CHECKLIST DE CONFORMITE À LA MR-007 À DESTINATION DES PORTEURS DE PROJETS

Si les éléments ci-dessous sont validés alors le projet est éligible à la procédure MR-007 simplifiant l’accès à la base principale du Système National des Données de Santé (SNDS)

|  |
| --- |
| **Notice de complétion**   * Cette checklist permet à tout responsable de traitement (RT) souhaitant réaliser un projet de recherche dans le domaine de la santé **d'auto évaluer sa conformité** à la [procédure simplifiée MR-007](https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000048194078) élaborée par la CNIL. * Cette grille est **exhaustive** : elle contient l’ensemble des exigences posées par la méthodologie de référence. C’est pourquoi il est nécessaire de connaître l’ensemble des caractéristiques de sa recherche (finalités, données traitées, information des personnes, sécurité, etc.) avant de se lancer dans la complétion de la grille. * Une case “faux” signifie que le projet de recherche ne respecte pas l’obligation associée et ainsi qu’il n’est **pas conforme au référentiel**. En cas de réponse partiellement positive, le RT doit considérer que la réponse est négative. * Le RT n’est **pas concerné par cette grille** si la recherche envisagée ne répond pas aux conditions du périmètre d’application présenté en slide 3 de [notre guide](https://docs.google.com/presentation/d/1qYG8hoIt1kjJ2mxV7e79-eeK5gU6CcOi/edit?slide=id.p1#slide=id.p1). * S’il apparaît une fois la grille remplie que : * Le projet de recherche est conforme à la MR-007, alors le RT doit réaliser une [déclaration de conformité](https://www.cnil.fr/fr/declarer-un-fichier) à la MR auprès de la CNIL pour réaliser la recherche et [enregistrer l’étude](https://www.health-data-hub.fr/depot) dans le répertoire public du Health Data Hub ; * Le projet de recherche n’est pas conforme à la MR-007, alors le RT doit demander une [autorisation à la CNIL](https://www.health-data-hub.fr/starter-kit) pour réaliser sa recherche. L’autorisation ne pourra être délivrée que si le traitement est suffisamment protecteur des données des personnes concernées et si des mesures supplémentaires sont mises en œuvre afin de compenser les points de non-conformité à la MR. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Condition | OUI *(conforme)* | N/A | NON  *(non-conforme)* | | Justifier la  non-conformité |
| Définitions, responsables de traitement concernés, champs d’application et intérêt public | | | | | |
| 1.2. Responsables de traitement concernés | | | | | |
| La mise en œuvre de la recherche, l’étude ou l’évaluation dans le domaine de la santé est nécessaire à la poursuite d’un intérêt légitime du responsable de traitement au sens de l’article 6-.1-.f du RGPD. | OUI  *Conformité à documenter aux points 1. Présentation de l'équipe projet et 2.3 Justification de l’intérêt public du protocole scientifique* |  | | NON | Justifier la  non-conformité : |
| Dans le cas d’une responsabilité conjointe de traitement, les responsables de traitement ont défini, de manière transparente, leurs obligations respectives conformément à l'article 26 du RGPD. | OUI  *Conformité à documenter 2.3 Justification de l’intérêt public du protocole scientifique* | N/A  *S’il n’y a pas de responsabilité conjointe* | | NON | Justifier la  non-conformité : |
| 1.3. Traitements de données à caractère personnel inclus dans le champ d'application de la présente méthodologie | | | | | |
| Le traitement envisagé a pour finalité la réalisation de recherches, études ou évaluations dans le domaine de la santé. | OUI  *Conformité à documenter 2.3 Justification de l’intérêt public du protocole scientifique* |  | | NON | Justifier la  non-conformité : |
| Un dossier de demande d’avis comportant notamment les documents suivants, sera transmis au CESREES pour avis avant le début de la mise en oeuvre du traitement:     * un protocole conforme au modèle mis à disposition par le Health Data Hub ; * une expression de besoins conforme au modèle mis à disposition par le Health Data Hub | OUI  *Conformité à documenter dans le protocole scientifique et l’expression des besoin (EDB)* |  | | NON | Justifier la  non-conformité : |
| |  | | --- | | En cas d’obtention d’un avis expressément favorable du CESREES, le responsable de traitement s’engage, si cet avis est accompagné de recommandations, à les prendre en compte et à modifier son dossier en conséquence, préalablement à la mise en œuvre du traitement. |   *Pour obtenir cet avis, un dossier doit être déposé auprès du secrétariat unique du HDH et doit comporter les éléments listés dans la MR-007 (§6.3).* | OUI  *Conformité à documenter dans le point 3.6 Préparation de données du protocole scientifique* |  | | NON | Justifier la  non-conformité : |
| Les données traitées proviennent exclusivement et directement de la CNAM. | OUI  *Conformité à documenter dans le point 3.6 Préparation de données du protocole scientifique* |  | | NON | Justifier la  non-conformité : |
| Les données seront mises à disposition du responsable de traitement ou du responsable de la mise en œuvre du traitement dans un environnement maîtrisé, tel que défini au point 1.1 (Définitions) et remplissant les conditions cumulatives suivantes :     * a fait l’objet d’une homologation conformément au référentiel de sécurité applicable au SNDS. Cette homologation, qui ne doit pas avoir expiré, doit faire l’objet d’un suivi régulier et est régulièrement renouvelée dans les délais prévus par la décision d’homologation ; * a été expertisé par la CNIL dans le cadre d’un traitement de données ayant fait l’objet d’une autorisation expresse par la CNIL. Cette autorisation doit dater de moins de trois ans ; * est conforme au titre V de la délibération MR-008 concernant les modalités d’hébergement des données et l’absence de transferts en dehors de l’Union européenne. | OUI  *Conformité à documenter dans le point 3.6 Préparation de données du protocole scientifique* |  | | NON | Justifier la  non-conformité : |
| Le responsable de traitement et le cas échéant, le responsable de la mise en œuvre du traitement, signeront préalablement une convention d’accès aux données avec le gestionnaire de l’environnement maîtrisé mettant à disposition les données du SNDS. | OUI  *Conformité à documenter par la convention de sous-traitance liant le RT et le sous-traitant* |  | | NON | Justifier la  non-conformité : |
| Le responsable de traitement et le cas échéant, le responsable de la mise en œuvre du traitement, font signer à chaque utilisateur habilité un engagement individuel à respecter les conditions d’utilisation définies par l’environnement maîtrisé. | OUI  *Conformité à documenter par la convention de sous-traitance liant le RT et le sous-traitant* |  | | NON | Justifier la  non-conformité : |
| Le responsable de traitement transmet au gestionnaire de l’environnement maîtrisé la liste, actualisable, des laboratoires de recherche ou bureaux d'études auxquels il a recours. | OUI  *Conformité à documenter par la convention de sous-traitance liant le RT et le sous-traitant* |  | | NON | Justifier la  non-conformité : |
| 1.4. Intérêt public et finalités interdites | | | | | |
| Le traitement envisagé présente un caractère d'intérêt public au sens de l’article 66 de la loi « informatique et liberté, justifié par le responsable de traitement dans le protocole, qui sera transmis au HDH lors de l’enregistrement dans le répertoire public. | OUI  *Conformité à documenter dans le point 2.3 Justification de l’intérêt public du protocole scientifique* |  | | NON | Justifier la  non-conformité : |
| Le traitement envisagé n’a pas pour objectif, principal ou secondaire, ou pour effet de permettre la réalisation d'une ou des finalités interdites, décrites à l'article L. 1461-1 V du CSP.  1. la promotion des produits mentionnés au II de l'article L. 5311-1 en direction des professionnels de santé ou d'établissements de santé ;  2. l’exclusion de garanties des contrats d'assurance et la modification de cotisations ou de primes d'assurance d'un individu ou d'un groupe d'individus présentant un même risque." | OUI |  | | NON | Justifier la  non-conformité : |
| 1. Traitements relatifs aux données des personnes concernées par des études | | | | | |
| 2.1. Finalité des traitements | | | | | |
| Le traitement de données envisagé s’inscrit dans l’une des finalités suivantes :   * évaluation comparative de l'offre de soins : analyses spatiales, analyses stratégiques ; * évolution des pratiques de prises en charge, incidence de certains facteurs dans les hospitalisations, analyses temporelles ; * analyses comparatives des activités de soins, études de trajectoire de patients, bassin de recrutement, devenir des patients; * description et analyse des pathologies et parcours de soins des patients dans les établissements de santé ; * analyse du territoire de santé, des groupements hospitaliers de territoires (GHT), études de collaboration entre établissements d'un périmètre défini ; * analyse continue d'évaluations comparatives, meilleure adaptation de l'offre de soins, optimisation, valorisation des séjours, réalisation d'indicateurs de pilotage, stratégie ; * travaux de modélisation, simulation, planning, logistique hospitalière, recherche opérationnelle (analyse de données dans le but d'optimiser des organisations ou de produire des éléments d'aide à la décision pour de nouvelles organisations) ; * ciblage des centres et/ou réalisation d'études de faisabilité pour la réalisation d'une recherche impliquant ou n'impliquant pas la personne humaine ; * études épidémiologiques ; * études médico-économiques. | OUI  *Conformité à documenter au point 2.3 Justification de l’intérêt public du protocole scientifique* |  | | NON | Justifier la  non-conformité : |
| 2.2. Origine et nature des données | | | | | |
| 2.2.1. Nature des données à caractère personnel - Pour les personnes concernées | | | | | |
| Seules les données issues de la base principale du SNDS, telle que définie à l’article R. 1461-2 du code de la santé publique, seront traitées dans le cadre de cette étude. La base principale comporte à ce jour :   * les données issues des systèmes d'information mentionnés à l’article L. 6113-7 du code de la santé publique (base PMSI) ; * les données du système national d'information inter régimes de l’assurance maladie mentionné à l'article L. 161-28-1 du code de la sécurité sociale (base SNIIRAM) ; * les données sur les causes de décès mentionnées à l'article L. 2223-42 du code général des collectivités territoriales (base du CépiDC de l’INSERM) ; * les données médico-sociales du système d'information mentionné à l’article L. 247- 2 du code de l'action sociale et des familles (données relatives au handicap) ; * les données issues des bases de données « Vaccin-Covid » et « SI-DEP » » (système d'information de dépistage). | OUI  *Conformité à documenter au point 3.4. Sources de données du protocole scientifique et dans l’EDB* |  | | NON | Justifier la  non-conformité : |
| La profondeur historique demandée par le responsable de traitement est inférieure ou égale à neuf ans en plus de l’année en cours. | OUI  *Conformité à documenter au point 3.4. Sources de données du protocole scientifique et dans l’EDB* |  | | NON | Justifier la  non-conformité : |
| Sont justifiés dans le protocole au regard de la finalité du traitement : les catégories de données traitées, la période de ciblage des personnes concernées, les composantes du SNDS et la profondeur historique des données consultées demandées, la durée d’accès, la zone géographique et le nombre de personnes concernées. | OUI  *Conformité à documenter au point 3. Méthodologie du protocole scientifique et dans l’EDB* |  | | NON | Justifier la  non-conformité : |
| 2.2.2. Nature des données à caractère personnel - Pour les utilisateurs | | | | | |
| Concernant les utilisateurs, seules sont traitées les catégories de données à caractère personnel suivantes :   * nom, prénom(s), prénoms, fonction, profils d'accès ; * si pertinent : * coordonnées téléphoniques, postales et/ou électroniques professionnelles, organisme employeur ; * formation, diplômes ; * éléments nécessaires à l'évaluation des connaissances afin de réaliser l'étude. | OUI  *Conformité à documenter au point 3.5. Variables du protocole scientifique* |  | | NON | Justifier la  non-conformité : |
| Les traitements de données des utilisateurs ont pour seule finalité la mise en œuvre de l'étude et le respect des obligations légales du responsable de traitement. En particulier, les données traitées ont pour finalité la gestion des déclarations d'intérêts, leur transmission au HDH, le cas échéant et la gestion des procédures d'habilitation internes. | OUI  *Conformité à documenter au point 2.2 Justification de l’intérêt public du protocole scientifique* |  | | NON | Justifier la  non-conformité : |
| 2.3. Accédants et destinataires des données traitées (utilisateurs) | | | | | |
| Le responsable de traitement ou, le cas échéant, le responsable de la mise en œuvre du traitement tient à jour et met à disposition du responsable de traitement des documents indiquant la ou les personnes compétentes en son sein pour délivrer l'habilitation à accéder aux données, la liste des personnes habilitées à accéder à ces données, leurs profils d’accès respectifs et les modalités d'attribution, de gestion et de contrôle des habilitations. | OUI |  | | NON | Justifier la  non-conformité : |
| Seules les personnes habilitées par le responsable de traitement ou, le cas échéant, par le responsable de la mise en œuvre du traitement, ont accès aux données traitées au regard de leurs fonctions et dans des conditions conformes à la réglementation. Ces catégories de personnes sont soumises au secret professionnel dans les conditions définies par les articles 226-13 et 226-14 du code pénal. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| La qualification des personnes habilitées et leurs droits d'accès sont régulièrement réévalués, conformément aux modalités décrites dans la procédure d'habilitation établie par le responsable de traitement ou par le responsable de la mise en œuvre du traitement. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| 2.4. Information et droits des personnes concernées par l'étude | | | | | |
| Les mesures suivantes sont mises en œuvre pour garantir une information publiquement disponible des personnes concernées :   * la diffusion de la note d’information sur le site web du responsable de traitement ainsi que, le cas échéant, du laboratoire de recherche ou bureau d’études ; * la mise en place d’un portail de transparence lorsque le responsable de traitement réalise plusieurs études à partir des données du SNDS. Ce portail de transparence comporte une information générale sur le SNDS et une note d’information spécifique à chaque étude mise en œuvre.   Ces documents comportent l'ensemble des mentions prévues à l'article 14 du RGPD. | OUI  *Conformité à documenter au point 4.1. Respect des droits des personnes concerné du protocole scientifique et dans la note d'information* |  | | NON | Justifier la  non-conformité : |
| 2.4.2. Exercice des droits des personnes | | | | | |
| La personne concernée exerce ses droits d'accès, de rectification, d’effacement, de limitation du traitement et d'opposition concernant le traitement mis en œuvre, directement auprès du délégué à la protection des données de l’organisme responsable du traitement. | OUI  *Conformité à documenter au point 4.1. Respect des droits des personnes concerné du protocole scientifique et dans la note d’information* |  | | NON | Justifier la  non-conformité : |
| 2.5. Durée d’accès ou de conservation des données | | | | | |
| La durée d’accès ou de conservation est limitée à celle strictement nécessaire à la mise en œuvre du traitement et n’excède pas la durée de l’étude. En tout état de cause, cette durée n’excède pas cinq ans à compter de la dernière mise à disposition effective des données. | OUI  *Conformité à documenter au point 4.1. Respect des droits des personnes concernées du protocole scientifique et l’AIPD* |  | | NON | Justifier la  non-conformité : |
| En cas de demande de prolongation de l’accès aux données de la base principale du SNDS qui concerne une étude en cours de réalisation ayant déjà fait l’objet d’un avis expressément favorable par le CESREES dans le cadre, celle-ci n’excède pas deux ans et fait suite à une demande motivée du responsable de traitement, à adresser au CESREES qui rendra un nouvel avis. | OUI | N/A | | NON | Justifier la  non-conformité : |
| Aucun archivage des données n’est réalisé. | OUI  *Conformité à documenter au point 4.1. Respect des droits des personnes concernées du protocole scientifique* |  | | NON | Justifier la  non-conformité : |
| Le cas échéant, seuls des résultats anonymes, au sens de l'avis du Groupe de l’article 29 (G29) n° 05/2014 ou à tout avis ultérieur du CEPD relatif à l’anonymisation, sont exportés. | OUI  *Conformité à documenter au point 4.1. Respect des droits des personnes concernées du protocole scientifique* |  | | NON | Justifier la  non-conformité : |
| Les données à caractère personnel des utilisateurs chargés de la réalisation de l'étude seront supprimées au plus tard cinq ans après la fin de l'étude. | OUI  *Conformité à documenter au point 4.1. Respect des droits des personnes concernées du protocole scientifique et l’AIPD* |  | | NON | Justifier la  non-conformité : |
| 2.6. Publication des résultats | | | | | |
| La présentation des résultats du traitement de données ne permettra en aucun cas l'identification directe ou indirecte des personnes concernées. | OUI  *Conformité à documenter au point 4.1. Respect des droits des personnes concernées du protocole scientifique et l’AIPD* | N/A | | NON | Justifier la  non-conformité : |
| 1. Sécurité (1) 2. *Le texte précise que les mesures ci-dessous ne sont pas exhaustives et devront être complétées au regard des risques pesants sur le traitement mis en œuvre.* | | | | | |
| Les mesures de sécurité sont conformes au référentiel de sécurité applicable au Système national des données de santé, prévu par l'arrêté du 22 mars 2017 et ses mises à jour ultérieures (ci-après- « référentiel de sécurité du SNDS »). | OUI  *Conformité à documenter dans le point 4. Confidentialité et sécurité des données*  *du protocole et l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| Lorsque le responsable de traitement a recours à un laboratoire de recherche ou un bureau d’études, le responsable de traitement s’est assuré que le contrat conclu avec le laboratoire de recherche ou bureau d'études précise les mesures et les conditions de sécurité relatives à la conformité au référentiel de sécurité du SNDS. En particulier, l’environnement maîtrisé a fait l’objet d’une homologation préalablement à la mise en œuvre du traitement de données nécessaire à l’étude. | OUI  *Conformité à documenter par la convention de sous-traitance liant le RT et le sous-traitant* | N/A  *(si le RT ne fait pas appel à un LRBE)* | | NON | Justifier la  non-conformité : |
| La répartition des rôles et responsabilités entre le ou les responsables de traitement, le responsable de la mise en œuvre du traitement et le gestionnaire de l’environnement maîtrisé est formalisée par une convention. Cette dernière porte notamment sur la sensibilisation des utilisateurs de l’étude, la surveillance des traces, la gestion des alertes et des incidents ainsi que la gestion des exportations de données anonymes. Cette convention est conforme à l’article 28 du RGPD. | OUI  *Conformité à documenter par la convention de sous-traitance liant le RT et le sous-traitant* |  | | NON | Justifier la  non-conformité : |
| **Gestion des habilitations et accès logique aux données** | | | | | |
| Différents profils d’habilitation sont prévus afin de gérer les accès aux données en tant que de besoin et de façon exclusive. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| Les personnes habilitées à accéder aux données à caractère personnel sont individuellement habilitées selon une procédure impliquant une validation par leur responsable hiérarchique. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| Une revue des habilitations est réalisée régulièrement et a minima annuellement, ainsi qu’à la fin de chaque étude. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| Les permissions d’accès sont retirées dès le retrait des habilitations, par exemple après le départ d’un utilisateur habilité ou une modification de ses missions. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| **Identification et authentification des utilisateurs** | | | | | |
| L’accès aux données à caractère personnel est subordonné à une identification locale ou nationale pour toute personne physique ou morale, conformément aux exigences du palier 2 du Référentiel d'identification de la PGSSI-S. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| L’accès aux données à caractère personnel est subordonné à une authentification forte faisant intervenir a minima deux facteurs d’authentification distincts, conformément aux exigences du palier 2 du Référentiel d'authentification de la PGSSI-S. Si un de ces facteurs est un mot de passe, celui-ci est conforme aux recommandations de la CNIL en matière de mots de passe à la date de rédaction de cette méthodologie de référence (délibération n° 2022-100 du 21 juillet 2022). | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| **Espace projet** | | | | | |
| Les données d’une étude sont manipulées par les utilisateurs habilités uniquement dans un espace projet spécifique à cette étude, étanche avec les données du SNDS central ainsi qu’avec les espaces projets d’autres études conduites dans le même environnement maîtrisé. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| Les jeux de données importés dans un espace projet spécifique à une étude doivent être minimisés et limités aux seules données nécessaires à l’étude. Un numéro pseudonyme unique spécifique à chaque espace projet doit être généré dans les mêmes conditions de pseudonymisation que celles définies par le référentiel de sécurité applicable au SNDS précité. Par exemple, ce numéro pseudonyme unique pourra être généré par une fonction de hachage cryptographique résistante aux attaques par force brute ou un générateur de nombres pseudo-aléatoires cryptographiquement sûr. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| **Transmission des données** | | | | | |
| Toutes les transmissions de données depuis ou vers l’environnement maîtrisé ou les espaces projet doivent faire l’objet de mesures de chiffrement conformes à l’annexe B1 du référentiel général de sécurité (RGS) afin d’en garantir la confidentialité.  Ces mesures de chiffrement s’appliquent aux données en transit et à leur stockage après réception dans l’environnement maîtrisé ou les espaces projets. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| **Exportation de données anonymes hors des espaces de travail** | | | | | |
| Seuls des jeux de données anonymes font l’objet d’une exportation hors de l’environnement maîtrisé ou d’un espace projet. Le processus d’anonymisation produit un jeu de données conforme aux trois critères définis par l'avis du G29 n° 05/2014 ou à tout avis ultérieur du CEPD relatif à l’anonymisation. Cette conformité est documentée. À défaut, si ces trois critères ne peuvent être réunis, une étude des risques de réidentification est menée et documentée, préalablement à chaque exportation. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| Les exportations de données sont soumises à la validation préalable d’un responsable afin d’en avaliser le principe, notamment au regard de l’exigence SEC-EXP-1. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| Les exportations font l’objet d’une surveillance automatique ou manuelle par un opérateur spécialisé afin d’en vérifier le caractère anonyme. Dans le cas où cette surveillance est automatique, toute exportation identifiée comme non conforme fait l’objet d’une remontée d’alerte et d’une mise en quarantaine dans un espace cloisonné et dédié, puis est vérifiée manuellement par un responsable spécifiquement formé et habilité. | OUI  *Conformité à documenter dans l’AIPD du RT* | N/A | | NON | Justifier la  non-conformité : |
| **Sensibilisation des utilisateurs et sécurité des postes de travail** | | | | | |
| Chaque personne habilitée à accéder à l’environnement maîtrisé est formée au respect du secret professionnel et sensibilisée régulièrement aux risques et obligations inhérents au traitement de données de santé. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| Chaque personne habilitée à accéder à l’environnement maîtrisé signe une charte de confidentialité. Celle-ci précise notamment les obligations au regard à la fois de la protection des données à caractère personnel de santé et des mesures de sécurité mises en place dans l’environnement maîtrisé, ainsi que les sanctions afférentes au non-respect de ces obligations. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| Les postes de travail des personnes habilitées à accéder à l’environnement maîtrisé, y compris les utilisateurs externes accédant uniquement aux espaces projet, font l’objet de mesures de sécurité spécifiques, par exemple en mettant en place des comptes nominatifs, une authentification adéquate, un verrouillage automatique des sessions, un chiffrement des disques durs et des mesures de filtrage. Dans le cas où les postes de travail ne sont pas sous le contrôle du responsable de traitement, les mesures de sécurité à mettre en place sur les postes de travail sont encadrées au moyen d’une convention entre les parties concernées. | OUI  *Conformité à documenter dans l’AIPD du RT et la convention de sous-traitance liant le RT et le sous-traitant* |  | | NON | Justifier la  non-conformité : |
| **Journalisation** | | | | | |
| Les actions des utilisateurs des espaces projet et celles des utilisateurs de l’environnement maîtrisé font l’objet de mesures de journalisation, conformément aux exigences du palier 3 du Référentiel d'imputabilité de la PGSSI-S. En particulier, les connexions (identifiants, date et heure), les requêtes et les opérations réalisées sont tracées. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| Un contrôle des traces est réalisé régulièrement et a minima mensuellement, ainsi qu’à la fin de chaque période d’habilitation liée à une étude. Ce contrôle est réalisé par :  - une solution réalisant une surveillance automatique avec une remontée d’alertes traitées manuellement par un opérateur habilité ;  - ou un contrôle semi-automatique via exécution de programmes permettant une sélection des traces anormales, suivi d’une relecture manuelle par un opérateur habilité | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| Les traces de journalisation définies aux exigences SEC-JOU-1 sont conservées pour une durée de six mois à un an à compter de leur collecte, sauf exception justifiée par l’importance du risque pour les personnes en cas de détournement des finalités du traitement et de la fréquence d’occurrences de telles pratiques. Dans ce dernier cas, la durée de conservation maximale des traces de journalisation peut être étendue à trois ans. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| **Gestion des incidents de sécurité et des violations de données à caractère personnel** | | | | | |
| Les parties à la convention prévoient une procédure de gestion et de traitement des incidents de sécurité et des violations de données à caractère personnel, précisant les rôles et responsabilités et les actions à mener en cas de survenue de tels incidents. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| Tout incident de sécurité, d’origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence, même temporaire, de compromettre l’intégrité, la confidentialité ou la disponibilité de données à caractère personnel, fait l’objet d’une documentation en interne dans un registre des violations. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| Toute violation de données est notifiée à la CNIL dans les conditions prévues à l’article 33 du RGPD. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| Dans l’hypothèse où la violation est susceptible d’engendrer un risque élevé pour les droits et libertés d’une personne physique, le responsable de traitement communique la violation des données aux personnes concernées dans les meilleurs délais, conformément à l’article 34 du RGPD. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| Conformément aux articles 5.1.f et 32 du RGPD, les mesures de sécurité sont mises à jour au regard de la réévaluation régulière des risques et pour que ces mesures soient conformes à l’état de l’art. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| 1. Sous-traitants | | | | | |
| Le cas échéant, le responsable de traitement choisit un sous-traitant présentant des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées, permettant de répondre aux exigences du RGPD et de la loi « informatique et libertés » et de garantir la protection des droits des personnes concernées. | OUI  *Conformité à documenter la convention de sous-traitance liant le RT et le sous-traitant* | N/A  *(si le RT ne fait pas appel à un LRBE)* | | NON | Justifier la  non-conformité : |
| Le responsable de traitement établit avec le sous-traitant un contrat ou un autre acte juridique précisant les obligations de chaque partie et reprenant les exigences de l'article 28 du RGPD.trat dont le contenu est défini par ces textes. | OUI  *Conformité à documenter la convention de sous-traitance liant le RT et le sous-traitant* | N/A  *(si le RT ne fait pas appel à un LRBE)* | | NON | Justifier la  non-conformité : |
| En outre, les sous-traitants :   * désignent, le cas échéant, un délégué à la protection des données conformément à l'article 37 du RGPD ; * tiennent un registre des catégories de traitements effectués pour le compte du responsable de traitement, conformément à l'article 30 du RGPD. | OUI  *Conformité à documenter la convention de sous-traitance liant le RT et le sous-traitant* | N/A  *(si le RT ne fait pas appel à un LRBE)* | | NON | Justifier la  non-conformité : |
| 1. Hébergement des données du SNDS et absence de transfert de données hors de l’union européenne | | | | | |
| Le responsable de traitement de l’étude s’assure :   * que les données issues de la base principale du SNDS sont hébergées exclusivement au sein des pays membres de l’espace économique européen et sans transfert de données possible en dehors de l’Union européenne * de l’absence d’accès distant aux données depuis l’extérieur du territoire de l’Union européenne. | OUI  *Conformité à documenter dans le point 4.1 Respect des droits des personnes concernées du protocole et l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| Les organismes et le cas échéant, leurs sous-traitants, accédant aux données du SNDS dans le cadre de la réalisation des opérations d’hébergement de l’infrastructure technique de l’environnement maîtrisé, ainsi que l’administration et l’exploitation associées à ce stockage, sont exclusivement soumis aux lois de l’Union européenne. | OUI  *Conformité à documenter dans le point 4.1 Respect des droits des personnes concernées du protocole et l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| 1. Mise en oeuvre du principe de responsabilité | | | | | |
| 6.1. Analyse d’impact sur la protection des données | | | | | |
| Le responsable de traitement effectue une analyse d'impact relative à la protection des données menée conformément aux dispositions de l'article 35 du RGPD, qui couvre en particulier les risques sur les droits et libertés des personnes concernées.  *Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques similaires.* | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| Cette analyse d’impact sera réexaminée et mise à jour régulièrement, notamment si des changements importants sont prévus dans le traitement mis en œuvre dans le cadre de la présente méthodologie, ou si les risques pour les personnes concernées ont évolué. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| 6.2. Formalités | | | | | |
| Chaque responsable de traitement désigne un délégué à la protection des données, en application de l'article 37 du RGPD. Ce délégué à la protection des données a notamment pour mission de vérifier le respect de la conformité des traitements mis en œuvre selon la présente méthodologie. | OUI  *Conformité à documenter dans l’AIPD du RT* |  | | NON | Justifier la  non-conformité : |
| Le responsable de traitement adresse à la CNIL une seule déclaration de conformité à la présente méthodologie pour l'ensemble des traitements qu'il met en œuvre dès lors qu'ils sont et seront réalisés en conformité avec l'ensemble des dispositions de la méthodologie. | OUI  *Conformité à documenter par le récepissé reçu suite à l’engagement de conformité du RT* |  | | NON | Justifier la  non-conformité : |
| Dans le cadre d’une responsabilité conjointe, chaque responsable de traitement procède à une déclaration de conformité à la méthodologie de référence pour son propre compte. | OUI  *Conformité à documenter par le récepissé reçu suite à l’engagement de conformité du RT* | N/A | | NON | Justifier la  non-conformité : |
| Le responsable de traitement tient à jour, au sein du registre des activités de traitement, la liste des traitements mis en œuvre dans le cadre de la présente méthodologie. Il vérifie régulièrement la conformité des traitements en cours au regard des exigences de la méthodologie de référence et documente cette analyse. | OUI  *Conformité à documenter dans le registre des activités de traitement du RT* |  | | NON | Justifier la  non-conformité : |
| 6.3. Principe de transparence | | | | | |
| Le responsable du traitement s'engage à enregistrer dans le répertoire public tenu par le HDH chaque étude réalisée dans le cadre de cette méthodologie. | OUI  *Conformité à documenter par la fiche projet sur le répertoire public du HDH* |  | | NON | Justifier la  non-conformité : |
| Cet enregistrement est effectué, avant le début de chaque étude, par le responsable de traitement ou la personne agissant pour son compte. Il s'accompagne de la transmission au HDH d'un dossier comportant :   * le protocole, incluant la justification de l'intérêt public, ainsi qu'un résumé, selon le modèle mis à disposition par le HDH. En cas d’avis favorable avec recommandations du CESREES, le protocole et le résumé tenant compte de manière apparente des recommandations, doivent être enregistrés ; * la déclaration d'intérêts, en rapport avec l’objet de l’étude, du responsable du traitement et le cas échéant du sous-traitant. | OUI  *Conformité à documenter dans le protocole, le résumé, la déclaration d’intérêts* |  | | NON | Justifier la  non-conformité : |
| À la fin de l’étude, la méthode et les résultats obtenus seront communiqués au HDH en vue de leur publication dans le respect du secret des affaires et de la propriété intellectuelle. | OUI  *Conformité à documenter par la fiche projet sur le répertoire public du HDH* |  | | NON | Justifier la  non-conformité : |
| Le responsable de traitement s’engage à ce que l'enregistrement du traitement et la transmission des résultats soient effectués conformément aux modalités définies par le HDH. | OUI  *Conformité à documenter par la fiche projet sur le répertoire public du HDH* |  | | NON | Justifier la  non-conformité : |
| 6.4. Bilan | | | | | |
| Le responsable de traitement, le cas échéant après avoir consulté le ou les sous- traitants, s’engage à transmettre tous les trois ans à la CNIL un bilan synthétisant son usage de la méthodologie de référence, en suivant le modèle mis à disposition par le HDH. | OUI  *Conformité à documenter par le Bilan synthétique* |  | | NON | Justifier la  non-conformité : |