Politique Institutionnelle de Protection Des Données à Caractère Personnel

Mars 2019

SOMMAIRE

1. RESUME 4
2. DEFINITIONS 4
3. CHAMP D'APPLICATION 4
4. GESTION DE LA POLITIQUE 4
5. ENJEUX ET OBJECTIFS 5
5.1 ENJEUX DE LA GESTION DES DONNEES A CARACTERE PERSONNEL 5
5.2 OBJECTIFS 5
6. UTILISATION DES DONNEES A CARACTERE PERSONNEL RECUEILLIES 6
6.1 COLLECTE DES DONNEES A CARACTERE PERSONNEL 6
6.2 FINALITES DES DONNEES COLLECTEES 6
7. RESPECT DES DROITS DES PERSONNES 7
8. ORGANISATION DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL 7
8.1 PRINCIPAUX ROLES ET RESPONSABILITES EN MATIERE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL 7
8.1.1 Président du Directoire de l'Institut Curie 7
8.1.2 Ligne managériale 8
8.1.2.1 Directeurs 8
8.1.2.2 Responsable d'entité 8
8.1.2.3 Responsable Opérationnel de Traitement 9
8.1.3 Fonctions en support de la protection des données à caractère personnel 9
8.1.3.1 Référent à la protection des données 9
8.1.3.2 Délégué à la protection des données (DPO) 10
8.1.3.3 Responsable de la Sécurité des Systèmes d'Information 10
8.1.3.4 Direction Juridique 11
8.1.3.5 Direction des Systèmes d'Information 11
8.1.3.6 Direction des Data 11
8.2 ROLE DES CRI EN MATIERE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL 11
8.2.1 Comité de Revue Institutionnelle (CRI) 12
8.2.2 CRI data 12
9. PRINCIPAUX PROCESSUS A METTRE EN ŒUVRE 13
9.1 REGISTRE DES TRAITEMENTS 13
9.2 DOCUMENTATION 13
9.3 ANALYSE D'IMPACT 14
9.4 AUDITS INTERNES 15
9.5 GESTION DES INCIDENTS ET GESTION DE CRISE 15
9.6 GESTION DES DROITS DES PERSONNES SUR LEURS DONNEES 16
9.7 GESTION DES RELATIONS AVEC L'AUTORITE DE CONTROLE 16
10. APPLICABILITE DE LA POLITIQUE AUX TIERS 16

1. Résumé

L'institut Curie est particulièrement attaché au respect de la vie privée et de la protection des données à caractère personnel des personnes physiques, patients comme personnels.

La présente politique présente les principes d'organisation et d'actions de l'Institut Curie dans le cadre de la protection des données à caractère personnel.

2. Définitions

Données à caractère personnel : toute information se rapportant à une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant.

Traitement : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel. Il peut s'agir d'une application informatique, de la constitution d'un fichier ou d'un questionnaire par exemple.

Personne concernée : personne physique dont les données à caractère personnel font l'objet d'un traitement.

Responsable de traitement : personne morale qui détermine les finalités et les moyens du traitement.

Responsable opérationnel de traitement : responsable d'une entité (direction, département, unité y compris unité mixte de recherche (UMR), plateforme…) ou d'un projet scientifique, responsable de la mise en œuvre du traitement et de la collecte des données.

3. Champ d'application

La présente politique de protection des données de l'Institut Curie s'applique à l'ensemble de ses activités, soit celles des services :

- Des Services du Siège,
- De l'Ensemble Hospitalier,
- Du Centre de Recherche.

De façon plus générale, cette politique s'applique aux personnels intervenant pour l'Institut Curie (quel que soit leur employeur et le site sur lequel ils exercent leur activité). En outre, les partenaires et personnels d'organismes extérieurs sont concernés par cette politique, en participant à son respect et son application sur leur périmètre respectif.

Les éléments décrits dans ce document sont, au besoin, déclinés en mesures spécifiques à une entité ou en procédures, de manière à faciliter leur mise en œuvre.

4. Gestion de la Politique

La mise en œuvre de la présente politique est, au sens du RGPD, de la responsabilité du Président du Directoire de l'Institut Curie. Cette politique est définie et approuvée par le Directoire.

La présente politique est diffusée, sous la responsabilité du Président du Directoire de l'Institut Curie, à l'ensemble des personnes devant l'appliquer et, en cas de nécessité, en totalité ou par extraits, aux partenaires et prestataires de l'Institut Curie.

La mise à jour de la présente politique est sous la responsabilité du Président de l'Institut Curie. Elle peut s'avérer nécessaire notamment en cas de changements d'origine interne à l'Institut Curie (par exemple l'évolution de ses activités) ou externe (évolution de la législation, de l'environnement économique, de la nature de ses partenaires, des enjeux stratégiques).

Le processus de révision et de mise à jour de la politique garantit son adéquation avec le fonctionnement de l'Institut Curie, et son efficacité.

5. Enjeux et objectifs

5.1 Enjeux de la gestion des données à caractère personnel

Par ses activités, l'Institut Curie est amené à utiliser des données à caractère personnel notamment des données concernant la santé de personnes physiques, ou encore concernant ses personnels. Dans ce cadre, l'Institut Curie se fixe un devoir de vigilance et d'exemplarité concernant l'utilisation de ces données de manière à protéger les libertés fondamentales des individus.

Cet enjeu est d'autant plus important qu'il doit permettre à l'Institut Curie d'exercer ses activités avec :

- La pleine confiance de ses patients, personnels, donateurs et partenaires,
- Une exemplarité en matière de soin et d'accompagnement des patients,
- Un niveau d'exigence scientifique qui est celui d'un institut de recherche de renommée internationale,
- La pleine conformité de ses actions à la règlementation applicable en matière de gestion des données à caractère personnel.

5.2 Objectifs

Par suite, cet enjeu se concrétise par deux objectifs forts en matière de gestion des données à caractère personnel :

- Favoriser, au sein de l'Institut Curie, une culture et des pratiques permettant d'accorder une attention particulière à l'utilisation et la protection des données à caractère personnel et ce d'autant plus lorsqu'elles revêtent un caractère sensible pour les individus, comme les données de santé,
- Assurer la conformité aux réglementations en matière de protection de données à caractère personnel, et en particulier au Règlement Général sur la Protection des Données (« RGPD ») entré en application le 25 mai 2018.

Le présent document constitue la politique de protection des données à caractère personnel de l'Institut Curie. Il décrit les principaux éléments et les principes d'action que l'Institut Curie met en œuvre pour atteindre ces objectifs et pérenniser les bonnes pratiques en matière de gestion des données à caractère personnel.

6. Utilisation des données à caractère personnel recueillies

6.1 Collecte des données à caractère personnel

L'Institut Curie peut être amené à collecter des données à caractère personnel dans le cadre de la réalisation de ses activités, en particulier les données suivantes:

- Données d'identification technique : carte d'identité / passeport, adresse IP, données de connexion ;
- Données d'état civil : nom, prénom, nationalité, lieu et date de naissance, données de décès le cas échéant, sexe, adresse postale ;
- Données de contact : adresse postale et électronique, numéro de téléphone ;
- Vie professionnelle : CV, fonction, date de début de carrière, temps de travail, diplômes/certifications, formations, carrière, congés/RTT, évolutions et objectifs ;
- Vie privée : statut marital, composition du ménage, permis de conduire ;
- Situation économique et financière : salaire, économies ou patrimoine, RIB ou numéro de carte bancaire ;
- Données de localisation : voyages / déplacements, site de travail, données GPS ;
- Images et vidéos : images, vidéosurveillance ;
- Numéro d'inscription au répertoire : numéro d'identification du patient, numéro de sécurité sociale ;
- Données de santé : maladie / pathologie, handicap, antécédents familiaux, traitement et soins, prélèvement biologique ;
- Données génétiques : ADN, origines raciales / ethniques ;
- Données physiologiques et biométriques : caractéristiques faciales, iris, empreintes digitales… ;
- Opinions personnelles : religion, habitudes alimentaires ;
- Vie sexuelle : orientation sexuelle, vie sexuelle.

6.2 Finalités des données collectées

L'Institut Curie collecte les données à caractère personnel sur la base d'une non-opposition ou d'un consentement éclairé des individus, d'une obligation légale ou dans le cadre de ses activités statutaires. Dans tous les cas, ces données sont collectées uniquement pour poursuivre ses intérêts légitimes et après information conforme des personnes.

Ainsi, l'Institut Curie collecte et utilise des données à caractère personnel, notamment pour les finalités suivantes :

- Assurer les soins et le suivi de la relation avec les patients : prise en charge, examens médicaux, diagnostic, soins, information et maintien de la relation,
- Conduire ses activités de recherche,
- Assurer la communication interne et externe de l'Institut Curie,
- Gérer ses relations avec les donateurs, ainsi qu'avec ses personnels, partenaires et fournisseurs,
- Assurer la gestion administrative et opérationnelle (par exemple : gestion RH, gestion financière, achats…),
- Répondre aux obligations légales ou administratives imposées par la règlementation en vigueur.

Dans l'hypothèse où les données à caractère personnel seraient traitées pour des finalités différentes de celles exposées lors de l'information ayant fondé la non opposition /le consentement de

l'individu, l'Institut Curie l'en informera et, lorsque la loi l'exige, recueillera à nouveau son consentement préalable.

7. Respect des droits des personnes

Les personnes concernées sont informées des caractéristiques du traitement avant sa mise en œuvre. En particulier, le responsable opérationnel de traitement veille à porter à la connaissance des personnes le nom et les coordonnées du responsable de traitement, les finalités, les catégories de personnes accédant aux données, la durée de conservation, les coordonnées du Délégué à la Protection des Données de l'Institut Curie et les modalités détaillées d'exercice des droits.

Le responsable opérationnel de traitement définit pour chaque traitement un processus de gestion des demandes d'opposition. En particulier, une procédure permet aux patients de l'Institut Curie d'exercer en toute circonstance leur droit d'opposition à l'échange et au partage, y compris au sein de l'équipe de soin, des données médicales le concernant.

Le responsable opérationnel de traitement garantit la possibilité pour les personnes concernées d'accéder aux données à caractère personnel les concernant.

Le responsable opérationnel de traitement répond dans un délai d'un mois maximum à une demande d'opposition ou d'accès aux données.

8. Organisation de la protection des données à caractère personnel

Sous la supervision et la responsabilité du Président de l'Institut Curie, la gestion des données à caractère personnel est mise en œuvre par l'ensemble du management.

Pour cela, les différents responsables bénéficient de l'appui de la Direction des Systèmes d'Information, de la Direction des Data, de la Direction Juridique, du Responsable de la sécurité des systèmes d'information (RSSI) et du Délégué à la protection des données (DPO).

En outre, des instances *ad hoc* et un réseau de référents complètent le dispositif.

Cette organisation vise à faciliter au mieux l'appropriation par chacun d'une culture de la gestion des données à caractère personnel afin de rendre opérante la protection de ces données.

8.1 Principaux rôles et responsabilités en matière de protection des données à caractère personnel

8.1.1 Président du Directoire de l'Institut Curie

La mise en œuvre de la protection des données à caractère personnel s'exerce sous la responsabilité globale du Président du Directoire de l'Institut Curie.

Plus précisément, le Président :

- Fixe les grandes orientations en matière de protection des données à caractère personnel, et en particulier la mise en œuvre et le respect de cette politique,
- Met en œuvre une organisation permettant d'assurer efficacement la protection des données à caractère personnel,
- Veille à la bonne allocation des moyens nécessaires au fonctionnement de cette organisation, afin notamment d'assurer que les compétences mobilisées sont suffisantes, adéquates et placées au bon niveau hiérarchique,
- Notifie à la Commission Nationale Informatique et Libertés (CNIL) tout cas de violation grave de données à caractère personnel, dans le cadre prévu par le droit applicable.

En outre, le Président du Directoire demande, en particulier au DPO, la réalisation de points de situation, de contrôle ou d'audits internes afin d'être informé du niveau d'effectivité et d'efficacité de la protection des données à caractère personnel. Il demande également toute investigation qu'il jugera nécessaire à l'amélioration du dispositif, par exemple à l'issue d'un incident.

8.1.2 Ligne managériale

8.1.2.1 Directeurs

Les Directeurs, tels que définis à l'article 5 des statuts de l'Institut Curie, sont en charge de :

- Revoir périodiquement la mise en œuvre de la présente politique dans leur périmètre,
- Proposer au Président du Directoire d'éventuels ajustements organisationnels ou de la politique,
- Coordonner les actions de protection des données à caractère personnel au sein de l'Institut Curie,
- Suivre l'efficacité de ces actions.

En lien avec le Président du Directoire, les Directeurs demandent, en particulier au DPO, la réalisation de points de situation, de contrôle ou d'audits internes afin de leur permettre de s'informer du niveau d'effectivité et d'efficacité de la protection des données à caractère personnel. Ils demandent également toute investigation qu'ils jugent nécessaire à l'amélioration du dispositif, par exemple à l'issue d'un incident.

8.1.2.2 Responsable d'entité

Le responsable d'une entité est le responsable d'une direction, d'un département, d'une unité y compris unité mixte de recherche (UMR), d'une plateforme.

Chaque manager, directeur ou responsable, est en charge, sur son périmètre, de :

- Décliner les orientations de la politique,
- Veiller à la mise en œuvre de processus adaptés à la protection des données à caractère personnel et au contexte de son entité, et en particulier à la bonne tenue du registre des traitements de son périmètre,
- Solliciter l'avis du DPO ou de toute autre fonction support de la protection des données à caractère personnel (visées à l'article « Fonctions en support » de la politique),
- Assurer l'efficacité du dispositif.

En particulier, il s'assure que :

- Les référents de son entité sont bien désignés, sensibilisés et formés au traitement de données à caractère personnel,

- Les responsables opérationnels de traitement de son entité disposent d'une information nécessaire et suffisante concernant les exigences et processus relatifs à la protection des données à caractère personnel,
- Les responsables opérationnels de traitement sollicitent, autant que nécessaire, prioritairement les référents de leur entité, voire le DPO ou la fonction support idoine (visées à l'article « Fonctions en support » de la politique) pour leur permettre de souscrire à leurs obligations (cf. infra).

8.1.2.3 Responsable Opérationnel de Traitement

Le responsable opérationnel de traitement est le responsable d'une entité (direction, département, unité y compris unité mixte de recherche (UMR), plateforme…) ou d'un projet qui implique l'utilisation de données à caractère personnel. Le traitement peut concerner en particulier un projet de recherche, le parcours patient, une opération particulière, un processus administratif.

Le responsable opérationnel de traitement prend en compte la protection des données à caractère personnel dès la phase de conception des projets, y compris dans le cas d'un renouvellement de marché. En particulier, chaque projet de traitement, qu'il repose sur une application informatique interne ou externe, fait l'objet d'une revue de conformité aux dispositions légales et règlementaires relatives à la protection des données avant sa mise en œuvre.

Le responsable opérationnel de traitement est dans ce cadre en charge de mettre en place sur son périmètre une organisation permettant de :

- S'assurer que les traitements de données à caractère personnel de son périmètre sont bien conformes à la réglementation en vigueur, et en particulier au règlement RGPD ainsi qu'aux Méthodologies de Recherche,
- S'assurer que les données à caractère personnel sont :
  - Utilisées uniquement pour des finalités explicites et légitimes ;
  - Pertinentes et non excessives ;
  - Accessibles aux seules personnes dont les missions le justifient ;
  - Conservées uniquement le temps nécessaire à l'accomplissement des finalités, et respectent les durées légales d'archivage ;
  - Traitées de manière à garantir leur sécurité et conformément à la Politique de Sécurité des Systèmes d'Information de l'Institut Curie.
- Déclarer à son référent le traitement mis en œuvre et lui fournir toute information utile à l'inscription au registre des traitements par le référent,
- S'assurer que les mesures organisationnelles, procédurales et techniques sont proportionnées aux enjeux du traitement et permettent de réduire le niveau de risque pour les personnes dont les données à caractère personnel ont été collectées, pesant sur lesdites données traitées à un niveau acceptable. Le responsable opérationnel de traitement documente toutes les mesures prises pour garantir la sécurité et la conformité du traitement aux dispositions légales et règlementaires relatives à la protection des données.
- Conduire une analyse d'impact pour tout projet portant sur un nouveau traitement ou une modification de traitement de données à caractère personnel, avec l'appui du référent de son entité, et si nécessaire, du DPO et de la Direction des Data.
- Exiger, en cas de recours à un sous-traitant, son respect aux principes de protection des données à caractère personnel, et le formaliser à travers une contractualisation.
- Faciliter les revues de conformité des traitements de son périmètre,
- Avertir immédiatement le DPO des risques de plaintes, réclamations relatives aux traitements,
- Déclarer immédiatement au DPO et à la Direction juridique tout incident ayant entraîné la rupture de la confidentialité sur des données à caractère personnel, et en particulier leur perte, leur indisponibilité, leur altération ou leur utilisation à des fins non prévues par la finalité initiale du traitement.

8.1.3 Fonctions en support de la protection des données à caractère personnel

8.1.3.1 Référent à la protection des données

Chaque entité (direction, département, unité) désigne un ou des référents à la protection des données en son sein. Celui-ci est en charge de :

- Se former aux principes de la protection des données à l'Institut Curie, notamment par le biais du module de formation dispensé par le DPO,
- Constituer le point de contact pour les collaborateurs de son entité et les fonctions en support de la protection des données,
- Répondre aux sollicitations des responsables opérationnels de traitement de son périmètre, en lien avec les autres fonctions en support,
- Relayer l'information et les bonnes pratiques relatives à la protection des données à caractère personnel, et en particulier l'information produite par la Direction juridique, la Direction des systèmes d'information et le DPO, et les sensibiliser sur leur responsabilité,
- Collecter les informations nécessaires à la bonne protection des données, et en particulier celles indispensables à la tenue du registre des traitements sur son périmètre, et pour les revues de conformité,
- Transmettre les informations pour l'inscription au registre des traitements de l'Institut Curie des traitements de données à caractère personnel de son périmètre,
- Alerter le DPO des risques de plaintes, réclamations relatives aux traitements,
- Identifier et remonter au DPO les éventuels doutes de non-conformité, et difficultés de mise en œuvre des directives des différentes tutelles de l'UMR, le cas échéant.

8.1.3.2 Délégué à la protection des données (DPO)

Le Délégué à la Protection des Données (DPO)de l'Institut Curie exerce ses missions conformément aux dispositions des articles 37 et suivants du Règlement Général sur la Protection des Données (RGPD), et en lien avec la Direction Juridique et le Responsable de la Sécurité des Systèmes d'Information.

Il est associé par l'Institut Curie à toutes les questions relatives à la protection des données à caractère personnel. Il agit pour ce faire en totale indépendance et répond de ses actions directement au Directoire de l'Institut Curie.

Dans ce cadre, le DPO assure les missions suivantes :

- Informer et conseiller l'Institut Curie, ses employés ou ses sous-traitants qui procèdent à des traitements de données à caractère personnel sur les obligations leur incombant en matière de protection des données,
- Contrôler le respect des dispositions du RGPD, et d'autres dispositions du droit de l'Union Européenne ou national, ainsi que des règles internes à l'Institut Curie en matière de protection des données, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant,
- Veiller à la mise en œuvre des processus de gestion des réponses aux demandes de droits (accès, opposition, rectification, suppression, limitation, portabilité), de réclamations et de requêtes des personnes concernées pour les traitements,
- Alerter le Directoire des manquements constatés,
- Dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données à caractère personnel et vérifier l'exécution de celle-ci,
- Etre l'interlocuteur privilégié et le point de contact des Autorités de contrôle (en particulier CNIL, ANSSI) et coopérer avec elles, sur les questions relatives aux traitements de données à caractère personnel,
- Réaliser ou assister l'ensemble des démarches auprès de la CNIL,

— Assurer la coordination des actions avec les autres tutelles des UMR de l'Institut.

8.1.3.3 Responsable de la Sécurité des Systèmes d'Information

Dans le cadre de ses fonctions, le RSSI est en charge d'assurer un soutien et une expertise pour la sécurisation de l'ensemble des données de l'Institut Curie. Concernant le périmètre des données à caractère personnel, il apporte son expertise pour :

— Analyser les risques et impacts portant sur les données à caractère personnel, et en particulier pour l'analyse des dispositifs techniques de sécurisation,
— Formuler un avis portant sur le niveau de sécurisation et de risque résiduel,
— Alerter le DPO en cas de risque grave ou de non-conformité identifiée,
— Formuler les recommandations nécessaires à la réduction des risques identifiés ou à la prise de mesures spécifiques,
— Assurer la coordination des actions avec les autres tutelles des UMR de l'Institut.

8.1.3.4 Direction Juridique

En matière de protection des données à caractère personnel, la Direction juridique apporte son expertise pour :

— Contribuer à la veille portant sur les évolutions réglementaires en matière de protection des données à caractère personnel et à l'analyse de leur impact pour l'Institut Curie,
— Contribuer dans le cadre de ses compétences à l'analyse des risques juridiques associés aux données à caractère personnel,
— Formuler un avis portant sur le niveau de sécurisation juridique du traitement et le risque résiduel y afférent,
— Alerter le DPO en cas de risque grave ou de non-conformité identifiée,
— Formuler les recommandations nécessaires à la réduction des risques identifiés ou à la prise de mesures spécifiques.

8.1.3.5 Direction des Systèmes d'Information

La Direction des Systèmes d'Information apporte son expertise technique pour :

— Contribuer à la veille portant sur les évolutions des menaces techniques pouvant fragiliser les dispositifs de protection des données à caractère personnel,
— Analyser les risques portant sur les données à caractère personnel, et en particulier en ce qui concerne les éléments techniques de l'analyse d'impact,
— Formuler un avis portant sur le niveau de sécurisation technique et de risque résiduel,
— Alerter le DPO en cas de risque grave ou de non-conformité identifiée,
— Formuler les recommandations nécessaires à la réduction des risques identifiés ou à la prise de mesures spécifiques,
— Porter un avis sur la faisabilité des mesures de sécurisation techniques envisagées, et leur proportionnalité aux enjeux sous-jacents.

8.1.3.6 Direction des Data

La Direction des Data apporte son expertise pour :

— Analyser les risques portant sur les mises à disposition des données à caractère personnel, et en particulier en ce qui concerne les finalités poursuivies par les traitements,
— Formuler un avis portant sur le niveau de sécurisation des données et de risque résiduel,
— Alerter le DPO en cas de risque grave ou de non-conformité identifiée,
— Formuler les recommandations nécessaires à la réduction des risques identifiés ou à la prise de mesures spécifiques,

— Porter un avis sur la faisabilité des mesures envisagées, et leur proportionnalité aux enjeux sous-jacents.

8.2 Rôle des CRI en matière de protection des données à caractère personnel

Deux comités de revue institutionnelle (CR)I ont été mis en place au sein de l'Institut Curie :

- Le CRI de l'Ensemble Hospitalier
- Le CRI DATA

Ces CRI sont des comités de revue institutionnelle internes à l'Institut Curie, dont la mission, en ce qui concerne la protection des données à caractère personnel, est d'examiner et d'émettre un avis sur la conformité des projets de recherche de l'Institut Curie.

Chaque CRI doit se doter d'une charte de fonctionnement intégrant cette mission.

8.2.1 Comité de Revue Institutionnelle (CRI)

Le Comité de Revue Institutionnelle de l'Institut Curie (CRI) a pour rôle de donner un avis sur toutes les Recherches impliquant la Personne Humaine au sens réglementaire, conçues et réalisées à l'Institut Curie ou par l'Institut Curie, au niveau national ou international. Son domaine de compétences couvre toutes les recherches organisées et pratiquées sur l'être humain en vue du développement des connaissances biologiques ou médicales, qu'il s'agisse de recherches interventionnelles ou non interventionnelles, sur l'être humain mais également sur échantillons et éléments du corps humain ou données recueillies lors de ces recherches.

Il s'assure de la conformité scientifique, médicale, réglementaire, éthique des recherches, de leur faisabilité, de leur organisation et de leur financement. Il propose également des axes d'amélioration dans l'avis émis pour une recherche.

Le CRI examine si le projet de recherche considéré :

- Nécessite de faire appel à des données à caractère personnel
- Nécessite un traitement de données sensibles
- Est conduit conformément à la réglementation applicable en matière de protection des données à caractère personnel
- Nécessite la mise en œuvre de mesures complémentaires

Il se réunit mensuellement. Il est composé de membres représentatifs de toutes les disciplines intervenant dans ces recherches, de la direction juridique, d'un membre qualifié dans le domaine éthique, et du DPO.

Le passage pour instruction d'une recherche devant le CRI est obligatoirement précédé par la validation du Groupe Thématique Transversal compétent.

Les avis du CRI sont tracés dans l'outil « Portail d'Echange et de Suivi Institutionnel des Etudes cliniques et translationnelles » (POESIE) de la Direction de la Recherche de l'Ensemble Hospitalier (DREH) et restitués dans un compte-rendu.

Le projet ne peut être accepté et/ou mis en œuvre tant que les recommandations relatives à la conformité à la protection des données à caractère personnel ne sont pas intégrées et conformes à la réglementation en vigueur.

8.2.2 CRI data

Le Comité de Revue Institutionnelle Data (CRI Data) a pour rôle d'examiner les projets de recherche n'impliquant pas la personne humaine, qui nécessite le traitement de données à caractère personnel. Le CRI Data s'assure que le projet de recherche a fait l'objet d'un protocole validé

scientifiquement et que les données sont pertinentes, adéquates et limitées. Son périmètre couvre aussi bien les projets du Centre de Recherche que de l'Ensemble Hospitalier.

A ce titre, le CRI Data se réunit périodiquement selon les projets à examiner. Il est composé de représentants de la Direction des Data, de la Direction des Systèmes d'Informations et de la Direction juridique, ainsi que du DPO.

En matière de protection des données à caractère personnel, son rôle est d'examiner si le projet considéré :

- Nécessite de faire appel à des données à caractère personnel,
- Nécessite le traitement de données sensibles,
- Est conduit conformément à la réglementation applicable, en particulier en matière de protection des données à caractère personnel,
- Pose un risque particulier en matière de sécurité, d'atteinte aux droits des personnes, etc.,
- Nécessite la mise en œuvre des mesures complémentaires.

Les avis du CRI Data sont tracés dans l'outil « Portail d'Echange et de Suivi Institutionnel des Etudes cliniques et translationnelles » (POESIE) de la Direction de la Recherche de l'Ensemble Hospitalier (DREH) et restitués dans un compte-rendu transmis systématiquement au DPO et au porteur de projet.

Le projet ne peut être accepté et/ou mis en œuvre tant que les recommandations relatives à la conformité à la protection des données à caractère personnel ne sont pas intégrées et conformes à la réglementation en vigueur.

9. Principaux processus à mettre en œuvre

9.1 Registre des traitements

L'Institut Curie documente l'ensemble des traitements de données à caractère personnel au moyen d'un registre précisant notamment :

- Les parties prenantes (représentant, sous-traitants, co-responsables, etc.) qui interviennent dans le traitement considéré,
- Les catégories de données traitées,
- La finalité du traitement,
- L'identité des personnes qui accèdent aux données et à qui ces dernières sont communiquées,
- La durée de conservation,
- Les moyens de sécurisation associés.

Ce registre des traitements :

- Est alimenté par les référents à la protection des données, sous la responsabilité de chaque responsable opérationnel de traitement,
- Est consolidé par le DPO, qui exerce un rôle de contrôle de cohérence et de sincérité,
- Sera transmis aux autorités réglementaires en cas de contrôle, et en particulier à la CNIL, dans le cadre de la réglementation en vigueur.

9.2 Documentation

Le responsable opérationnel du traitement formalise, conserve et met à disposition du DPO la documentation permettant de démontrer la conformité du traitement.

Cette documentation comporte en particulier :

- La description du traitement
- Le responsable de traitement et des co-responsables, les sous-traitants
- Les catégories et nombre de personnes concernées, de destinataires des données
- Les délais prévus pour l'effacement des données,
- Les finalités
- Les principes essentiels
    - Licéité, loyauté, transparence,
    - Finalités déterminées, explicites, légitimes, traitement ultérieur pas incompatible avec les finalités
    - Données adéquates, pertinentes et limitées, exactes, nécessaires et tenues à jour,
    - Durée n'excédant pas celles nécessaires aux finalités
    - Sécurité
- Base légale (consentement, contrat, obligation légale, intérêts vitaux, mission de service public, intérêts légitimes
- Les applications informatiques utilisées,
- Les catégories de données personnelles traitées, les données sensibles, les exceptions autorisant le traitement,
- Les transferts de données hors UE et les organisations destinataires,
- L'information faite (type, modalités de diffusion, ...)
- Procédures opérationnelles et techniques permettant l'exercice des droits des personnes (accès, rectification, limitation, portabilité, opposition, …)
- Les risques (droits et liberté, destruction, altération, divulgation, accès non autorisé, …)
- Les mesures de sécurité techniques et organisationnelles, mises en œuvre pour pallier aux risques, au niveau responsable de traitement, au niveau des sous-traitants
- Les mesures de sécurité spécifiques (pseudonymisation, chiffrement, confidentialité, intégrité, disponibilité, en cas d'incident, procédure d'évaluation régulière de l'efficacité des mesures techniques et organisationnelles, …
- Pour chaque sous-traitant, contrat, garanties apportées
- Documents complémentaires (nom, contenu, références)

9.3 Analyse d'impact

Dès lors qu'un nouveau traitement de données à caractère personnel doit être mis en œuvre, par exemple dans le cadre d'un nouveau projet de recherche, d'une nouvelle application, d'une nouvelle technique médicale, etc., ou lors d'une modification d'un traitement existant, la question de L'analyse d'impact doit être conduite afin d'examiner :

- La légitimité de la finalité du traitement,
- Le caractère raisonnable des données à caractère personnel collectées, au regard de la finalité poursuivie,
- Le caractère sensible ou non des données concernées,
- Les modalités de collecte,
- Les dispositifs de protection des données à caractère personnel et leur efficacité escomptée
- La conformité de l'ensemble des traitements réalisés pour une finalité identifiée à la réglementation applicable,
- Le niveau de risque pour l'Institut Curie et pour les personnes.

L'analyse d'impact sur la protection des données à caractère personnel est systématiquement faite pour les traitements suivants :

- Traitements de données de santé pour la prise en charge des personnes (dossier patient, prise de décision médicale, vigilances sanitaires, gestion du risque, télémédecine, laboratoire de biologie médicale, pharmacie à usage intérieur, …)
- Traitements portant sur des données génétiques (recherche médicale, consultation de génétique, …)

- Traitements établissant des profils de personnes à des fins de gestion de ressources humaines (détection de potentiels, aide au recrutement, actions de formations personnalisées, prévention des départs, …)
- Traitements visant à surveiller de manière constante l'activité des employés (cyber surveillance, vidéosurveillance, …)
- Traitements de gestion d'alertes et signalements en matière sociale et sanitaire, ou en matière professionnelle
- Traitements de données de santé nécessaires à la constitution d'entrepôt de données ou de registre (pour servir à des finalités de recherche, …)
- Traitements de profilage faisant appel à des données provenant de sources externes, …

La mise en œuvre de cette analyse relève de la responsabilité des responsables opérationnels de traitement, qui pourront pour cela s'appuyer notamment sur :

- Le DPO,
- La Direction des Data,
- La Direction des Systèmes d'Information,
- La Direction Juridique.

Dans le cas de projets de recherche, l'analyse d'impact constitue **un prérequis** à l'évaluation de tout projet en CRI ou CRI Data.

Dans tous les cas, les résultats de l'analyse d'impact doivent être obligatoirement communiqués au référent de l'entité et au DPO. Le DPO pourra rendre un avis sur la méthodologie employée et le niveau de risque résiduel du projet. Le DPO pourra assortir son analyse d'une série de recommandations, dont la mise en œuvre restera de la responsabilité du responsable opérationnel du traitement.

9.4 Audits internes

Les audits internes relatifs à la protection des données à caractère personnel ont pour objectif de vérifier que les principes, mesures et processus édictés dans le cadre de cette politique sont effectivement mis en œuvre.

Ces audits peuvent être commandités par le Comité d'audit et des finances, le Président et les membres du Directoire et être conduits par le DPO. Ces opérations d'audit sont planifiées en concertation avec les acteurs impliqués afin de limiter les risques de perturbation sur les activités de l'Institut Curie.

Chaque audit donne lieu à :

- Une lettre de mission validée par le Directoire,
- Un rapport de mission indiquant les résultats obtenus ainsi qu'un ensemble de recommandations assorti d'un calendrier de réalisation et attribuées à un responsable.

La mise en œuvre du plan d'actions est de la responsabilité des Directions concernées et les résultats des audits comme de l'effectivité des plans d'actions seront suivis, au moins annuellement, par le Directoire.

9.5 Gestion des incidents et gestion de crise

L'Institut Curie met en œuvre une procédure de gestion d'incidents relatifs à la protection des données à caractère personnel qui lui permet d'apporter une réponse rapide et adaptée à leur gestion, selon le principe suivant :

- Dès lors qu'une violation des données à caractère personnel est détectée par un collaborateur, celui-ci doit le signaler immédiatement à sa hiérarchie directe, au DPO, à la Direction juridique et à la Direction des Systèmes d'Information,
- Dans un second temps, et le plus rapidement possible, le DPO sera en charge d'investiguer et de documenter la violation afin de formuler une analyse sur son niveau de criticité,
- Une fois cette analyse partagée avec la Direction juridique et la Direction des Systèmes d'Information, et en cas de violation d'un certain niveau de criticité, des mesures de gestion de crise pourront être déclenchées.

Ces mesures pourront, selon les cas, se matérialiser par :

- L'organisation d'une réunion de crise en interne avec l'encadrement de l'entité concernée voire les membres du Directoire, afin d'arrêter la stratégie de traitement et les actions appropriées,
- Une déclaration auprès de la CNIL, sous 72h et dans les modalités prévues par la loi,
- Une information des individus, dans le cas où l'incident ferait courir un risque élevé pour la vie privée des personnes concernées.

9.6 Gestion des droits des personnes sur leurs données

L'Institut Curie définit une procédure de gestion des demandes d'exercice des droits des personnes sur leurs données.

Cette procédure de gestion est appliquée en lien avec le DPO et la Direction des Systèmes d'Information.

Toute demande est adressée par une personne via un mail ou un formulaire dédié sur le site internet de l'Institut Curie. Cette demande est redirigée :

- Soit au responsable opérationnel de traitement, s'il peut être identifié directement,
- Soit au DPO qui la transmet à la (aux) Direction(s) opérationnelle(s) concernée(s) et assure le contrôle de sa réalisation.

9.7 Gestion des relations avec l'autorité de contrôle

Toutes les interactions et relations avec la CNIL se font par l'intermédiaire du DPO.

Chaque échange, demande ou réponse à une requête, qu'elle qu'en soit la nature doit être communiqué *a minima* et en amont de son envoi au DPO, qui en valide les modalités et contenus avec l'appui de la Direction juridique.

De même, lors d'événements extérieurs où la CNIL et des représentants de l'Institut Curie seraient présents, en plus du DPO, un représentant de la Direction juridique devra être également être présent ou *a minima* en être informé en amont.

10. Applicabilité de la politique aux tiers

Les tiers (partenaires, prestataires) peuvent être amenés à intervenir dans le cadre des traitements de données à caractère personnel opérés par l'Institut Curie. Dans ce cadre, ils pourront être

responsables de la bonne mise en œuvre de la présente politique, sur un périmètre déterminé. Cette responsabilité sera déterminée et formalisée (contrats, conventions, marchés, …) au cas par cas.