RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Inserm
La science pour la santé
From science to health

GUIDE POUR LA REDACTION D'UNE ANALYSE D'IMPACT RELATIVE A LA PROTECTION DES DONNEES DANS LE DOMAINE DE LA RECHERCHE EN SANTE

Version du	16 mars 2022

SOURCES ET REFERENCES

Ce guide s'appuie sur :

- 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- RGPD) :

https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679#d1e40-1-1

- Les lignes directrices du Comité Européen de la Protection des Données (CEPD)

https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf

- Les informations et documents mis à disposition par la Commission Nationale de l'Informatique et des Libertés (CNIL) :

https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd

Ce guide n'a qu'une valeur indicative. Il ne se substitue pas au RGPD, aux lois ou aux recommandations publiées par la Commission Nationale de l'Informatique et des Libertés (CNIL) ou par le Comité Européen de la Protection des Données (CEPD).

Il conviendra également, afin d'établir l'analyse d'impact relative à la protection des données (AIPD), de se référer aux guides de la CNIL :

- Analyse d'impact relative à la protection des données (AIPD) 1 : la méthode

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-fr-methode.pdf

- Analyse d'impact relative à la protection des données (AIPD) 2 : les modèles

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-fr-modeles.pdf

- Analyse d'impact relative à la protection des données (AIPD) 3 : les bases de connaissances

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf

Le présent guide constitue une synthèse de ces guides.

L’ANALYSE D’IMPACT EN QUELQUES MOTS

Les traitements nécessitant une analyse d’impact :

Principe : Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

Les cas particuliers : Liste des traitements, établie par la CNIL, pour lesquels une analyse d’impact relative à la protection des données est obligatoire :

https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-requise.pdf

Liste des traitements, établie par le CEPD, pour lesquels une analyse d’impact relative à la protection des données est obligatoire. L’AIPD est requise lorsque le traitement remplit au moins deux des neuf critères issus des lignes directrices du CEPD dont :

- collecte de données sensibles ou données à caractère hautement personnel ;
- collecte de données personnelles à large échelle ;
- croisement de données ;
- personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
- usage innovant (utilisation d’une nouvelle technologie) ;

La non réalisation d’une AIPD, alors qu’imposée par les textes, peut faire l’objet d'amendes administratives pouvant s'élever jusqu'à 10 000 000 EUR.

Le contenu de l’analyse d’impact (principes) :

L'analyse contient au moins:

- une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement;
- une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités;
- une évaluation des risques pour les droits et libertés des personnes concernées
- les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

Mise en place et vie de l’AIPD (principes)

L'AIPD doit être menée avant la mise en œuvre du traitement. Elle doit être démarrée le plus en amont possible et sera mise à jour tout au long du cycle de vie du traitement.

La mise en place de l’AIPD relève de la responsabilité du responsable de traitement qui est tenu de s’assurer de la conformité de son traitement au RGPD.

Il demande conseil au Délégué à la Protection des données.

Il s’appuie également, tant pour le processus de réalisation de l'AIPD que de sa validation:

- Sur les métiers (maîtrise d’ouvrage), les équipes chargées de la mise en œuvre (maîtrise d’œuvre), et la personne chargée de la sécurité des systèmes d’information.
- Si un sous-traitant intervient dans le traitement, sur ledit sous-traitant qui doit fournir son aide et les informations nécessaires à la réalisation de l'AIPD.

L’AIPD doit faire l’objet d’une revue régulière pour s’assurer que le niveau de risque reste acceptable tout au long de la vie du traitement, dans la mesure où l’environnement, technique notamment, sera amené à évoluer, ce qui nécessitera d’adapter les mesures mises en œuvre.

CONTENU TYPE D'UNE ANALYSE D'IMPACT ET CONSEILS POUR SON ELABORATION

Table des matières

1. PERSONNES IMPLIQUEES DANS L'ELABORATION DE L'ANALYSE D'IMPACT

Commentaire :

Cette section n'est pas obligatoire mais est vivement conseillée car elle permet d'identifier les différents intervenants et facilite le cas échéant la révision de l'AIPD.

Exemple :

Nom et Prénom	*Fonction*	*Rôle dans l'élaboration de l'AIPD*	*Date d'intervention*

2. INFORMATIONS GENERALES

Exemple :

Intitulé de la recherche	
Référence de la recherche	
Investigateur coordonnateur ou Responsable scientifique	

3. PIECES JOINTES

Commentaires :

Le cas échéant, établir la liste des pièces jointes à l'AIPD en précisant l'intitulé de la pièce ainsi que sa date d'édition ou sa version.

4. ETUDE DU CONTEXTE

4.1 Vue d'ensemble du traitement

4.1.1 Présentation générale du traitement concerné par l'AIPD

Commentaires :

Il existe trois catégories de recherches impliquant la personne humaine :

1° Les recherches interventionnelles qui comportent une intervention sur la personne non justifiée par sa prise en charge habituelle ;

2° Les recherches interventionnelles qui ne comportent que des risques et des contraintes minimes, dont la liste est fixée par arrêté du ministre chargé de la santé, après avis du directeur général de l'Agence nationale de sécurité du médicament et des produits de santé ;

3° Les recherches non interventionnelles qui ne comportent aucun risque ni contrainte dans lesquelles tous les actes sont pratiqués et les produits utilisés de manière habituelle.

Le projet peut également être une recherche n'impliquant pas la personne humaine.

Pour plus d'informations

https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032722870

Intranet Inserm : notamment

https://pro.inserm.fr/rubrique/support-a-la-recherche/droit-de-la-recherche/la-personne-humaine-et-la-recherche/la-personne-humaine-et-la-recherche-2

Résumé de la Recherche :

Commentaires :

Résumez de façon très synthétique la recherche objet du traitement, notamment au regard de l'état actuel des recherches portant sur la même thématique, sur une problématique contemporaine de santé etc…

Objectifs de la Recherche:

Commentaires :

Indiquez de façon très synthétique et compréhensible les objectifs de la recherche. Indiquez le cas échéant s'il s'agit d'objectifs nouveaux conférant au projet un caractère inédit.

Enjeux de la Recherche :

Commentaires :

Intérêt en terme de santé publique, Valorisation du projet.

Le cas échéant préciser, si l'étude est demandée par une autorité. Le cas échéant, positionner la recherche au regard des recherches antérieures ou en cours sur la même thématique.

4.1.2 Identification du responsable du traitement

Commentaire :

Le responsable du traitement est la personne physique ou la personne morale (par exemple l'AP-HP, l'Inserm, le CNRS), l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement. En d'autres termes, le responsable de traitement détermine les objectifs et la façon de les réaliser.

Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du RGPD, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations destinées à ces personnes, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis. Un point de contact pour les personnes concernées peut être désigné dans l'accord.

Dans cette section, identifier le responsable de traitement et présenter les responsables opérationnels du traitement

Les tâches et donc les responsabilités dévolues à chacun de ces responsables opérationnels doivent être clairement établies : Qui gère la collecte des données ? Qui héberge les données et les services ? Qui opère l'analyse des données ?

Exemple :

Le traitement de données à caractère personnel nécessaire à la mise en œuvre de l'étude est placé sous la responsabilité de l'Inserm, promoteur de la Recherche et responsable du traitement des données à caractère personnel.

Le traitement sera mis en œuvre sous la responsabilité opérationnelle du Docteur, investigateur principal (si étude monocentrique) /coordonnateur (si étude multicentrique) de la Recherche.

De plus, les responsables opérationnels suivants sont impliqués dans la réalisation de la Recherche et sont destinataires des données à caractère personnel pour la réalisation de tâches identifiées :

Identification du responsable opérationnel	*Tâches réalisées par le responsable opérationnel*

4.1.3 Identification des sous-traitants

Commentaire :

Le terme «sous-traitant» désigne ici la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel traitées, les catégories de personnes concernées, et les obligations et les droits du responsable du traitement.

Par principe, une unité Inserm n'est pas considérée comme sous-traitant mais comme responsable opérationnel de la mise en œuvre de tout ou partie du traitement.

Les tâches et donc les responsabilités dévolues à chacun des sous-traitants doivent être clairement établies.

Il est essentiel que le(s) contrat(s) de sous-traitance soi(en)t établi(s) de façon concomitante au PIA.

Exemple :

Les sous-traitants suivants interviennent dans le traitement des données :

Identification du sous-traitant	*Tâches confiées au sous-traitant*

Des contrats conformes aux dispositions de l'article 28 du RGPD seront conclus avec le(s) sous-traitant(s).

Pour plus d'informations : section 33 du Guide CNIL Base de connaissance

4.1.4 Textes et référentiels applicables au traitement

Commentaire :

La CNIL établit et publie des lignes directrices, recommandations ou référentiels destinés à faciliter la mise en conformité des traitements de données à caractère personnel avec les textes relatifs à la protection des données à caractère personnel et à procéder à l'évaluation préalable des risques par les responsables de traitement et leurs sous-traitants. Elle encourage l'élaboration de codes de conduite définissant les obligations qui incombent aux responsables de traitement et à leurs sous-traitants, compte tenu du risque inhérent aux traitements de données à caractère personnel pour les droits et libertés des personnes physiques, notamment des mineurs. Elle homologue et publie les méthodologies de référence destinées à favoriser la conformité des traitements de données de santé à caractère personnel. Elle prend en compte, dans tous les domaines de son action, la situation des personnes dépourvues de compétences numériques, et les besoins spécifiques des collectivités territoriales, de leurs groupements et des microentreprises, petites entreprises et moyennes entreprises.

Il s'agit ici d'identifier les référentiels applicables au traitement, utiles ou à respecter, notamment les codes de conduite approuvés (cf. art. 40 du [RGPD]) et certifications en matière de protection des données (cf. art. 42 du [RGPD]) dont politique de sécurité, normes juridiques sectorielles, méthodologie de référence.

Au titre des référentiels, des méthodologies de référence sont homologuées et publiées par la Commission nationale de l'informatique et des libertés. Les méthodologies de référence adoptées par la CNIL pour les recherches dans le domaine de la santé sont accessibles sur le site de la CNIL.

Exemple :

Le traitement des données est notamment encadré par :

- *le règlement (UE) 2016/679 du 27 avril 2016, dit Règlement Général sur la Protection des Données (Règlement (UE) 2016/679) ;*
- *la loi n° 78-17 du 6 janvier 1978 (78-17), relative à l'informatique, aux fichiers et aux libertés qui règlemente le recueil et l'utilisation de données personnelles dans le cadre de cette étude*
- *le décret n° 2019-536 du 29 mai 2019 modifié pris pour l'application de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;*
- *Les dispositions du code de la santé publique relatives aux recherches impliquant la personne humaine :*

Le référentiel est la MR001

4.1.5 Points de non-conformité à la méthodologie de référence (référence de la méthodologie à compléter)

Commentaire

Pour rappel, les traitements de données à caractère personnel dans le domaine de la santé (Articles 64 à 77 de la loi 78-17, modifiée), ne peuvent être mis en œuvre qu'après autorisation de la CNIL. Néanmoins, lorsque le traitement est conforme à une méthodologie de référence, il peut être mis en œuvre, sans autorisation, à la condition que son responsable adresse préalablement à la Commission nationale de l'informatique et des libertés une déclaration attestant de cette conformité.

Pour qu'un responsable de traitement puisse se prévaloir d'une méthodologie de référence, il doit respecter l'ensemble des conditions et modalités inscrites dans la méthodologie de référence. Il convient donc de procéder à une lecture attentive de ces méthodologies avant de s'en prévaloir :

https://www.cnil.fr/fr/recherches-dans-le-domaine-de-la-sante-la-cnil-adopte-de-nouvelles-mesures-de-simplification

S'il n'est pas possible de s'en prévaloir, il conviendra de préciser, à l'appui de la demande d'autorisation, les points de non-conformité à la méthodologie de référence applicable au traitement et justifier cette non-conformité.

Identifiez l'ensemble des points de non-conformité à la méthodologie de référence applicable au traitement.

Une attention toute particulière doit être portée à la rédaction de ce paragraphe qui doit pleinement convaincre la CNIL de la plus haute nécessité de déroger à la méthodologie de référence sur un ou plusieurs aspects.

Ainsi, lorsque le point de non-conformité à la MR consiste à recueillir une catégorie de donnée qui en est exclue, cela doit être justifiée scientifiquement de la façon la plus précise et aboutie possible.

Exemple :

Points de non-conformité à la méthodologie de référence MR001

Le traitement est conforme aux dispositions de la MR001 à l'exclusion des points de non-conformité suivants :

Point de non-conformité	***Justification de la non-conformités***
• *Recueil de la date de naissance complète, de l'identité complète, de la commune de résidence, de la religion, photographies permettant d'identifier un individu, recueil du NIR.*	

• *Un appariement des données avec le SNDS.* • *Une demande de dérogation à l'obligation d'information.*	

4.2 Présentation des données, processus et supports liés aux opérations de traitement associés

4.2.1 Catégories de personnes concernées

Commentaire :

Indiquez les catégories de personnes concernées par le traitement. Par exemple : patients, volontaires sains, personnes vulnérables telles que mineurs, personnes faisant l'objet d'une mesure de protection juridique…

Justifiez la raison pour laquelle il est nécessaire d'inclure les personnes dites vulnérables (ces personnes vulnérables sont notamment identifiées aux articles L1121-5 et suivants du Code de la Santé Publique)

Vérifier également le respect de la loi 78-17 puisque la loi contient des dispositions spécifiques notamment pour les mineurs, les personnes sous tutelle ou les majeurs protégés dont l'état ne leur permet pas de prendre seuls une décision personnelle éclairée.

https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000037823040

Le projet peut également conduire au traitement des données des personnels (médecin investigateur, ARC, etc.) impliquées dans sa réalisation. Il convient de le prendre en compte dans le présent document.

4.2.2 Catégories de données traitées

Commentaire : De manière générale : Listez les catégories de données à caractère personnel collectées et traitées.

Définissez pour chacune des données, les sources, les destinataires (les personnes y ayant accès dans le cadre de la recherche), et les durées de stockage.

Les sources de données se définissent comme les origines de données. Il peut s'agir des dossiers médicaux, de données obtenues directement auprès de la personne par voie de questionnaire, de résultats obtenus suite à une analyse etc…

Toutes les données traitées à des fins de recherche doivent être présentées ici ; y compris celles qui sont collectées dans le cadre des soins et réutilisées secondairement dans le cadre de la recherche.

Il convient de commencer par les données susceptibles d'identifier directement un individu (identité complète, adresse de résidence, NIR). Les destinataires des données directement ou indirectement identifiantes doivent être indiqués de façon exhaustive.

Pour rappel, une donnée à caractère personnel correspond à toute information se rapportant à une personne physique identifiée ou identifiable; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques

propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Les données directement identifiantes ne doivent être traitées et conservées que pour une durée la plus courte possible. Le maintien des données sous une forme directement identifiante doit être justifié. Lorsque les données identifiantes sont recueillies et conservées, il est conseillé de les conserver dans une base distincte des autres données de la recherche.

Cette organisation est à faire figurer impérativement dans l'AIPD.

Pour la distinction entre Types de données et Catégories de données voir Section 1.1 Guide CNIL Les Bases des connaissances

4.2.3 Destinataires

Commentaire :

Les destinataires peuvent être les services internes du responsable du traitement ayant besoin de traiter les données ainsi que les sous-traitants ou les responsables conjoints du traitement.

Exemple :

Les destinataires sont

Les responsables opérationnels suivants

- *L'unité mixte de recherche U5437 en charge de réaliser la tâche A*
- *L'unité mixte de recherche U 6589 en charge de réaliser la tâche B*

Les sous-traitants suivants :

- *Société A en charge de réaliser la tâche C en application du contrat de sous-traitance conclu en application de l'article 28 du RGPD*
- *Société B en charge de réaliser la tâche D en application du contrat de sous-traitance conclu en application de l'article 28 du RGPD*

4.2.4 Durée de conservation

Commentaire :

Il convient de préciser la durée de conservation et de préciser le cas échéant s'il s'agit d'une conservation en base active ou pour archivage.

4.2.5 Tableau de synthèse

Commentaire : il est possible de présenter les informations sous la forme d'un tableau. Les sections 4.2.1, 4.2.2, 4.2.3 et 4.2.4 seront à supprimer en conséquence.

Exemple :

Types de données	**Catégorie de données**	**Directement identifiantes/indirectement identifiantes**	**Sources**	**Destinataires**	**Durée de conservation en base active (à exprimer en années : exemple : de 2022 à 2026)**	**Durée de conservation (archive) (à exprimer en années : exemple : de 2026 à 2041)**

4.2.6 Description synthétique du cycle de vie des données

Insérer un schéma afin de présenter le cycle de vie des données

4.2.7 Description des processus fonctionnels et des supports des données

Commentaires :

Il conviendra ici d'identifier les différents processus de traitement mis en œuvre puis de les décrire.

Cette description est à mettre en relation avec le tableau de synthèse relevant de la section précédente. Il s'agira ici de décrire les processus de traitement mis en place pour chacune des catégories ou pour un ensemble de catégorie de données.

La description du processus sera l'occasion de mener une réflexion sur les moyens d'assurer la conformité du traitement avec le RGPD notamment pour les aspects liés à la sécurité des traitements et à la confidentialité des données.

Il sera utile de distinguer parmi les processus, ceux portant sur les données directement identifiantes et ceux mis en œuvre pour les données non directement identifiantes.

Plusieurs supports des données peuvent être mobilisés dans le cadre d'une recherche : support papier et support information. Le choix du support devra également être fait en fonction des risques liés à l'usage du support. Ainsi l'usage de clefs USB comme support est vivement déconseillé.

<u>En cas de sous-traitance, il conviendra de prévoir un paragraphe par sous-traitant.</u>

Par exemple:

- Support papier

Détaillez de façon exhaustive tous les documents papiers sur lesquels des données de la recherche seront recueilles, cela peut être des questionnaires, des cahiers d'observation papiers, des cahiers de laboratoires, des prises de notes, des photographies, des cahiers d'enregistrement etc.

L'ensemble de ces supports papiers doit être listé.

- Support informatique

Détaillez de façon exhaustive tous les supports informatiques sur lesquels des données de la recherche seront recueillies. Les données peuvent être collectées via des questionnaires en ligne, des CRF électroniques, des cahiers de laboratoires, des prises de notes, des photographies, des cahiers d'enregistrement, des bases de données, des données recueillies via des applications ou des objets connectés etc.

L'ensemble de ces supports électroniques doit être listé.

Indiquez si le traitement nécessite un recours à un stockage temporaire. Cela peut être le cas si la recherche s'appuie sur des objets connectés dont les données sont stockées temporairement sur un serveur dans l'attente de leur envoi vers la base de donnée de l'étude.

Indiquez où se trouve(nt) le ou les supports électroniques concerné(s), les modalités d'accès physique à ce ou ces supports (notamment accessibilité de l'étage, bureau fermé à clé, ouverture du poste par mot de passe), indiquez si ce poste permet un accès à distance à la base de données de l'étude. Indiquez qui porte la responsabilité du parc informatique. Indiquez notamment, le cas échéant, si le PC est dédié à une activité Inserm.

4.2.8 Description des processus fonctionnels et des supports des données (tableau)

L'article 4.2.7 peut être présenté sous la forme d'un tableau.

En cas de sous-traitance, il conviendra de prévoir un tableau par sous-traitant.

Exemple :

Processus	*Description détaillée du processus*	*Support des données concernées*

5. ETUDE DES PRINCIPES FONDAMENTAUX

5.1 Evaluation des mesures garantissant la proportionnalité et la nécessité du traitement

5.1.1 Explication et justification des finalités du traitement

Commentaire :

Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

Les finalités du traitement étant déterminées dans le protocole de la recherche, notamment au niveau des objectifs principaux il convient de reporter dans cette section les éléments présents dans le protocole.

Par exemple

Améliorer à terme la prise en charge des patients
Orienter les décisions en termes de santé publique
Améliorer les diagnostics / les traitements
Aboutir à de nouvelles recommandations en terme de santé publique.

5.1.2 Les fondements qui rendent le traitement licite

Commentaire :

Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie:

- la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;
- le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;
- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;
- le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;
- le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Pour l'Inserm, le traitement réalisé à des fins de recherche s'inscrit dans les missions de l'Inserm. D'autres fondements, dont le consentement, sont possibles.

Exemple

Pour les traitements mis en œuvre à des fins de recherche dans le domaine de la santé :

Le traitement de données à caractère personnel nécessaire à la mise en œuvre de l'étude répond à l'exécution d'une mission d'intérêt public dont est investi l'Inserm (RGPD, art. 6.1.e) qui justifie le traitement des données personnelles de santé des participants à des fins de recherche scientifique. (RGPD, art. 9.2.j).

Cette étude est une recherche impliquant la personne humaine (RIPH) telle que définie au 1° de l'article L. 1121-1 du code de la santé publique.

A ce titre et conformément aux dispositions de l'article précité, le comité de protection des personnes (CPP) a rendu un avis favorable et l'Agence nationale de sécurité du médicament et des produits de santé (ANSM) a autorisé la recherche.

OU

Cette étude n'est pas une recherche impliquant la personne humaine (RIPH) au sens du Code de la Santé Publique. Elle est qualifiée de recherche prospective/rétrospective non interventionnelle. Il ne s'agit pas d'une recherche organisée et pratiquée sur l'être humain en vue du développement des connaissances biologiques ou médicales.

A ce titre et conformément aux dispositions de l'article précité, le Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé CESREES a rendu un avis favorable.

5.1.3 Respect du principe de minimisation des données : collecte adéquate, pertinente et limitée à ce qui est nécessaire au regard des finalités pour lesquelles les données sont traitées

Commentaire : (issu notamment du guide CNIL : base de connaissance : https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf)

La minimisation permet d'être conforme à l'article 6 de la loi informatique et libertés et à l'article 5.1(c) du règlement général sur la protection des données (RGPD) ; réduire la gravité des risques en limitant la collecte des données à caractère personnel au strict nécessaire au regard d'une finalité définie ; éviter la collecte de données non nécessaires, l'utilisation de données sans lien avec la finalité et des impacts excessifs pour les personnes.

Minimisation de la collecte

• Justifier de la collecte de chaque donnée.

• Bien faire la distinction entre les données directement identifiantes et les données indirectement identifiantes (pseudonymes).

• Éviter les champs de saisie en texte libre (ex : zones « commentaires »), en raison du risque que les utilisateurs y consignent des informations ne respectant pas les principes de minimisation. On préférera donc des champs de saisie à base de listes déroulantes. Si on ne peut éviter la saisie de texte libre, une sensibilisation des utilisateurs devra être faite quant à

l'usage de ces champs, vis-à-vis des conditions générales du service et vis-à-vis de la loi (pas de propos injurieux, pas de données sensibles non déclarées, etc.).

Vérifier que les données sont adéquates, pertinentes et non excessives au regard de la finalité poursuivie, et ne pas les collecter dans le cas contraire. Au regard de la finalité du traitement, justifier en quoi chaque catégorie de données est indispensable, et enfin écarter toute donnée qui ne rend pas la finalité irréalisable ; si besoin, revoir la finalité si des données sont nécessaires à autre chose que la finalité initialement prévue.

Vérifier que les données ne font pas apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale, ainsi que les données relatives à la santé ou à la vie sexuelle, et ne pas les collecter dans le cas contraire à moins d'être dans des circonstances d'exception (consentement, intérêt public, conformément à l'article 8 de la loi informatique et libertés et à l'article 9 du RGPD).

En raison du caractère sensible des données relatives à un mineur et en tenant compte du principe de loyauté de collecte vis-à-vis d'un utilisateur vulnérable, la collecte de données concernant un enfant, ses parents ou sa famille devra être particulièrement limitée et justifiée.

Minimisation de la donnée après collecte

Il est également possible de minimiser la donnée en procédant à son traitement.

Par exemple : Réduire la sensibilité par transformation. Celles-ci peuvent être converties en une forme moins sensible ou pseudonymisée (par exemple, la date de naissance peut faire l'objet d'un traitement afin de transformer cette information en tranche d'âge).

Réduire l'accumulation de données : le système peut être structuré en parties indépendantes avec des fonctions de contrôle d'accès distinctes. Les données peuvent également être réparties entre ces sous-systèmes indépendants et contrôlées par chaque sous-système en utilisant différents mécanismes de contrôle d'accès. Si un sous-système est compromis, les impacts sur l'ensemble des données peuvent ainsi être réduits.

Restreindre l'accès aux données : le système peut limiter l'accès aux données selon le principe du « besoin d'en connaître ». Le système peut séparer les données sensibles et appliquer des politiques de contrôle d'accès spécifiques. Le système peut aussi chiffrer les données sensibles pour protéger leur confidentialité lors de la transmission et du stockage.

Limiter l'envoi des documents électroniques contenant des données.

Utiliser un outil d'effacement sécurisé pour les documents électroniques.

Pour en savoir plus : section 25 du Guide PIA, les bases de connaissances Édition février 2018

Exemple :

Catégories de données	Détail des données traitées	Justification du besoin et de la pertinence des données	Mesures de minimisation

5.1.4 Explication et justification de la qualité des données

Commentaire : De manière générale, vous devez ici décrire les mesures prévues pour vous assurer de la qualité des données c'est-à-dire que les données sont exactes et tenues à jour (cf. art. 5.1 (d) du RGPD).

Indiquez ici comment les personnes qui recueillent les données sont formées / sensibilisés à l'importance de la qualité de collecte des données. Indiquez si ces personnes ont un référent auquel elles peuvent s'adresser si elles ont une question particulière en lien avec la collecte des données.

Détailler notamment le cas échéant :

- les modalités mises en œuvre pour éviter les erreurs de collecte s'agissant des supports papier.
- les modalités mises en œuvre pour éviter les erreurs de saisie informatique des données
- les modalités de double relecture, l'audit, de contrôles de cohérence
- la traçabilité des modifications des données
- le lien entre la donnée qui identifie une personne et les données qui concernent cette personne.

Exemple :

Intitulé de la mesure mises en œuvre pour s'assurer de la qualité des données	Explication et justification de la mesure

Pour en savoir plus : section 29 du Guide Bases de Connaissances

5.1.5 Durées de conservation en base active et d'archivage des données

Commentaire : Précisez la durée de conservation. Le cas échéant, distinguer la durée de conservation en base active puis la durée d'archivage pour chaque type de données et justifiez ces durées. Expliquez en quoi ces durées sont nécessaires à l'accomplissement des finalités de votre traitement, à défaut d'une autre obligation légale imposant une conservation spécifique.

Attention à ne pas oublier les données techniques. Ainsi, par exemple, les traces fonctionnelles ou les journaux techniques (logs à un outil informatique) constituent des données à caractère personnel.

Exemple :

*Durée de **conservation en base active** :*

- De l'inclusion du premier participant à la validation du rapport final (1 an après la fin de la recherche). En d'autres termes, les données seront conservées en base active de 20XX à 20XX.

-

***Durée d'archivage des données** :*

- De la fin de la période de conservation en base active à la fin de l'archivage des documents de la recherche (différentes selon les types de recherche). En d'autres termes, les données seront conservées en archivage de 20XX à 20XX.

Exemple

Type de données	*Durée de conservation*	*Justification*	*Mécanisme de suppression à la fin de la conservation (le cas échéant)*

Pour en savoir plus : *section 9 du Guide CNIL Base de connaissance*

5.2 Évaluation des mesures protectrices des droits des personnes des personnes concernées

Identifier ou déterminer, et décrire, les mesures retenues (existantes ou prévues) pour respecter les exigences suivantes (nécessitant d'expliquer comment il est prévu de les mettre en œuvre).

Pour les recherches dans le domaine de la santé, les informations à reporter dans l'AIPD sont celles habituellement présentes dans les notices d'information/ consentement/ non-opposition.

Pour en savoir plus : consulter les pages de l'intranet Inserm pour le modèle de document d'information et de consentement : https://pro.inserm.fr/rubrique/recherche-responsable/donnees-personnelles/outils/information-des-participants

5.2.1 Information des personnes concernées par le traitement

Commentaire :

Le contenu de l'information à délivrer à une personne est fixée notamment par le RGPD et ses articles 13 (Informations à fournir lorsque les données à caractère personnel ont été collectées auprès de la personne concernée) et 14 (Informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée). On retiendra les éléments suivants (liste non exhaustive) :

- Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement lui fournit, au moment où les données en question sont obtenues, toutes les informations suivantes:
    - l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement
    - le cas échéant, les coordonnées du délégué à la protection des données;
    - les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement;
    - les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent; et
    - le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition;
    - la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;
    - l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données;
    - le cas échéant, l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci;
    - le droit d'introduire une réclamation auprès d'une autorité de contrôle;
- Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée au paragraphe 2.

Pour en savoir plus : *https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679#d1e2207-1-1*

Pour en savoir plus : *section 22 Information des personnes concernées (traitement loyal et transparent) du Guide CNIL Bases de connaissance*

Pour en savoir plus : consulter les pages de l'intranet Inserm pour le modèle de document d'information et de consentement : https://pro.inserm.fr/rubrique/recherche-responsable/donnees-personnelles/outils/information-des-participants

Commentaire

En plus des dispositions du RGPD, il convient de prendre en considération les dispositions du Code de la Santé Publique et de la loi « informatique et libertés », qui peuvent prévoir, notamment pour certaines situations ou pour certaines catégories de personnes, dont les

personnes dites vulnérables, des modalités et des conditions spécifiques d'information, de consentement ou de non opposition.

Le Code de la Santé Publique précise les conditions et modalités selon lesquelles il est possible de solliciter des personnes vulnérables : Voir notamment les articles L112-1-5 et suivants.

Pour chacune des catégories de personne susceptibles d'être incluses dans la Recherche, ce même code précise les modalités d'information et d'expression de la volonté : voir notamment les articles L1122-1 et suivants du Code de la Santé Publique.

Enfin, la loi 78-17 dite informatique et liberté comporte des dispositions en la matière : Voir articles 70 et suivants de la loi 78-17.

Exemple :

Si le traitement bénéficie d'une exemption au droit d'information, prévue par l'article 32 de la loi « informatique et libertés » et les articles 12, 13 et 14 du RGPD

Dispense d'information des personnes concernées	*Justification*

Si le traitement est soumis au droit d'information, prévue par la loi 78-17 ou le RGPD :

Mesure pour le droit à l'information	*Modalités de mise en œuvre*	*Justification des modalités ou de l'impossibilité de leur mise en oeuvre*

5.2.2 Détermination et description des mesures pour le recueil du consentement (le cas échéant)

Commentaires :

Il convient ici de distinguer :

- Le consentement ou l'accord de participation à la recherche fondé sur les dispositions du Code de la Santé Publique :Pour cette question, se reporter aux dispositions des articles L1122-1 du Code de la Santé Publique. Se reporter également pour la

génétique aux dispositions des articles L1130-1 et suivants du Code de la Santé Publique.

- Le consentement des personnes au traitement des données à caractère personnel les concernant fondé sur les articles 7 et 8 du RGPD

Le RGPD définit le consentement de la personne concernée comme toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Dans les cas où le traitement repose sur le consentement (base légale du traitement), le responsable du traitement doit être en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.

Pour en savoir plus : *section 30 Recueil du consentement du Guide CNIL Bases de connaissance :*

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A302%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

Pour en savoir plus : consulter les pages de l'intranet Inserm pour le modèle de document d'information et de consentement : https://pro.inserm.fr/rubrique/recherche-responsable/donnees-personnelles/outils/information-des-participants

5.2.3 Modalités d'exercice par les personnes concernées de leur droit d'accès et de leur droit à la portabilité

Commentaire :

Le droit d'accès est la possibilité pour la personne concernée d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel ainsi que des informations relatives aux finalités du traitement, les catégories de données à caractère personnel concernées, les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, en particulier les destinataires qui sont établis dans des pays tiers ou les organisations internationales.

Il conviendra de s'assurer que le droit d'accès pourra toujours s'exercer ; il faut donc bien prendre en considération la durée de conservation des données et mettre en place une organisation permettant pendant toute cette durée, l'exercice des droits.

Pour en savoir plus : section 13 Exercice des droits d'accès et à la portabilité G*uide CNIL Bases de connaissance*

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A152%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

Pour en savoir plus : consulter les pages de l'intranet Inserm pour le modèle de document d'information et de consentement : https://pro.inserm.fr/rubrique/recherche-responsable/donnees-personnelles/outils/information-des-participants

5.2.4 Modalités d'exercice par les personnes concernées de leur droit de rectification et droit à l'effacement (droit à l'oubli)

Commentaire :

L'objectif est de garantir aux personnes la possibilité de rectifier, compléter, mettre à jour, verrouiller ou supprimer des données à caractère personnel qui les concernent.

Déterminer les moyens pratiques qui vont être mis en œuvre pour permettre l'exercice du droit de rectification. Ce droit doit pouvoir être exercé le plus rapidement possible, sans jamais excéder deux mois, dans une forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches à effectuer ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais.

Il conviendra de s'assurer que ce droit pourra toujours s'exercer ; il faut donc bien prendre en considération la durée de conservation des données et mettre en place une organisation permettant pendant toute cette durée, l'exercice de ce droit.

Pour en savoir plus : section 12 Exercice des droits de rectification et d'effacement G*uide CNIL Bases de connaissance*

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A143%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

Pour en savoir plus : consulter les pages de l'intranet Inserm pour le modèle de document d'information et de consentement : https://pro.inserm.fr/rubrique/recherche-responsable/donnees-personnelles/outils/information-des-participants

5.2.5 Modalités d'exercice par les personnes concernées de leur droit de limitation et droit d'opposition

Commentaire :

Le droit à la limitation des données est un droit qui complète les autres droits (rectification, opposition…). L'objectif est de garantir aux personnes la possibilité de s'opposer à l'utilisation de données à caractère personnel qui les concernent et permettre à l'utilisateur d'exiger le « gel » du traitement de ses données, comme mesure conservatoire le temps d'en vérifier la légitimité dudit traitement.

Pour en savoir plus : section 11 Exercice des droits de limitation et d'opposition - G*uide CNIL Bases de connaissance*

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A132%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

Pour en savoir plus : consulter les pages de l'intranet Inserm pour le modèle de document d'information et de consentement : https://pro.inserm.fr/rubrique/recherche-responsable/donnees-personnelles/outils/information-des-participants

5.2.6 Détermination et description des mesures pour la sous-traitance

Commentaire :

Le sous-traitant est une personne physique ou morale, autorité publique, service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement (Article 4.8 du RGPD).

Le sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne peut pas traiter ces données, excepté sur instruction du responsable du traitement, à moins d'y être obligé par le droit de l'Union ou le droit d'un État membre (Article 29 du RGPD).

Pour chaque sous-traitant, décrivez le périmètre de ses responsabilités et indiquez les références aux contrats, codes de conduite et certifications qui fixent ses obligations.

Un contrat de sous-traitance doit être conclu avec chacun des sous-traitants, précisant l'ensemble des éléments prévus à l'article 28 du RGPD et notamment : durée du traitement, périmètre, finalité, des instructions de traitement documentées, l'autorisation préalable en cas de recours à un sous-traitant, mise à disposition de toute documentation apportant la preuve du respect du RGPD, notification dans les meilleurs délais de toute violation de données, etc.

Exemple :

Nom du sous-traitant	Finalité	Périmètre de la sous-traitance = tâches sous-traités	Durée du traitement

5.2.7 Détermination et description des mesures pour le transfert de données en dehors de l'Union européenne

Commentaire : le transfert visé par cette section ne concerne que le transfert de données en dehors de l'Union Européenne. Un transfert, vers un pays tiers ou à une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si, sous réserve des autres dispositions du RGPD, les conditions définies dans le chapitre V du RGPD consacré à ces transfert sont respectées par le responsable du traitement et le sous-traitant, y compris pour les transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation

internationale vers un autre pays tiers ou à une autre organisation internationale. Le dispositif mis en place vise à ce que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis par le transfert

La CNIL met à disposition une page sur son site : En cliquant sur ce lien, vous accèderez à une carte interactive vous permettant de visualiser les différents niveaux de protection des données des pays dans le monde et les mesures à mettre en place : https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

Il conviendra de détailler le lieu géographique de stockage des différentes données du traitement. En fonction du pays concerné, justifier le choix d'un hébergement éloigné et indiquer les modalités d'encadrement juridique mises en œuvre afin d'assurer une protection adéquate aux données faisant l'objet d'un transfert transfrontalier.

Les personnes concernées doivent être informées de la possibilité d'un transfert de données hors de l'Union Européenne et renvoyées aux garanties appropriées ou adaptées (ex : clauses contractuelles types adoptées par la Commission européenne, clauses contractuelles ad hoc…) et aux moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition.

Pour en savoir plus : section 41 Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne - G*uide CNIL Bases de connaissance*

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A416%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C219%2C0%5D

6. ETUDE DES RISQUES LIES A LA SECURITE DES DONNEES

Commentaire : (Extrait du guide CNIL « Pia la méthode, édition février 2018 »)

Un risque est un scénario hypothétique qui décrit un événement redouté et toutes les menaces qui permettraient qu'il survienne. Plus précisément, il décrit :

- comment des sources de risques (ex. : un salarié soudoyé par un concurrent)
- pourraient exploiter les vulnérabilités des supports de données (ex. : le système de gestion des fichiers, qui permet de manipuler les données)
- dans le cadre de menaces (ex. : détournement par envoi de courriers électroniques)
- et permettre à des événements redoutés de survenir (ex. : accès illégitime à des données)
- sur les données à caractère personnel (ex. : fichier des clients)
- et ainsi provoquer des impacts sur la vie privée des personnes concernées (ex. : sollicitations non désirées, sentiment d'atteinte à la vie privée, ennuis personnels ou professionnels).

Le niveau d'un risque est estimé en termes de gravité et de vraisemblance :

- la gravité représente l'ampleur d'un risque. Elle dépend essentiellement du caractère préjudiciable des impacts potentiels ;
- la vraisemblance traduit la possibilité qu'un risque se réalise. Elle dépend essentiellement des vulnérabilités des supports face aux menaces et des capacités des sources de risques à les exploiter.

Pour la mise en œuvre des mesures techniques, il est conseillé de s'appuyer sur des dispositifs ou des infrastructures déjà constitués en conformité avec les normes ou référentiels en vigueur.

On rappellera le besoin de prendre connaissance de documents relatifs à la sécurité informatique à l'Inserm (sur l'intranet Inserm)

https://pro.inserm.fr/rubrique/services-et-supports-informatiques/securite-informatique/securite-informatique

Et notamment la Politique des Systèmes d'Information de Recherche formalisant les règles de sécurité des systèmes d'information des structures recherche de l'Inserm.

https://pro.inserm.fr/wp-content/uploads/2021/03/PSSI-recherche-V1.1.pdf

6.1 Mesures existantes ou prévues

Dans cette section, si l'étude est multicentrique (avec plusieurs centres d'inclusion donc), vous devez pour chaque sous-paragraphe décrire les mesures prises au niveau de chacun des centres et au niveau de la coordination qui travaillera sur la base de données globale.

6.1.1 Mesures portant spécifiquement sur les données du traitement

6.1.1.1 Chiffrement

Commentaire : Le chiffrement d'un message permet de garantir que seuls l'émetteur et le(s) destinataire(s) légitime(s) d'un message en connait/connaissent le contenu. Une fois chiffré, faute d'avoir la clé spécifique, un message est inaccessible et illisible, que ce soit par les humains ou les machines.

On se référera utilement au Guide « PIA, les bases de connaissances Édition février 2018 » et plus spécifiquement sa section 4 consacrée au chiffrement qui aborde les mesures génériques et les spécificités suivantes :

- Spécificités pour un chiffrement symétrique
- Spécificités pour un chiffrement asymétrique (ou à clé publique)
- Spécificités pour le chiffrement de matériels
- Spécificités pour le chiffrement de bases de données
- Spécificités pour le chiffrement de partitions ou de conteneurs
- Spécificités pour le chiffrement de fichiers isolés
- Spécificités pour le chiffrement de courriers électroniques
- Spécificités pour le chiffrement d'un canal de communication

Concernant le chiffrement symétrique et le chiffrement asymétrique.

- Le chiffrement symétrique permet de chiffrer et de déchiffrer un contenu avec la même clé, appelée alors la « clé secrète ». Le chiffrement symétrique est particulièrement rapide mais nécessite que l'émetteur et le destinataire se mettent d'accord sur une clé secrète commune ou se la transmettent par un autre canal. Celui-ci doit être choisi avec précautions, sans quoi

la clé pourrait être récupérée par les mauvaises personnes, ce qui n'assurerait plus la confidentialité du message.

- Le chiffrement asymétrique suppose que le (futur) destinataire est muni d'une paire de clés (clé privée, clé publique) et qu'il a fait en sorte que les émetteurs potentiels aient accès à sa clé publique. Dans ce cas, l'émetteur utilise la clé publique du destinataire pour chiffrer le message tandis que le destinataire utilise sa clé privée pour le déchiffrer. Parmi ses avantages, la clé publique peut être connue de tous et publiée. Mais attention : il est nécessaire que les émetteurs aient confiance en l'origine de la clé publique, qu'ils soient sûrs qu'il s'agit bien de celle du destinataire. Autre point fort : plus besoin de partager une même clé secrète ! Le chiffrement asymétrique permet de s'en dispenser mais il est plus lent.

Dans le cas où la mesure est choisie pour traiter des risques, décrivez les moyens mis en œuvre pour assurer la confidentialité des données conservées (en base de données, dans des fichiers plats, dans les sauvegardes, etc.) ainsi que les modalités de gestion des clés de chiffrement (création, conservation, modification en cas de suspections de compromission, etc.).

Détaillez les moyens de chiffrement employés pour les flux de données (VPN, TLS, etc.) intégrés dans le traitement.

Pour de plus amples informations sur le chiffrement : consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 4

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A59%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.1.2 Anonymisation / Pseudonymisation

Commentaire :

Le but d'une solution d'anonymisation est de faire perdre le caractère identifiant des données à caractère personnel. Une solution d'anonymisation doit être construite au cas par cas et adaptée aux usages prévus. Pour aider à évaluer une bonne solution d'anonymisation, le G29 propose trois critères :
- L'individualisation : est-il toujours possible d'isoler un individu ?
- La corrélation : est-il possible de relier entre eux des ensembles de données distincts concernant un même individu ?
- L'inférence : peut-on déduire de l'information sur un individu ?

Ainsi : un ensemble de données pour lequel il n'est possible ni d'individualiser ni de corréler ni d'inférer est a priori anonyme ;

Un ensemble de données pour lequel au moins un des trois critères n'est pas respecté ne pourra être considéré comme anonyme qu'à la suite d'une analyse détaillée des risques de ré-identification.

Dans le cadre d'une RIPH avec collecte active de données, l'anonymisation ne peut raisonnablement pas être envisagée.

La pseudonymisation consiste à traiter des données à caractère personnel de telle façon que celles-ci ne peuvent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires sont conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.

La pseudonymisation réduit le risque de mise en corrélation d'un ensemble de données avec l'identité originale d'une personne concernée; à ce titre, c'est une mesure de sécurité utile, mais non une méthode d'anonymisation.

Dans le cas où la mesure est choisie pour traiter des risques, décrivez les mécanismes de pseudonymisation les garanties qu'ils apportent contre une ré-identification éventuelle et à quelle fin ils sont mis en œuvre.

Pour de plus amples informations sur l'anonymisation : consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 2

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A45%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.1.3 Cloisonnement

Commentaire : le cloisonnement est l'ensemble de méthodes permettant de réduire la possibilité de corréler des données à caractère personnel et de provoquer une violation de l'ensemble des données. Le cloisonnement des données s'apprécie par rapport au reste du système d'information.

Dans le cas où la mesure est choisie pour traiter des risques, indiquez les mesures et modalités du cloisonnement du traitement

Pour de plus amples informations : Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 5 cloisonnement

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A75%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.1.4 Contrôle des accès logiques

Commentaire : Le contrôle d'accès logique est un système de contrôle d'accès à un système d'information. Il est souvent couplé avec le contrôle d'accès physique et permet de restreindre le nombre d'utilisateurs du système d'information. Il consiste à limiter les risques que des personnes non autorisées accèdent aux données à caractère personnel sous forme numérique.

Pour cela, il convient de :

1. Gérer les privilèges des utilisateurs sur les données notamment via les mesures suivantes :

- Définir des profils d'habilitation dans les systèmes en séparant les tâches et les domaines de responsabilité, afin de limiter l'accès des utilisateurs aux seules données strictement nécessaires à l'accomplissement de leurs missions.
- Identifier toute personne ayant un accès légitime aux données (employés, contractants et autres tiers) par un identifiant unique.
- Limiter l'accès aux outils et interfaces d'administration aux personnes habilitées.
- Limiter l'utilisation des comptes permettant de disposer de privilèges élevés aux opérations qui le nécessitent.
- Limiter l'utilisation des comptes « administrateurs » au service en charge de l'informatique et ce, uniquement pour les actions d'administration qui le nécessitent.
- Journaliser les informations liées à l'utilisation des privilèges.
- Retirer les droits des employés, contractants et autres tiers dès lors qu'ils ne sont plus habilités à accéder à un local ou à une ressource ou à la fin de leur contrat, et les ajuster en cas de changement de poste. Pour les personnes ayant un compte temporaire (stagiaire, prestataire...), configurer une date d'expiration à la création du compte
- Réaliser une revue annuelle des habilitations afin d'identifier et de supprimer les comptes non utilisés et de réaligner les droits accordés sur les fonctions de chaque utilisateur.

2. Authentifier les personnes désirant accéder aux données
3. Gérer les authentifiants

Indiquez ici comment les profils utilisateurs sont définis et attribués. Précisez les moyens d'authentification mis en œuvre. Le cas échéant, précisez les règles applicables aux mots de passe (longueur minimale, structure obligatoire, durée de validité, nombre de tentatives infructueuses avant blocage du compte, etc.).

Recommandations de la CNIL : Le mot de passe doit être constitué de 8 caractères, devra contenir au moins 1 chiffre, 1 lettre en minuscule et 1 lettre en majuscule. Il devra être renouvelé tous les 6 mois. De plus, l'accès au compte devra temporairement être bloqué au bout de 3 échecs de connexion.

Pour de plus amples informations

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 8 Contrôle des accès logiques :

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A99%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

Voir la délibération de la CNIL n°2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots : de passe :

6.1.1.5 Journalisation et traçabilité

Commentaire : La journalisation est le dispositif permettant d'enregistrer des actions effectuées sur le système informatique afin de pouvoir identifier un accès frauduleux ou une utilisation abusive de données personnelles, ou de déterminer l'origine d'un incident. Pour ce faire, mettre en place un système de journalisation applicative permettant de conserver une trace des accès et modifications de données opérés par les utilisateurs et du moment où ils ont eu lieu. Dans tous les cas, il ne faut pas conserver ces éléments pendant une durée excessive.

Indiquez ici si des événements sont journalisés et la durée de conservation de ces traces.

Indiquez s'il existe des mesures mises en place pour être capable de détecter les incidents concernant des données à caractère personnel de façon précoce et de disposer d'éléments exploitables pour les étudier ou pour fournir des preuves dans le cadre d'enquêtes (architecture et politique de journalisation, respect des obligations en matière de protection des données à caractère personnel, etc.).

Pour de plus amples informations

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 42 traçabilité (journalisation) :

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A427%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.1.6 Contrôle d'intégrité

Commentaire : ce contrôle doit permettre d'*être alerté en cas de modification non désirée ou de disparition de données à caractère personnel (fonction de hachage, code d'authentification de message, signature électronique, prévenir les injections SQL, etc.).*

Indiquez ici si des mécanismes de contrôle d'intégrité des données stockées sont mis en œuvre, lesquels et à quelle fin. Détaillez les mécanismes de contrôle d'intégrité employés sur les flux de données

Pour de plus amples informations

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 7 Contrôle d'intégrité) :

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A87%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.1.7 Archivage

Commentaire : Décrivez ici le processus de gestion des archives (versement, stockage, consultation, etc.) relevant de votre responsabilité. Précisez les rôles en matière d'archivage (service producteur, service versant, etc.) et la politique d'archivage. Indiquez si les données sont susceptibles de relever des archives publiques.

Pour de plus amples informations

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 3 Archivage

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A50%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.1.8 Sécurisation des documents papiers

Commentaire : Si des documents papiers contenant des données sont utilisés dans le cadre du traitement, indiquez ici comment ils sont imprimés, stockés, détruits et échangés.

Pour de plus amples informations

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 38 sécurité des documents papier

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A393%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.2 Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre

6.1.2.1 Sécurisation de l'exploitation

Commentaire : Dans le cas où la mesure est choisie pour traiter des risques, décrivez ici comment les mises à jour des logiciels (systèmes d'exploitation, applications, etc.) et l'application des correctifs de sécurité sont réalisées.

Politiques permettant de limiter la vraisemblance et la gravité des risques visant les biens supports utilisés en exploitation (documenter les procédures d'exploitation, inventaire et mise à jour des logiciels et matériels, correction des vulnérabilités, duplication des données, limiter l'accès physique au matériel, etc.).

Le cas échéant, il convient de créer, documenter et diffuser des procédures d'exploitations.

Pour de plus amples informations

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 36 Sécurité de l'exploitation

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A363%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.2.2 Lutte contre les logiciels malveillants

Commentaire : Dans le cas où la mesure est choisie pour traiter des risques, précisez si un antivirus est installé et régulièrement mis à jour sur tous les postes. L'objectif est de protéger les accès vers des réseaux publics (Internet) ou non maîtrisés (partenaires), ainsi que les postes de travail et les serveurs contre les codes malveillants qui pourraient affecter la sécurité des données à caractère personnel (antivirus, firewall, proxy, anti-spyware, remontée des événements de sécurité, etc.).

Pour de plus amples informations

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 23 lutte contre les logiciels malveillants

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A243%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.2.3 Gestion des postes de travail

Commentaire : dans le cas où la mesure est choisie pour traiter des risques, détaillez ici les mesures prises afin de diminuer la possibilité que les caractéristiques des logiciels (systèmes d'exploitation, applications métiers, logiciels bureautiques, paramétrages…) ne soient exploitées pour porter atteinte aux données à caractère personnel (mises à jour, protection physique et des accès, travail sur un espace réseau sauvegardé, contrôleurs d'intégrité, journalisation, etc.).

La notion de poste de travail englobe notamment les postes nomades, les téléphones mobiles ou les tablettes

Détaillez également les mesures mises en œuvre sur les postes de travail (verrouillage automatique, pare-feu, etc.).

Recommandations de la CNIL : Le mot de passe du poste de travail doit être constitué de 8 caractères, devra contenir au moins 1 chiffre, 1 lettre en minuscule et 1 lettre en majuscule. Il devra être renouvelé tous les 6 mois. De plus, l'accès au compte devra temporairement être bloqué au bout de 3 échecs de connexion.

Pour de plus amples informations

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 9 Gestion des postes de travail

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A194%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.2.4 Sécurité des sites web

Commentaire : dans le cas où la mesure est choisie pour traiter des risques, indiquez ici si les "recommandations pour la sécurisation des sites web" de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) sont mises en œuvre.

Pour de plus amples informations

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 40 sécurité des sites web

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A416%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.2.5 Sauvegarde des données

Commentaire : Dans le cas où la mesure est choisie pour traiter des risques, indiquez ici comment les sauvegardes sont gérées. Précisez si elles sont stockées dans un endroit sûr.

De manière générale, indiquez s'il existe une politique de sauvegarde permettant d'assurer la disponibilité et/ou l'intégrité des données à caractère personnel, tout en protégeant leur confidentialité (régularité des sauvegardes, chiffrement du canal de transmission des données, test d'intégrité, etc.).

Pour de plus amples informations

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 32 Sauvegardes

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A329%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.2.6 Maintenance

Commentaire : Dans le cas où la mesure est choisie pour traiter des risques, décrivez ici comment est gérée la maintenance physique des équipements, et précisez si elle est sous-traitée. Indiquez si la maintenance à distance des applications est autorisée, et suivant quelles modalités. Précisez si les matériels défectueux sont gérés spécifiquement. Indiquez ici si une surveillance en temps réel du réseau local est mise en œuvre et avec quels moyens.

Lorsque les pannes matérielles pénalisent le fonctionnement du système d'information, différentes causes peuvent être identifiées : matériel obsolète, mal utilisé ou surchargé, maintenance préventive défaillante.

Dans le but de s'assurer de la maintenance régulière du matériel, les documents suivants doivent être mis en place : contrat de maintenance, registre permettant de retracer les interventions (à expliciter).

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 24 Maintenance

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A249%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.2.7 Surveillance

Commentaire : Indiquez ici si une surveillance en temps réel du réseau local est mise en œuvre et avec quels moyens. Indiquez si un contrôle des configurations matérielles et logicielles est effectué et par quels moyens.

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 35 Surveillance

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A352%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.2.8 Sécurité des canaux informatique (réseaux)

Commentaire : l'objectif de cette mesure est de diminuer la possibilité que les caractéristiques des canaux informatiques (réseau filaire, wifi, ondes radio, fibre optique, etc.) soient exploitées pour porter atteinte aux données à caractère personnel (cartographie du réseau, pare-feu, détection et prévention d'intrusion, protocole SSH, chiffrement des flux, authentification forte, etc.).

Dans le cas où la mesure est choisie pour traiter des risques, indiquez ici sur quel type de réseau le traitement est mis en œuvre (isolé, privé, ou Internet). Précisez quels systèmes de pare-feu, sondes de détection d'intrusion, ou autres dispositifs actifs ou passifs sont chargés d'assurer la sécurité du réseau.

Vous pourrez utilement consulter le Guide de la CNIL « les bases des connaissances », pour traiter les spécificités suivantes :

- Spécificités pour les connexions aux équipements actifs du réseau
- Spécificités pour les postes nomades ou se connectant à distance
- Spécificités pour le transfert de fichiers
- Spécificités pour la messagerie électronique

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 37 Sécurité des canaux informatiques (réseaux)

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A371%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.2.9 Contrôle d'accès physique

Commentaire :

L'objectif du contrôle d'accès physique est de limiter les risques que des personnes non autorisées n'accèdent physiquement aux données à caractère personnel (liste des personnes autorisées, authentification des collaborateurs et des visiteurs, trace des accès, alerte en cas d'effraction, etc.)

La sécurité physique est un aspect fondamental de tout type de sécurité pour garantir l'intégrité, la confidentialité et la disponibilité des informations. Si quelqu'un réussit à accéder au système informatique de l'entreprise, il peut l'endommager ou même le détruire.

La sécurité physique consiste aussi en l'usage de barrières, alarmes, serrures et autres contrôles physiques permettant de conditionner l'accès physique aux locaux, aux ordinateurs et aux équipements. Ces mesures sont nécessaires pour protéger les ordinateurs, leur contenu et les autres ressources matérielles contre l'espionnage, le vol et la destruction accidentelle ou intentionnelle.

Dans le cas où la mesure est choisie pour traiter des risques, vous devez décrire ici Indiquez ici la manière dont est réalisé le contrôle d'accès physique aux locaux hébergeant le traitement (zonage, accompagnement des visiteurs, port de badge, portes verrouillées, etc.). Indiquez s'il existe des moyens d'alerte en cas d'effraction.

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 6 Contrôle d'accès physique

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A80%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.2.10 Sécurisation des matériels

Commentaire : Indiquez ici les mesures de sécurité physique des serveurs et des postes clients (stockage sécurisé, câbles de sécurité, filtres de confidentialité, effacement sécurisé avant mise au rebut, etc.)

Existence de mesures prises pour diminuer la possibilité que les caractéristiques des matériels (serveurs, postes fixes, ordinateurs portables, périphériques, relais de communication,

supports amovibles, etc.) soient exploitées pour porter atteinte aux données à caractère personnel (inventaire, cloisonnement, redondance matérielle, limiter l'accès, etc.).

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 39 Sécurité des matériels

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A402%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.2.11 Éloignement des sources de risques

Commentaire : l'objectif est d'éviter que des sources de risques, humaines ou non humaines, portent atteinte aux données à caractère personnel (produits dangereux, zones géographiques dangereuses, transfert des données en dehors de l'UE, etc.).

Dans le cas où la mesure est choisie, les bonnes pratiques pour traiter des risques peuvent être les suivantes :

- Placer les produits dangereux (inflammables, combustibles, corrosifs, explosifs, aérosols, humides, etc.) dans des lieux de stockage appropriés et éloignés de ceux où sont traitées des données
- Ne pas stocker les données dans un Etat étranger sauf s'il existe des garanties permettant d'assurer un niveau de protection des données suffisant.

Indiquez ici si la zone d'implantation est sujette à des sinistres environnementaux (zone inondable, proximité d'industries chimiques, zone sismique ou volcanique, etc.). Précisez si la zone contient des produits dangereux.

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 10 5.1.2.10. Éloignement des sources de risques

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A126%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.2.12 Protection contre les sources de risques non humaines

Commentaire : l'objectif est de réduire ou d'éviter les risques liés à des sources non humaines (phénomènes climatiques, incendie, dégât des eaux, accidents internes ou externes, animaux, etc.) qui pourraient affecter la sécurité des données à caractère personnel (mesures de prévention, détection, protection, etc.).

Décrivez ici les moyens de prévention, de détection et de lutte contre l'incendie. Le cas échéant, indiquez moyens de prévention de dégâts des eaux. Précisez également les moyens de surveillance et de secours de l'alimentation électrique.

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 28 Protection contre les sources de risques non humaines

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A288%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.3 Mesures organisationnelles

6.1.3.1 Organisation et gestion de la politique de protection de la vie privée au sein de l'Inserm

Commentaire : il convient de justifier de l'existence d'une organisation apte à diriger et contrôler la protection des données à caractère personnel au sein de l'organisme

Indiquez si les rôles et responsabilités en matière de protection des données sont définis. Précisez si une personne est chargée de la mise en application des lois et règlements touchant à la protection de la vie privée. Précisez s'il existe un comité de suivi (ou équivalent) chargé des orientations et du suivi des actions concernant la protection de la vie privée.

Exemple : L'Inserm est doté d'une délégation à la protection des données. Placée auprès de la direction, la délégation est chargée du pilotage stratégique de la politique de l'établissement relative à la protection des données personnelles.

La délégation à la protection des données a pour mission de coordonner le plan de mise en conformité au cadre légal relatif à la protection des données. Elle mène ainsi des actions de formation et de sensibilisation, participe à l'élaboration et la promotion, en concertation avec les communautés de recherche, de solutions méthodologiques, juridiques et techniques, homologuées par la CNIL, adaptées aux spécificités de la recherche biomédicale et en santé et contribue à la démarche d'accompagnement des chercheurs dans l'utilisation des données de santé, au bénéfice de la santé des populations et dans le respect des cadres éthique, réglementaire et de confidentialité des données personnelles.

Source : https://www.inserm.fr/actualites-et-evenements/actualites/rgpd-inserm-frederique-lesaulnier-nommee-deleguee-protection-donnees

6.1.3.2 Politique (gestion des règles)

Commentaire : l'objectif est de disposer d'une base documentaire formalisant les objectifs et les règles à appliquer dans le domaine « Informatique et libertés » (plan d'action, révision régulière de la politique « Informatique et libertés », etc.).

Indiquez ici s'il existe une charte informatique (ou équivalent) traitant de la protection des données et de la bonne utilisation des moyens informatiques

Exemple :

L'Inserm s'est doté d'un ensemble de documents visant à garantir les objectifs suivants :

- *disponibilité : les données sont accessibles au moment voulu par les utilisateurs*
- *intégrité : les données ne sont ni corrompues ni modifiées sans autorisation*
- *authenticité : les données disponibles sont uniquement celles que l'établissement souhaite divulguer*
- *confidentialité : les données sont exclusivement disponibles à ceux auxquels elles sont destinées*
- *non répudiation : les données publiées de façon authentique sont certifiées. Leur auteur ne peut pas nier les avoir publiées, il en assume la responsabilité.*

Ces documents sont non limitativement :

Pour la Politique de sécurité des systèmes d'information (PSSI/Inserm – mars 2021)

Politique générale des systèmes d'information (PSSI)pdf – Mis à jour le 3.03.21
Politique des systèmes d'information de recherche (PSSI)pdf – Mis à jour le 3.03.21
Politique des systèmes d'information administrative (PSSI)pdf – Mis à jour le 3.03.21

Pour les Guides et formulaires

Formulaire Retour sur incident doc à retourner au Fonctionnaire de sécurité et de défense (FSD) de l'Inserm – Mis à jour le 21.08.20
Procédure de demande de certificat numérique Renater – Terena.pdf – Mis à jour le 21.08.20

Pour les Chartes d'utilisation

Pour mémoire, « Réseau Renater » désigne l'ensemble des réseaux ou nœuds de communication délivrant directement ou indirectement, sur le territoire national, aux sites agréés, tout ou partie des services pour lesquels le GIP Renater est maître d'ouvrage, quel qu'en soit l'opérateur ou le maître d'œuvre.

Terms of Use for access of INSERM's computing resources and Internet servicespdf – Mis à jour le 24.09.20
Charte de l'administrateur de système et de réseau.pdf – Mis à jour le 21.08.20
Charte déontologique RENATER.pdf – Mis à jour le 21.08.20
Textes législatifs et réglementaires

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 27 Politique (gestion des règles)

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A282%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.3.3 Gestion des risques

Commentaire : Préciser l'existence d'une politique définissant les processus destinés à maîtriser les risques que les traitements de l'organisme font peser sur les droits et libertés des personnes concernées (recensement des traitements de données à caractère personnel, des données, des supports, appréciation des risques, déterminer les mesures existantes ou prévues, etc.).

Indiquez ici si les risques que les traitements font peser sur la vie privée des personnes concernées sont étudiés pour les nouveaux traitements, si c'est systématique ou non, et le cas échéant, selon quelle méthode. Précisez s'il existe, au niveau de l'organisme, une cartographie des risques sur la vie privée

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 21 Gestion des risques

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A219%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.3.4 Gestion des projets

Commentaire : il s'agit ici d'expliquer comment est pris en compte la protection des données à caractère personnel dans tout nouveau traitement (labels de confiance, référentiels, gestion de risques CNIL, formalités CNIL, etc.).

Dans le cas où la mesure est choisie pour traiter des risques : Privilégier le recours à des labels de confiance dans les domaines de la sécurité des systèmes d'information (SSI) et « Informatique et libertés ».

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 20 Gestion des projets

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A210%2C%22ge

n%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.3.5 Gestion des incidents de sécurité et les violations de données

Commentaire : Précise l'existence d'une organisation opérationnelle permettant de détecter et de traiter les événements susceptibles d'affecter les libertés et la vie privée des personnes concernées (définition des responsabilités, plan de réaction, qualifier les violations, etc.).

Indiquez ici si les incidents font l'objet d'une gestion documentée et testée, notamment en ce qui concerne les violations de données à caractère personnel.

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 17 Gestion des incidents et des violations de données :

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A181%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.3.6 Gestion des personnels

Commentaire : Indiquez ici les mesures de sensibilisation prises à l'arrivée d'une personne dans sa fonction. Indiquez les mesures prises au départ des personnes accédant aux données.

Exemple : Au cours ou en fin de recherche, des attachés de recherche clinique (ARC) du promoteur et les auditeurs mandatés par ce dernier accèdent aux données cliniques du dossier médical aux seules fins de vérification des données recueillies par l'investigateur ou son équipe. Ils sont soumis au secret professionnel, c'est-à-dire au respect de la confidentialité des données personnelles. Dans cette optique, ils disposent d'une formation diplômante et adaptée pour mener à bien cette mission.

Au moment des visites, les ARC et les auditeurs présentent à la demande des sites d'investigations les documents attestant de leur mission pour le compte du promoteur Inserm (accord de rendez-vous, ordre de mission, mandat de l'auditeur, planning d'audit).

A l'occasion de la mise en place de la recherche, le promoteur Inserm rappelle aux intervenants les principes généraux de confidentialité et de protection des données personnelles des personnes se prêtant à la recherche. Ces principes s'appliquent du recueil du consentement à la fin de la durée d'archivage des données et des documents comportant des données à caractère personnel.

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 18 Gestion des personnels :

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A189%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.3.7 Gestion des tiers accédant aux données : Relation avec les tiers.

Commentaire : préciser l'existence d'une procédure visant à réduire les risques que les accès légitimes aux données par des tiers peuvent faire peser sur les libertés et la vie privée des personnes concernées (identification des tiers, contrat de sous-traitance, convention, etc.)

Indiquez ici, notamment pour les sous-traitants amenés à avoir accès aux données, les modalités et les mesures de sécurité mises en œuvre pour ces accès.

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 31 Relation avec les tiers :

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A321%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.1.3.8 Superviser la protection de la vie privée

Commentaire : préciser l'existence de mesures permettant de disposer d'une vision globale et à jour de l'état de protection des données et de la conformité au RGPD (contrôler la conformité des traitements, objectifs et indicateurs, responsabilités, etc.).

Indiquez ici si l'effectivité et l'adéquation des mesures touchant à la vie privée sont contrôlées.

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 34 Supervision :

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A346%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.2 Appréciation des risques : les atteintes potentielles à la vie privée

Commentaire : il s'agit ici pour chaque événement redouté :

1. un accès illégitime à des données,
2. une modification non désirée de données, et

3. une disparition de données :

    - De déterminer les impacts potentiels sur la vie privée des personnes concernées s'ils survenaient
    - D'estimer sa gravité, notamment en fonction du caractère préjudiciable des impacts potentiels et, le cas échéant, des mesures susceptibles de les modifier;
    - D'identifier les menaces sur les supports des données qui pourraient mener à cet événement redouté et les sources de risques qui pourraient en être à l'origine ;
    - D'estimer sa vraisemblance, notamment en fonction des vulnérabilités des supports de données, des capacités des sources de risques à les exploiter et des mesures susceptibles de les modifier.

    L'élaboration de cette partie s'appuie sur un processus itératif visant à déterminer si les risques ainsi identifiés peuvent être jugés acceptables compte tenu des mesures existantes ou prévues.

    Si le risque n'est pas jugé acceptable, il conviendra, dans le cadre du processus itératif de proposer des mesures complémentaires et procéder à une nouvelle estimation du niveau de chacun des risques en tenant compte de celles-ci.

    Au terme du processus, seront déterminés les risques résiduels qui seront mentionnés dans cette AIPD.

Dans le cadre du processus, il conviendra donc dans un premier temps, pour chacun des évènements redoutés (accès illégitime à des données ; modification non désirée des données, disparition des données) de documenter le tableau :

Principales sources de risques	***Principales menaces***	***Principaux impacts potentiels***	***Principales mesures réduisant la gravité et la vraisemblance***	***Gravité***	***Vraisemblance***

Il existe trois types de sources de risques :

- Source de risques humaines internes
- Source de risques humains externes
- Source de risques non humains

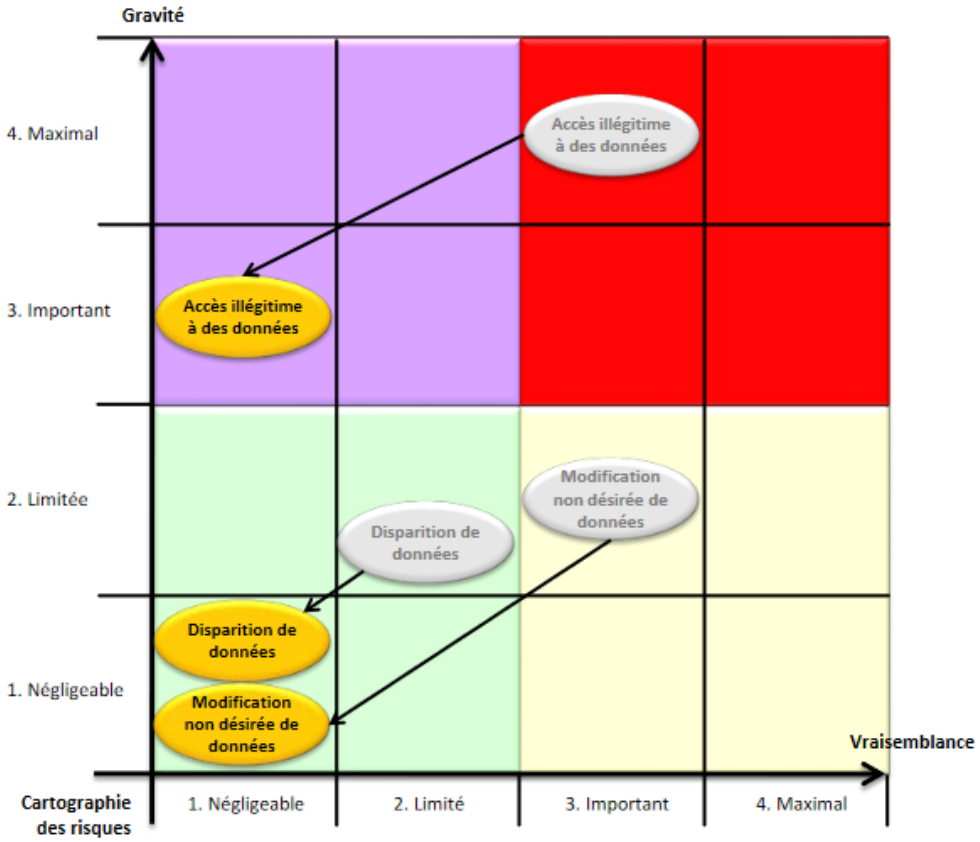
La gravité est l'estimation de l'ampleur des impacts potentiels sur la vie privée des personnes concernées.

La vraisemblance est l'estimation de la possibilité qu'un risque se réalise.

Puis procéder à son analyse afin d'identifier des voies d'amélioration de la gravité et de la vraisemblance :

Risques	Appréciation du risque : acceptable/améliorable	Identification des mesures correctives	Gravité résiduelle après application des mesures correctives	Détermination de la vraisemblance résiduelle
	L'évaluateur devra estimer si les mesures existantes ou prévues (déjà engagées) réduisent suffisamment ce risque pour qu'il puisse être jugé acceptable	Le cas échéant, indiquer ici les mesures complémentaires qui seraient nécessaires ayant un impact sur la gravité et la vraisemblance		

La cartographie des risques et le travail d'analyse de la gravité et de la vraisemblance peut se résumer sous la forme d'un schéma (source : https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-fr-modeles.pdf)



Pour plus d'informations : https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A28%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

Le résultat de ce processus sera ensuite documenté dans l'AIPD, dans les sections suivantes puis résumé sous la forme d'un schéma identifiant la gravité résiduel et la vraisemblance résiduelle :

6.2.1 Risque d'Accès illégitime à des données

Commentaire : Vous pouvez, au choix présenter l'analyse sous la forme d'un tableau ou sous forme d'un texte

Principales sources de risques	***Principales menaces***	***Principaux impacts potentiels***	***Principales mesures réduisant la gravité et la vraisemblance***	***Gravité résiduelle***	***Vraisemblance résiduelle***

6.2.1.1 Principales sources de risques

Commentaire : les principales sources de risques sont les suivantes :

- Sources humaines externes : destinataires des données, anciens salariés, participants, cybercriminel, puissance étrangère, activiste idéologique, organisme de recherche, banque, mutuelle, assurance, etc.
- Sources humaines internes : salariés, stagiaires, administrateurs informatiques, etc.
- Sources non humaines : eau, épidémies, catastrophes naturelles, matières inflammables, corrosives ou explosives

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 1.3 Typologie de sources de risques :

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A28%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.2.1.2 Principales menaces qui pourraient permettre la réalisation du risque

➢ Exemples de menaces pouvant conduire à un accès illégitime aux données

- Utilisation ou transport d'un matériel sensible à des fins personnelles

- Utilisation de clefs USB ou disques durs inappropriés à la sensibilité des informations
- Observation d'un écran à l'insu de son utilisateur
- Photographie d'un écran et publication sur les réseaux sociaux
- Géolocalisation d'un matériel
- Branchement d'un appareil (ex : clé USB) pour récupérer des données
- Vol/perte d'un ordinateur portable, vol/perte d'un téléphone portable
- Vol/perte d'un support de stockage électronique
- Fouille de contenu
- Croisement illégitime de données
- Influence (hameçonnage, ingénierie sociale, corruption), pression (chantage, harcèlement moral)
- Vol de dossiers/documents dans les bureaux, vol de courriers dans les boîtes aux lettres
- Récupération de documents mis au rebut
- Corruption par un code malveillant

NB : Cette liste n'est pas exhaustive et doit être adaptée à votre recherche.

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 1.6 Menaces qui peuvent mener à un accès illégitime à des données :

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A37%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C658%2C0%5D

6.2.1.3 Les principaux impacts potentiels sur les personnes concernées si le risque se produit

Commentaire : Les risques qui sont analysés sont les risques pour la personne résultant de la mise en œuvre d'un traitement et non les risques pour l'Inserm : dommages physiques, matériels, préjudice moral tels qu'une discrimination, un vol, une usurpation d'identité, une perte financière, une atteinte à la vie privée, une atteinte à la réputation....

Les impacts peuvent être :

- Corporels
- Matériels
- Moraux

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 1.4 Échelle et règles pour estimer la gravité

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A28%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C589%2C0%5D

6.2.1.4 Principales mesures, parmi celles identifiées, contribuant à traiter le risque

Commentaire : Parmi les mesures existantes ou prévues ci-avant, identifier celles qui permettront de traiter le risque.

6.2.1.5 Estimation de la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues

Commentaire : La gravité représente l'ampleur d'un risque. Elle dépend essentiellement du caractère préjudiciable des impacts potentiels

Indiquez, en justifiant, si la gravité du risque vous semble négligeable, limitée, importante ou maximale.

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 1.4 : échelle et règles pour estimer la gravité :

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A28%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C589%2C0%5D

6.2.1.6 Estimation de la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues

Commentaire : La vraisemblance est essentiellement estimée au regard

- des vulnérabilités des supports concernés et
- de la capacité des sources de risques à les exploiter,
- compte tenu des mesures existantes, prévues ou complémentaires (qu'il convient de mentionner en tant que justification).

Les mesures mises en place doivent permettre de limiter le risque.

Indiquez en justifiant si la vraisemblance du risque vous semble négligeable, limitée, importante ou maximale.

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 1.4 : échelle et règles pour estimer la vraisemblance :

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A34%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C403%2C0%5D

6.2.2 Risque de modification non désirée de données

Commentaire : Vous pouvez, au choix présenter l'analyse sous la forme d'un tableau ou sous forme d'un texte

Principales sources de risques	***Principales menaces***	***Principaux impacts potentiels***	***Principales mesures réduisant la gravité et la vraisemblance***	***Gravité résiduelle***	***Vraisemblance résiduelle***

6.2.2.1 Principales sources de risques

Commentaire : les principales sources de risques sont les suivantes :

- Sources humaines externes : destinataires des données, anciens salariés, participants, cybercriminel, puissance étrangère, activiste idéologique, organisme de recherche, banque, mutuelle, assurance, etc.
- Sources humaines internes : salariés, stagiaires, administrateurs informatiques, etc.
- Sources non humaines : eau, épidémies, catastrophes naturelles, matières inflammables, corrosives ou explosives

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 1.3 Typologie de sources de risques :

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A28%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.2.2.2 Principales menaces qui pourraient permettre la réalisation du risque

- Menaces pouvant conduire à une modification non désirée des données
  - Ajout d'un matériel incompatible menant à un dysfonctionnement
  - Erreur de manipulation
  - Remplacement d'un document par un faux
  - Corruption par un code malveillant

NB : Cette liste n'est pas exhaustive et doit être adaptée à votre recherche.

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 1.6 Menaces qui peuvent mener à un accès illégitime à des données :

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A37%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C658%2C0%5D

6.2.2.3 Les principaux impacts potentiels sur les personnes concernées si le risque se produit

Commentaire : Les risques qui sont analysés sont les risques pour la personne résultant de la mise en œuvre d'un traitement et non les risques pour l'Inserm : dommages physiques, matériels, préjudice moral tels qu'une discrimination, un vol, une usurpation d'identité, une perte financière, une atteinte à la vie privée, une atteinte à la réputation....

Les impacts peuvent être :

- Corporels
- Matériels
- Moraux

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 1.4 Échelle et règles pour estimer la gravité

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A28%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C589%2C0%5D

6.2.2.4 Principales mesures, parmi celles identifiées, contribuant à traiter le risque

Commentaire : Parmi les mesures existantes ou prévues ci-avant, identifier celles qui permettront de traiter le risque.

6.2.2.5 Estimation de la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues

Commentaire : La gravité représente l’ampleur d’un risque. Elle dépend essentiellement du caractère préjudiciable des impacts potentiels

Indiquez, en justifiant, si la gravité du risque vous semble négligeable, limité, importante ou maximale.

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 1.4 : échelle et règles pour estimer la gravité :

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A28%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C589%2C0%5D

6.2.2.6 Estimation de la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues

Commentaire : La vraisemblance est essentiellement estimée au regard

- des vulnérabilités des supports concernés et
- de la capacité des sources de risques à les exploiter,
- compte tenu des mesures existantes, prévues ou complémentaires (qu'il convient de mentionner en tant que justification).

Les mesures mises en place doivent permettre de limiter le risque.

Indiquez en justifiant si la vraisemblance du risque vous semble négligeable, limité, importante ou maximale.

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 1.4 : échelle et règles pour estimer la vraisemblance :

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A34%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C403%2C0%5D

6.2.3 Risque de disparition de données

Commentaire : Vous pouvez, au choix présenter l'analyse sous la forme d'un tableau ou sous forme d'un texte

Principales sources de risques	***Principales menaces***	***Principaux impacts potentiels***	***Principales mesures réduisant la gravité et la vraisemblance***	***Gravité résiduelle***	***Vraisemblance résiduelle***

6.2.3.1 Principales sources de risques

Commentaire : les principales sources de risques sont les suivantes :

- Sources humaines externes : destinataires des données, anciens salariés, participants, cybercriminel, puissance étrangère, activiste idéologique, organisme de recherche, banque, mutuelle, assurance, etc.
- Sources humaines internes : salariés, stagiaires, administrateurs informatiques, etc.
- Source non humaines : eau, épidémies, catastrophes naturelles, matières inflammables, corrosives ou explosives

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 1.3 Typologie de sources de risques :

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A28%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C770%2C0%5D

6.2.3.2 Principales menaces qui pourraient permettre la réalisation du risque

➢ <u>Menaces pouvant conduire à une dispartion des données</u>

- Attaque par déni de services
- Ajout d'un matériel incompatible menant à une panne
- Inondation, incendie,
- Vandalisme
- Dysfonctionnement d'un dispositif de stockage
- Vol/perte d'un ordinateur portable, vol/perte d'un téléphone
- Erreur de manipulation
- Effacement volontaire/involontaire de partie de texte
- Corruption par un code malveillant

NB : Cette liste n'est pas exhaustive et doit être adaptée à votre recherche.

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 1.6 Menaces qui peuvent mener à un accès illégitime à des données :

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A37%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C658%2C0%5D

6.2.3.3 Les principaux impacts potentiels sur les personnes concernées si le risque se produit

Commentaire : Les risques qui sont analysés sont les risques pour la personne résultant de la mise en œuvre d'un traitement et non les risques pour l'Inserm : dommages physiques, matériels, préjudice moral tels qu'une discrimination, un vol, une usurpation d'identité, une perte financière, une atteinte à la vie privée, une atteinte à la réputation....

Les impacts peuvent être :

- Corporels
- Matériels
- Moraux

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 1.4 Échelle et règles pour estimer la gravité

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A28%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C589%2C0%5D

6.2.3.4 Principales mesures, parmi celles identifiées, contribuant à traiter le risque

Commentaire : Parmi les mesures existantes ou prévues ci-avant, identifier celles qui permettront de traiter le risque.

6.2.3.5 Estimation de la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues

Commentaire : La gravité représente l'ampleur d'un risque. Elle dépend essentiellement du caractère préjudiciable des impacts potentiels

Indiquez, en justifiant, si la gravité du risque vous semble négligeable, limité, importante ou maximale.

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 1.4 : échelle et règles pour estimer la gravité :

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A28%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C589%2C0%5D

6.2.3.6 Estimation de la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues

Commentaire : La vraisemblance est essentiellement estimée au regard

- des vulnérabilités des supports concernés et
- de la capacité des sources de risques à les exploiter,
- compte tenu des mesures existantes, prévues ou complémentaires (qu'il convient de mentionner en tant que justification).

Les mesures mises en place doivent permettre de limiter le risque.

Indiquez en justifiant si la vraisemblance du risque vous semble négligeable, limitée, importante ou maximale.

Pour de plus amples informations et des exemples :

Consulter le Guide de la CNIL : PIA, les bases de connaissances Édition février 2018, Section 1.4 : échelle et règles pour estimer la vraisemblance :

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf#%5B%7B%22num%22%3A34%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C52%2C403%2C0%5D

1.1. Synthèse de l'évaluation des risques

Gravité	**Maximale**				
	Important				
	Limité				
	Négligeable				
		Négligeable	**Limité**	**Important**	**Maximale**
		Vraisemblance			

7. VALIDATION FORMELLE

Formalisation de la validation

Le [jj/mm/aaaa], le [poste du responsable de traitement] de [nom de l'organisme] valide le PIA du traitement [nom du PIA], au vu du PIA mené, en sa qualité de responsable du traitement.

Le traitement a pour finalité de [rappel de la finalité du traitement].

le responsable du traitement a sollicité [à compléter]

Les mesures prévues pour respecter les principes fondamentaux de la protection de la vie privée et pour traiter les risques sur la vie privée des personnes concernées sont en effet jugées acceptables au regard de cet enjeu. La mise en œuvre des mesures complémentaires devra toutefois être démontrée, ainsi que l'amélioration continue du PIA.

[Signature]

Le [jj/mm/aaaa], le délégué à la protection des données de [nom de l'organisme] a rendu l'avis suivant concernant la conformité du traitement et le PIA mené