, données d'identification… |  |
| Coordonnées |  |
| Vie personnelle (habitudes de vie, situation familiale, etc.) |  |
| Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, etc.) |  |
| Image |  |
| Données de connexion (adresse IP, logs, etc.) |  |
| Données de localisation (déplacements, données GPS, GSM, etc.) |  |
| Données bancaires |  |
| Données révélant l'origine raciale ou ethnique |  |
| Données révélant les opinions politiques |  |
| Données révélant les convictions religieuses ou philosophiques |  |
| Données révélant l'appartenance syndicale |  |
| Données génétiques |  |
| Données biométriques aux fins d'identifier une personne physique de manière unique |  |
| Données concernant la santé |  |
| Données concernant la vie sexuelle ou l'orientation sexuelle |  |
| Données relatives à des condamnations pénales ou infractions |  |
| Numéro d’identification national unique (NIR pour la France) |  |
| Données professionnelles |  |

• Finalité(s) du traitement : [à compléter]

• Nature des opérations réalisées sur les données : [à compléter]

• Catégorie(s) de personnes concernées par le traitement : [à compléter]

• Destinataires des données : [à compléter]

• Durée du traitement : [à compléter]

# Obligations du sous-traitant vis-à-vis du responsable de traitement

Le sous-traitant s'engage à :

1. Traiter les données **uniquement pour la ou les seule(s) finalité(s)** qui fait/font l’objet de la sous-traitance.
2. Traiter les données **conformément aux instructions documentées** du responsable de traitement. 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. En outre, si le sous-traitant 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 responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.
3. **Garantir la confidentialité** des données à caractère personnel traitées dans le cadre du présent contrat.
4. Veiller à ce que **les personnes autorisées à traiter les données à caractère personnel** en vertu du présent contrat :

* s’engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
* reçoivent la formation nécessaire en matière de protection des données à caractère personnel.

1. Prendre en compte, s’agissant de ses outils, produits, applications ou services, les principes de**protection des données dès la conception** et de**protection des données par défaut.**
2. **Sous-traitance de rang(s) ultérieur(s)** :

***a) Principes généraux***

Le sous-traitant peut faire appel à un autre sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques.

À la date de signature du contrat, le sous-traitant déclare qu’il fait d’ores et déjà appel au(x) sous-traitant(s) de rang ultérieur suivant :

[à compléter le cas échéant]

Pour tout changement envisagé concernant l’ajout ou le remplacement d’autres sous-traitants, le sous-traitant informera préalablement et par écrit le responsable de traitement contact : […], en indiquant clairement les éléments listés précédemment (activités, identité, coordonnées, date). Le responsable de traitement dispose d’un délai minimum de 20 jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant ultérieur est tenu de respecter les obligations des présentes clauses pour le compte et selon les instructions du responsable de traitement. En conséquence, il appartient au sous-traitant initial de s’assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données et de la loi informatique et libertés. Pour ce faire, le sous-traitant prendra toutes les mesures nécessaires, notamment en répercutant toutes les exigences prévues aux présentes clauses qu’il conclura avec le sous-traitant ultérieur. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l’exécution par l’autre sous-traitant de ses obligations.

***b) Prestation d’hébergement de données de santé***

En cas d’hébergement « en Saas » de données de santé, et sans préjudice des dispositions ci-dessus, le sous-traitant garantit expressément que son prestataire d’hébergement, qualifié de sous-traitant ultérieur, présente les garanties cumulatives suivantes :

• serveurs du prestataire d’hébergement ultérieur localisés en France ou au sein de l’UE ;

• prestataire d’hébergement disposant de la certification HDS (si le contrat prévoit l’hébergement de données de santé) ;

• prestataire d’hébergement conforme au référentiel SecNumCloud publié par l’ANSSI ;

• prestataire d’hébergement garantissant sans réserve son immunité contre toute réglementation ou décision extra-européenne sur le transfert des données (garantie écrite, qui pourra être communiquée au responsable de traitement à première demande) ;

• prestataire d’hébergement soumis aux lois et réglementations applicables au sein de l’UE en matière de protection des données personnelles et garantissant à tout moment le respect des dispositions du RGPD ;

• prestataire d’hébergement fournissant des garanties de réversibilité des services permettant au responsable de traitement de récupérer ou faire récupérer l’ensemble des données sans atteinte à la continuité de son activité.

A défaut pour le sous-traitant de pouvoir s’engager sur les principes ci-dessus au jour de la signature des présentes, celui-ci s’engage (à défaut, le marché pourra être résilié sans frais ni indemnité à première demande du responsable de traitement) :

• à migrer les services d’hébergement sans délai de 24 mois maximum vers une offre présentant l’intégralité des garanties exigées ci-dessus ;

• à mettre en place sans délai avec son sous-traitant ultérieur en charge de l’hébergement « en Saas » des données de santé les garanties appropriées exigées par le chapitre V du RGPD (par exemple, intégrer dans son contrat conclu avec son prestataire d’hébergement des clauses contractuelles types publiées par la Commission européenne dûment accompagnée des mesures supplémentaires permettant de garantir un niveau de protection équivalent à celui garanti au sein de l’UE). Le sous-traitant garantit à ce titre que la législation du pays tiers à laquelle son sous-traitant ultérieur est soumis n'empiétera pas sur ces mesures supplémentaires de manière à les priver d'effectivité, ni ne risque de compromettre le niveau de protection adéquat que les clauses contractuelles types et les mesures supplémentaires sont précisément censées garantir ;

• à avertir sans délai le responsable de traitement en cas de demande d’accès ou de risque d’accès par des autorités publiques étrangères aux données hébergées, prendre toutes les actions légales et recours pour les contester et remettre au responsable de traitement toute documentation en ce sens.

En tout état de cause pour les projets qui le permettent seules des données pseudonymisées et protégées par un code pourront être transférées, avec conservation de la table de correspondance exclusivement au sein du CHU DIJON BOURGOGNE, sans aucune possibilité pour le sous-traitant ou ses sous-traitants ultérieurs d’y avoir accès. Le sous-traitant ou ses sous-traitants ultérieurs ne sont pas autorisés à procéder à des rapprochements ou croisements avec d’autres bases de données pour tenter de réidentifier tout ou partie des personnes concernées.

1. **Notification des violations de données à caractère personnel** :

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel par courrier électronique avec accusé de lecture à l’adresse suivante : [dpo@ght21-52.fr](mailto:dpo@ght21-52.fr) dans un délai maximum de 48 heures après en avoir pris connaissance, sous peine pour le sous-traitant de devoir justifier de ce retard auprès du responsable de traitement qui pourra en faire part à l’autorité de contrôle (CNIL). 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. La notification contient au moins :

* La description de la nature de la violation de 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 ;
* Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
* La description des conséquences probables de la violation de données à caractère personnel ;
* La description des mesures prises ou 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.

Après accord du responsable de traitement, le sous-traitant communique, au nom et pour le compte du responsable de traitement, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

Après accord du responsable de traitement, le sous-traitant notifie à l’autorité de contrôle compétente (CNIL), au nom et pour le compte du responsable de traitement, les violations de données à caractère personnel dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d’engendrer un risque pour les droits et libertés des personnes physiques.

Si le délai de **72 heures est dépassé**, le sous-traitant devra expliquer les motifs du retard à l’autorité de contrôle compétente (CNIL).

1. **Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations**

Le sous-traitant aide le responsable de traitement pour la réalisation d’analyses d’impact relative à la protection des données en fournissant tous les éléments relatifs à la sécurité et aux conditions d’utilisation des Données traités pour le compte du responsable de traitement.

Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l’autorité de contrôle en fournissant tous les éléments relatifs à la sécurité et aux conditions d’utilisation des Données traités pour le compte du responsable de traitement.

1. **Mesures de sécurité**

Le sous-traitant s’engage à mettre en œuvre les mesures de sécurité suivantes :

Décrire les mesures techniques et organisationnelles garantissant un niveau de sécurité adapté au risque, y compris, entre autres :

* La pseudonymisation et le chiffrement des données à caractère personnel ;
* Les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
* Les 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 ;
* Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ;
* La sécurité physique et logique (informatique et réseaux de communication) ;
* La mise en place de mesures pour protéger les données contre une destruction fortuite ou illicite, une perte accidentelle, une altération, une divulgation ou un accès non autorisé, dont le hacking ou la tentative de hacking des données ;
* Des mécanismes de restriction et de contrôle d’accès des données, permettant d’affecter aux individus, les droits d’accès aux données strictement nécessaires à leur mission ;
* La conservation d’une documentation appropriée sur les activités de traitements ;
* Détenir les certifications nécessaires (notamment en termes d’hébergement de données de santé si la réglementation le lui impose) ;
* Adopter des clauses d’entreprises contraignantes (BCR) avec ses filiales le cas échéant.

1. **Sort des données**

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s’engage à détruire toutes les données à caractère personnel et à renvoyer à titre gratuit et dans un format exploitable toutes les données à caractère personnel au responsable de traitement, à moins que le droit de l’Union européenne ou le droit national n’impose de les conserver plus longtemps.

Le renvoi doit s’accompagner de la destruction de toutes les copies existantes dans les systèmes d’information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

Le sous-traitant n’est pas autorisé à anonymiser les données sans avoir fait valider au préalable sa procédure d’anonymisation par le responsable de traitement.

Le sous-traitant mettra à la disposition du responsable de traitement à première demande toute la documentation nécessaire pour démontrer le respect de ses obligations.

1. **Délégué à la protection des données**

Le sous-traitant communique au responsable de traitement **le nom et les coordonnées de son délégué à la protection des données,** s’il en a désigné un conformément à l’article 37 du règlement européen sur la protection des données : [à compléter].

1. **Registre des catégories d’activités de traitement**

Le sous-traitant déclare **tenir par écrit un registre** de toutes les catégories d’activités de traitement effectuées pour le compte du responsable de traitement comprenant :

* le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
* les catégories de traitements effectués pour le compte du responsable du traitement ;
* le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
* dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
  + la pseudonymisation et le chiffrement des données à caractère personnel;
  + des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
  + des 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;
  + une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

1. **Documentation et audit**

Le sous-traitant met à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

Les audits doivent permettre une analyse du respect des dispositions relatives à la protection des Données, notamment : par la vérification de l’ensemble des mesures de sécurité mises en œuvre par le sous-traitant, par la vérification des journaux de localisation des Données, de copie et de suppression des Données, par l’analyse des mesures mises en place pour supprimer les Données, pour prévenir toutes transmissions illégales de Données à des juridictions non adéquates ou pour empêcher le transfert de Données vers un pays non autorisé. L’audit doit enfin pouvoir permettre de s’assurer que les mesures de sécurité et de confidentialité mises en place ne peuvent être contournées sans que cela ne soit détecté et notifié.

Moyennant le respect d’un préavis raisonnable, le sous-traitant s'engage à collaborer de bonne foi avec tout auditeur ainsi désigné. Il facilitera l'accès des auditeurs à tout document ou information ou autre élément utile au bon déroulement de la mission d'audit et lui facilitera sa mission en particulier en répondant à toute question et en lui accordant l'accès à tous les outils et moyens nécessaires à l'audit. L’audit ne peut avoir lieu que sur des jours de travail ouvrés et ne peut avoir pour conséquence de perturber le bon fonctionnement du service.

Si les conclusions de l'audit démontrent un manquement du sous-traitant à ses obligations contractuelles (i) les mesures correctives seront étudiées en comité de pilotage qui statuera sur la suite qu'il convient d'y donner et des éventuelles mesures correctives à mettre en œuvre, sans surcoût, (ii) les frais d’audit seront mis à la charge du sous-traitant. En cas de non-respect du délai de remédiation, des pénalités de retard pourront être appliquées.

# Obligations du responsable de traitement vis-à-vis du sous-traitant

Le responsable de traitement s’engage à :

1. fournir au sous-traitant les données visées au II des présentes clauses ;
2. documenter par écrit toute instruction concernant le traitement des données par le sous-traitant ;
3. 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 ;
4. superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant.

# Droit d’information des personnes concernées

Il appartient au responsable de traitement de fournir l’information aux personnes concernées par les opérations de traitement au moment de la collecte des données. Le sous-traitant s’engage le cas échéant à transmettre au responsable de traitement préalablement tous les éléments nécessaires à cette information à première demande du responsable de traitement.

# Droit des personnes concernées

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d’exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique et dans un délai maximum de 72 heures à l’adresse suivante : [dpo@ght21-52.fr](mailto:dpo@ght21-52.fr)

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement à s’acquitter 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 individuelle automatisée (y compris le profilage). Le sous-traitant doit se conformer, dans la mesure du possible et dès que cela est nécessaire, à toute instruction documentée du responsable de traitement participant à donner suite, de manière pleinement effective, aux demandes d’exercice des droits des personnes concernées.