Politique de Protection des Données Personnelles

FICHE DE CONTROLE DU DOCUMENT

Auteur : Délégué à la Protection des Données	
Date de création	21 juin 2019
Date de dernière modification	26/03/2020

Version	Date	Auteur(s)	Section	Observations
V2	26/03/2020	Nicolas Barras (Responsable opérationnel de PELyon)	4.2 Sous-Traitants	« UCBL » remplacé par les prestataires actuels
V2	26/03/2020	Nicolas Barras (Responsable opérationnel de PELyon)	5.1 Mesures générales de sécurité	« UCBL » remplacé par « XEFI »
V2	26/03/2020	Nicolas Barras (Responsable opérationnel de PELyon)	5.3.3 Marketing et prospection commerciale	Adresse DPO mise à jour
V2	26/03/2020	Nicolas Barras (Responsable opérationnel de PELyon)	Footer	Adresse de la société mise à jour

Sommaire

1. PREAMBULE

La société PELyon (ci-après désignée « **PELyon** ») est une société spécialisée dans la conduite d'études réalisées à partir des données du Système National des Données de Santé, (ci-après « SNDS »), aussi appelé SNDS central, principalement en pharmaco épidémiologie, afin d'étudier les fardeaux économiques et cliniques des maladies, et de comparer des stratégies de prise en charge.
La présente politique de protection des données personnelles (ci-après la « ***Politique*** ») a pour objet de décrire les conditions du respect des règles de protection des données personnelles par les utilisateurs du système d'information de **PELyon**.

Cette Politique s'inscrit dans le cadre des Procédures Opérationnelles Standardisées (POS) de PELyon. Elle est élaborée de manière à garantir que PELyon exerce ses activités conformément aux législations nationales, européennes et internationales relatives à la protection des données personnelles et, en particulier, le Règlement (UE) n° 2016/679 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 (dit « Règlement général sur la protection des données » ou « ***RGPD*** ») et la loi française n° 78-17 du 6 janvier 1978 modifiée, relative à l'informatique aux fichiers et aux libertés (la « ***Loi Informatique et Libertés*** ») (ensemble la « ***Réglementation Applicable*** »).

S'agissant du traitement de données personnelles réalisé à partir du portail SNDS, PELyon s'engage par ailleurs à exercer ses activités dans le respect du référentiel déterminant les critères de confidentialité, d'expertise et d'indépendance pour les laboratoires de recherche et bureaux d'études établi par l'arrêté du 17 juillet 2017, ainsi que le référentiel de sécurité applicable au Système national des données de santé prévu par l'arrêté du 22 mars 2017.

1.1 Respect de cette Politique

Le respect de cette Politique est essentiel pour assurer la conformité de PELyon aux exigences de la Réglementation Applicable. Le non-respect des principes posés par la Réglementation Applicable est passible de sanctions administratives[1] et/ou de sanctions pénales[2].

Il est de la responsabilité de chaque Employé, tel que défini ci-après, d'adhérer à cette Politique et d'en respecter l'ensemble des termes lorsqu'il accède et utilise le système d'information de PELyon et qu'il traite des Données Personnelles. Cela permet de fournir l'assurance, tant en interne que vis-à-vis des tiers, de l'engagement de PELyon à maintenir la confidentialité et la sécurité des Données Personnelles traitées et à respecter les exigences de la Réglementation Applicable.

Cette Politique devra être remise à chaque nouvel Employé qui s'engage à la lire et la signer en double exemplaire. Un exemplaire sera conservé par l'Employé et un exemplaire sera conservé par le département Ressources Humaines, dans le dossier de l'Employé.

[1] Sanctions administratives pouvant atteindre 10 ou 20 millions d'euros selon la nature du manquement (ou 2%/4% du chiffre d'affaires mondial d'une entreprise).
[2] Sanctions pénales pouvant atteindre 300 000 euros d'amende et 5 ans d'emprisonnement pour une personne physique et de 1,5 millions d'euros pour une personne morale.

Cette Politique sera par ailleurs communiquée, par email ou tout autre moyen avec accusé de réception, à tout Employé de PELyon en exercice au jour de l'entrée en vigueur de la Politique. L'Employé devra lire la Politique et la signer en double exemplaire.

1.2 Contrôle

PELyon a désigné un Délégué à la Protection des Données (« ***DPO*** ») afin de mettre en œuvre sa conformité à la Réglementation Applicable. Une des fonctions du DPO est de contrôler le respect des principes de protection des Données Personnelles par PELyon, dont, notamment, le respect par les Employés de la Politique.

Le DPO de PELyon peut être contacté par courriel à l'adresse suivante : dpo@pelyon.fr.

1.3 Définitions

Afin de mieux comprendre les notions utilisées dans la Politique, le RGPD a proposé un certain nombre de définitions des termes couramment employés en matière de protection des données personnelles. Les définitions reproduites ci-après sont issues de l'article 4 du RGPD.

Dans la Politique, les mots ou expressions commençant par une majuscule, qu'ils soient employés au singulier ou au pluriel, ont la définition ci-après :

- **Anonymisation :** processus empêchant la ré-identification des individus. Concrètement, cela signifie que toutes les informations directement ou indirectement identifiantes sont supprimées ou modifiées, rendant ainsi impossible toute réidentification de la personne.

- **Consentement :** 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 personnelles la concernant fassent l'objet d'un traitement.

- **Destinataire :** la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement.

- **Donnée Personnelle** : toute information relative à une personne identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques qui lui sont propres. A titre d'exemples, les coordonnées du personnel de PELyon, les données des Employés sur l'absence de conflit d'intérêt relatif à l'objet du Traitement opéré dans le cadre de l'étude, les données de pharmacovigilance, les noms des clients et fournisseurs, sont autant de données rattachables à une personne identifiée directement ou identifiable par un numéro de référence. Elles doivent donc être considérées comme des données personnelles.

- **Donnée SNDS :** Données Personnelles issues du SNDS et traitées par PELyon dans un espace projet du portail SNDS

- **Données :** désigne collectivement les Données Personnelles ainsi que la catégorie particulière des Données SNDS qui font l'objet du Traitement par PELyon dans le cadre de ses activités.

- **Employé :** une personne employée de PELyon, quel que soit son statut (CDI, CDD, intérim, stage, etc.) ou mise à disposition de PELyon, ayant accès et utilisant le système d'information de PELyon pour l'exercice de ses fonctions, qu'il soit dans les locaux de PELyon ou à l'extérieur.

- **Fichier :** tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

- **Personne Concernée** : personne physique à laquelle se rapportent les Données Personnelles. Il s'agit essentiellement des usagers du système national de santé, mais vise également les Employés de PELyon dont les Données Personnelles sont traitées dans le cadre de leur contrat de travail.

- **Pseudonymisation :** Procédé visant à la génération d'un identifiant pseudonymisé, appelé ici pseudonyme, à partir d'un identifiant initial signifiant lié à une personne (par exemple: nom, prénom, numéro de sécurité sociale NIR). Le procédé de pseudonymisation ne doit pas permettre l'identification individuelle directe de la personne associée à ce pseudonyme (l'identification indirecte reste toutefois possible). Ce processus est utilisé pour contribuer à l'anonymat et au respect de la vie privée des individus.

- **Responsable de traitement** : la personne physique ou morale qui décide de la finalité et des moyens d'un traitement de données personnelles.

- **Sous-traitant** : la personne physique ou morale qui traite des données personnelles pour le compte du responsable de traitement.

- **Traitement de Données Personnelles ou Traitement** : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données personnelles, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

- **Traitement transfrontalier** : a) un traitement de données personnelles qui a lieu dans l'Union européenne dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres; ou b) un traitement de données personnelles qui a lieu dans l'Union européenne dans le cadre des

activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres.

2. PRINCIPES DE PROTECTION DES DONNEES PERSONNELLES

La Politique est fondée sur le respect des principes décrits ci-après, posés par la Réglementation Applicable.

En tant que Responsable des traitements qu'elle met en œuvre dans le cadre notamment de la gestion des ressources humaines, les relations clients, prospects, fournisseurs ou autres partenaires commerciaux, PELyon est responsable du respect de ces principes et doit être en mesure de démontrer à tout moment leur respect.

PELyon doit également s'assurer du respect de ces principes lorsqu'elle agit comme Sous-Traitant de ses clients qui font appel à ses services pour la réalisation d'études.

La mise en œuvre et le respect de ces principes sont essentiels et doivent être contrôlés régulièrement par les personnes qui sont responsables des problématiques liées au Traitement de Données Personnelles au sein de PELyon.

2.1 Licéité, loyauté et transparence

Les Données Personnelles doivent être traitées de manière licite, loyale et transparente au regard de la Personne Concernée par le Traitement de Données Personnelles.

2.2 Limitation des finalités

Les Données Personnelles doivent être traitées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

2.3 Minimisation des données

Les Données Personnelles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

2.4 Exactitude

Les Données Personnelles doivent être exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les Données Personnelles qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder.

2.5 Limitation de la conservation

Les Données Personnelles doivent être conservées sous une forme permettant l'identification des Personnes Concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Elles peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt

public, à des fins de recherche scientifique ou historique ou à des fins statistiques, pour autant que soient mises en œuvre des mesures techniques et organisationnelles appropriées afin de garantir les droits et libertés de la personne concernée.

2.6 Intégrité et confidentialité

Les Données Personnelles doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le Traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.

3. DONNEES PERSONNELLES TRAITEES PAR PELYON

3.1 Données traitées dans le cadre des activités de PELyon

En fonction des finalités des Traitements de Données PELyon agit comme Responsable ou Sous-Traitant des Traitements de Données mis en œuvre. La nature desdites Données traitées varie en fonction de la qualité de PELyon.

3.1.1 Données traitées par PELYON en tant que Responsable de Traitement

Les Données Personnelles collectées et traitées par PELyon en tant que Responsable de Traitement concernent essentiellement les Employés de PELyon, laquelle doit, en tant qu'employeur, traiter les Données Personnelles nécessaires à la conclusion et à l'exécution de leurs contrats de travail.
Les Données Personnelles ainsi traitées par PELyon sont collectées directement auprès de ses Employés au cours de la phase de recrutement, préalablement à la conclusion de leur contrat de travail. PELyon peut également collecter certaines Données Personnelles en cours d'exécution du contrat de travail, notamment en cas d'évolution de la situation de l'Employé.

PELyon collecte et traite aussi des Données Personnelles sur les Employés aux fins qu'ils attestent dans la déclaration d'intérêt réalisée par PELyon en application de l'arrêté du 17 juillet 2017 portant référentiel déterminant les critères de confidentialité, d'expertise et d'indépendance pour les laboratoires de recherche et bureaux d'études, de l'absence de conflits d'intérêt avec l'objet du Traitement de Données SNDS dans lequel il intervient.

Les Données Personnelles des Employés traitées par PELyon sont notamment les suivantes :

- Etat civil (nom, prénom, âge, sexe) ;
- Coordonnées personnelles (adresse postale, adresse e-mail, numéro de téléphone) ;
- Informations d'ordre économique (RIB notamment pour le versement des salaires) ;
- Situation familiale des Employés (état civil des ayant-droits, nombre d'enfants, etc.) ;
- Numéro de sécurité sociale des Employés et, le cas échéant, de leurs ayant-droits ;
- Informations sur l'existence de liens d'intérêt avec l'objet du Traitement de Données SNDS (activités exercées à titre principal e/ou secondaire au cours des trois dernières années au sein ou avec des organismes ou établissements dont les activités, techniques et produits entrent dans le champ de l'objet du Traitement de Données SNDS dans lequel i intervient.

PELyon collecte par ailleurs les Données Personnelles des candidats à l'embauche qui lui adressent leurs curriculum vitae dans le cadre de leurs candidatures, et réalise d'autres Traitements tels que ceux relatifs à la gestion des relations clients, prospects, fournisseurs ou autres partenaires commerciaux

3.1.2 Données traitées par PELYON en tant que Sous-Traitant

3.1.2.1. Données du Système National des Données de Santé

Dans le cadre de ses activités, PELyon est amenée à traiter les Données Personnelles, notamment les Données SNDS.

Le SNDS regroupe ainsi :

- Les données de l'Assurance Maladie (Système National d'Information Inter Régimes de l'Assurance Maladie - base SNIIRAM) ;
- Les données des hôpitaux et autres établissements de santé (Programme de Médicalisation des Systèmes d'Information - base PMSI) ;
- Les données statistiques relatives aux causes médicales de décès (BCMD - base du CépiDC de l'Inserm).

Après que l'étude commandée par le client ait été autorisée par la CNIL, les Données SNDS sont extraites par la Caisse Nationale d'Assurance Maladie (ci-après la « **Cnam** ») sur la base des critères d'extraction communiqués par PELyon sur instructions du client. Une fois les Données SNDS extraites par la Cnam, celles-ci sont mises à disposition de PELyon sur un espace projet du portail SNDS, lequel est dédié au Traitement mis en œuvre dans le cadre de l'étude menée par PELyon. Cet espace projet mis à disposition de PELyon répond aux exigences de sécurité, de confidentialité, d'intégrité des Données, et de traçabilité des accès, conformément au référentiel de sécurité applicable au SNDS défini par l'arrêté du 22 mars 2017, et de l'autorisation délivrée par la Commission Nationale Informatique et Libertés.

3.1.2.2. Données des dossiers médicaux ou de programmes de recherches communiquées par les clients de PELyon

Dans le cadre de ses activités, PELyon peut également être amenée à traiter des Données pseudonymisées issues de dossiers médicaux des Personnes Concernées ou de programme de recherche, qui lui sont communiquées par ses clients, pour la réalisation des études.
Ces Données sont exportées vers l'espace projet mis à disposition de PELyon par la Cnam sur le portail SNDS, puis chaînées avec les Données SNDS extraites par la CNAM).

PELyon conserve par ailleurs une copie des Données qui lui sont adressées par ses clients sur son système d'information.

3.2 Finalités des traitements de données

Les finalités des Traitements de Données Personnelles varient selon que PELyon agisse comme Responsable ou Sous-Traitant des Traitements de Données Personnelles qu'elle met en œuvre.

3.2.1 PELyon Responsable de traitement

PELyon, Responsable de traitement, collecte et traite les Données Personnelles des Employés notamment pour les finalités suivantes :

- La gestion administrative du personnel (dossiers des Employés, développement de carrière, formation, annuaire, paie, mutuelle, prévoyance, déplacements, etc.) ;
- Le respect de ses obligations légales en tant qu'employeur
- La gestion des recrutements
- L'attestation de l'absence de conflit d'intérêt avec l'objet du Traitement des Données SNDS.

3.2.2 PELyon Sous-Traitant

PELyon est amenée à traiter les Données SNDS, ainsi que les Données qui lui sont communiquées par ses clients pour être appariées avec les Données SNDS, aux fins de réaliser les études qui lui ont été confiées par ses clients, et dont les finalités sont décrites dans les protocoles rédigés par ces derniers et autorisées par la CNIL.

Les Employés reconnaissent être informés que l'accès aux Données SNDS et leur utilisation pour les finalités précitées ne peuvent se faire que dans les conditions respectant le référentiel de sécurité applicable au SNDS prévu par l'arrêté du 22 mars 2017, visant à garantir la confidentialité et l'intégrité des Données et la traçabilité des accès et autres Traitements.

Cet accès est par ailleurs conditionné par un engagement de confidentialité des Employés conforme au référentiel de sécurité applicable au SNDS établi par l'arrêté du 22 mars 2017

Il est à ce titre précisé que l'Employé autorisé à accéder à l'espace projet sur le portail SNDS reconnait expressément que ses identifiants d'accès audit portail sont strictement personnels et confidentiels, de sorte qu'il ne doit en aucun cas les divulguer à un quelconque autre Employé de PELyon ou à un tiers.

3.3 Registre des traitements

Conformément à la Réglementation Applicable, le Responsable de traitement et le Sous-Traitant doivent tenir un registre des activités de Traitement de Données Personnelles (le « ***Registre*** »). Le Registre permet de cartographier de façon précise les Traitements effectués par PELyon. Le Registre est ainsi constitué d'autant de fiches qu'il existe de Traitements identifiés.

Le Registre du Responsable de traitement doit comporter les informations suivantes :

- date de création du Traitement ;
- noms et coordonnées du Responsable du Traitement (PELyon), de son représentant au sein de la direction et du DPO ;
- finalités du Traitement ;
- catégories de Personnes Concernées ;
- catégories de Données Personnelles traitées ;
- catégories de destinataires auxquels les Données seront communiquées ;

- transferts de données hors de l'Union européenne ;
- délais prévus pour l'effacement des différentes catégories de Données ;
- mesures de sécurité techniques et organisationnelles.

Le Registre du Sous-Traitant doit comporter les informations suivantes :

- noms et coordonnées du Sous-Traitant (PELyon) et de chaque Responsable de Traitement (client) pour le compte duquel le Sous-Traitant agit, le cas échéant, les noms de leur représentant et du DPO ;
- catégories de Traitements effectués pour le compte de chaque Responsable de Traitement ;
- le cas échéant, les transferts de Données Personnelles mis en œuvre ;
- mesures de sécurité techniques et organisationnelles.

La tenue et la mise à jour du Registre sont contrôlées par PELyon.

Dans l'hypothèse où un Employé entendrait effectuer un nouveau Traitement de Données Personnelles ou lorsque des modifications sont apportées à un Traitement existant (ex. nouvelles catégories de données traitées, nouveaux destinataires, etc.), l'Employé s'engage à en informer le la personne en charge de la tenue du registre au sein de PELyon afin de créer une nouvelle fiche de traitement ou mettre à jour une fiche existante.

Cette notification permet également au DPO de contrôler la bonne tenue du Registre et de déterminer si le Traitement considéré, du fait des risques élevés qu'il pourrait engendrer sur les droits et libertés des Personnes Concernées, nécessite la réalisation d'une analyse d'impact relative à la protection de la vie privée (dite « ***PIA*** » pour Privacy Impact Assessment). Dans ce dernier cas, l'Employé concerné par le Traitement s'engage à coopérer avec le DPO dans la réalisation de ce PIA et à prendre toutes mesures prescrites par le DPO pour réduire les risques engendrés par le traitement.

4. COMMUNICATION ET ECHANGES DE DONNEES PERSONNELLES

PELyon est particulièrement sensible à la question de la protection des Données Personnelles qu'elle collecte et/ou traite dans le cadre de ses activités.

PELyon prend ainsi toutes les précautions utiles pour que les Données Personnelles des Personnes Concernées soient accessibles aux seuls Employés susceptibles d'en avoir l'utilité pour l'exercice de leurs fonctions et aux seuls tiers pour lesquels leur transmission est fondée sur un motif légitime tenant à la finalité du Traitement opéré.

PELyon assure par conséquent un haut niveau de sécurité et de confidentialité des Données Personnelles qu'elle traite par la mise en œuvre de mesures techniques, juridiques et organisationnelles appropriées et adéquates, et dans le strict respect des règles applicables au portail SNDS auquel PELyon a accès dans le cadre des études conduites pour le compte de ses clients.

Chaque Employé amené à connaître et/ou traiter des Données Personnelles s'engage à se conformer à la Politique et mettre en œuvre les mesures de sécurité qu'elle définit.

4.1 Employés de PELyon

Seuls les Employés dont la connaissance de Données Personnelles est strictement nécessaire pour l'exercice de leurs fonctions doivent être autorisés à recevoir des Données Personnelles. Il appartient au responsable hiérarchique direct de l'Employé de veiller au bon respect de cette règle.

Chaque Employé s'engage à ne traiter que les Données Personnelles pertinentes au regard de la finalité du traitement qu'il opère, de sorte que :

- Seuls les Employés ayant à connaitre des Données Personnelles dans le cadre de leurs fonctions doivent avoir accès aux Données Personnelles des Employés ;

- Seuls les Employés de PELyon ayant à connaitre des Données du SNDS pour la réalisation des études confiées par les clients de PELyon doivent être autorisés à accéder à l'espace projet du portail SNDS. De plus, seuls les Employés qui sont nommément désignés dans le protocole de l'étude pour laquelle la CNIL a donné une autorisation sont autorisés à accéder aux Données du portail SNDS.

Les Employés amenés à connaitre, utiliser et/ou plus largement traiter des Données Personnelles s'engagent à maintenir une stricte confidentialité des Données Personnelles qu'ils traitent, ainsi que la stricte confidentialité de leurs identifiants d'accès à l'espace projet du portail SNDS, de sorte qu'il leur est formellement interdit de divulguer lesdits identifiants à un Employé qui n'a pas été nommément autorisé à accéder aux Données SNDS ou à un tiers.

S'agissant particulièrement des Données du portail SNDS accessibles depuis l'espace projet, il est expressément précisé qu'en aucun cas un Employé ne saurait réaliser une quelconque copie, duplication, importation, transfert, partage et/ou échange de Données, lesquels constituent des pratiques prohibées de nature à engager sa responsabilité professionnelle.

Ainsi, les Données du portail SNDS ne doivent en aucun cas quitter l'environnement sécurisé (serveurs sécurisés du SNDS), dont les accès sont restreints aux seuls Employés autorisés à connaître des Données Personnelles, conformément aux règles de sécurité posées par la Politique, le référentiel de sécurité applicable au SNDS (arrêté du 22 mars 2017) et au référentiel déterminant les critères de confidentialité, d'expertise et d'indépendance pour les laboratoires de recherche et bureaux d'études (arrêté du 17 juillet 2017).

L'Employé veillera à ce qu'aucune Donnée Personnelle directement identifiante ne soit rendue accessible à PELyon sur le portail SNDS. Le cas échéant, l'Employé informera son supérieur hiérarchique et le DPO de PELyon afin que ce dernier informe la Cnam de la violation de Données Personnelles.

S'agissant des Données Personnelles relatives aux Employés qui sont nécessaires à la conclusion et l'exécution des contrats de travail, tout Employé en charge du Traitement de telles Données Personnelles veille à stocker le minimum de documents contenant des Données Personnelles sur son poste de travail (sur le bureau, dans un dossier Windows, dans le dossier de Téléchargement, etc.). L'Employé s'engage à régulièrement vérifier la pertinence des Données Personnelles qu'il

stocke sur le système d'information de PELyon et supprimer les Données Personnelles obsolètes (suppression du fichier et vidage de la corbeille).

4.2 Sous-Traitants

Dans le cadre de ses activités PELyon est amenée à partager ou communiquer les Données Personnelles de ses Employés, ainsi que les éventuelles Données communiquées par ses clients, au prestataires :
-XEFI et ACRT qui mettent à disposition et gère le système d'information et de communications de PELyon ;
-BNP Paribas Real Estate qui gère les moyens d'accès au lieu de travail.

Au sens de la Réglementation Applicable, ces prestataires agissent à ce titre comme Sous-Traitant de PELyon. Leur accès aux Données Personnelles doit être strictement encadré par contrat signé avec PELyon. Les contrats doivent prévoir les conditions et modalités d'accès et d'utilisation des Données Personnelles par ces prestataires, ainsi que les mesures de sécurité appropriées devant être mises en œuvre par ces derniers.

4.3 Autres destinataires

PELyon peut être amenée à communiquer des Données Personnelles d'Employés à des tiers autres que le Sous-Traitant visé au point 4.2 ci-avant, tels que les autorités réglementaires et/ou gouvernementales, ou toute autre entité lorsque cela est requis par la Réglementation Applicable ou une décision de justice.

Tout Employé amené à divulguer des Données Personnelles d'Employés à des tiers doit veiller à ce que cette communication soit couverte contractuellement par un accord de confidentialité devant préciser les conditions et modalités de la communication et de l'utilisation subséquente pouvant être faite des Données Personnelles. Cette disposition ne s'applique pas en cas d'audit diligenté par une autorité administrative en application de la Réglementation Applicable.

Aucune Donnée accessible depuis l'espace projet du portail SNDS ne pourra faire l'objet d'une communication à des tiers par PELyon, cette dernière n'étant pas autorisée à procéder à une quelconque copie ou extraction desdites Données. Tout tiers souhaitant avoir accès aux Données du portail SNDS devra s'adresser directement auprès de la Cnam, PELyon ne pouvant consentir à de telles demandes.

5. MESURES DE SECURITE DES DONNEES PERSONNELLES

5.1 Mesures générales de sécurité

Les Données Personnelles des Employés ainsi que les Données communiquées à PELyon par ses Clients sont protégées par les mesures de sécurité du système d'information mis en œuvre et géré par le prestataire XEFI. XEFI maintient un haut niveau de sécurité du système d'information afin de protéger les Données Personnelles qui y sont stockées et emploie des mesures de sécurité techniques et organisationnelles conformes aux standards de l'industrie prévues pour prévenir la

destruction, la perte ou l'altération, la divulgation et/ou l'accès non autorisés aux Données Personnelles.

5.2 Protection des Données contenues sur le portail SNDS

La sécurité et la confidentialité des Données contenues sur le portail SNDS et qui sont mises à disposition de PELyon via l'espace projet sont garanties par l'application stricte de l'arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au SNDS, lequel établi les standards devant être mis en place avant la mise à disposition de données du SNDS, ainsi que par le respect des règles du RGPD, de la Politique générale de sécurité des systèmes d'information en sante (PGSSI-S), de la Politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSU MCAS), des règles applicables dans le cadre du Référentiel Général de Sécurité (RGS) et de la Loi Informatique et Libertés.

Il est expressément préconisé à l'Employé de conserver ses identifiants et dispositif d'accès (tokken i.e. calculette) à l'espace projet du portail SNDS dans un environnement sécurisé, sous clé et à ne jamais les partager avec un autre Employé ou un tiers.

5.3 Messagerie électronique

Les Employés de PELyon s'engagent expressément à mettre en place les règles de bonnes pratiques du courrier électroniques définies ci-après, lesquelles prévoient les mesures de sécurité que chaque Employé doit respecter lorsqu'il utilise sa messagerie électronique.

Chaque Employé s'engage à limiter autant que faire se peut la divulgation de Données Personnelles par le biais de sa messagerie électronique, que ce soit dans le corps du courriel ou en pièce jointe.

5.3.1 Expédition d'emails

Lorsqu'il expédie un email contenant des Données Personnelles ou auquel serait joint un fichier contenant des Données Personnelles, l'Employé doit veiller à ce que les destinataires soient autorisés à recevoir ces Données Personnelles, en vertu de leurs fonctions, du contrat qui les lie à PELyon, d'une obligation légale ou d'une décision de justice. En cas de doute, l'Employé doit en référer à son responsable hiérarchique direct et au DPO avant l'envoi du courriel.

Les emails expédiés doivent être classés dans le dossier correspondant s'il en existe un. Ils doivent être conservés pendant le temps nécessaire au Traitement des Données Personnelles conformément aux règles de conservation définies dans la Politique (point 6 ci-après).

5.3.2 Réception d'emails

Lorsqu'il reçoit un email contenant des Données Personnelles ou auquel serait joint un fichier contenant des Données Personnelles, l'Employé veille à vérifier l'adéquation et la pertinence des Données Personnelles reçues par rapport à la finalité de l'opération traitée par email.

Toutes Données Personnelles reçues qui ne seraient pas pertinentes ne devront en aucun cas être stockées sur le système d'information de PELyon et devront être supprimées immédiatement par

l'Employé (suppression de l'email et des pièces jointes, vidage de la corbeille, le cas échéant suppression du fichier dans le dossier « Téléchargement » sur le poste de travail de l'Employé) ou anonymisées conformément à la Politique (point 5.4 ci-après).

L'Employé veillera également à informer l'expéditeur de l'inadéquation des Données Personnelles transmises par rapport à la finalité de l'opération considérée et lui rappeler les règles de protection des données personnelles. Au besoin, l'Employé s'adressera au DPO de PELyon afin d'obtenir les informations utiles pour répondre à l'expéditeur.

5.3.3 Marketing et prospection commerciale

Lorsque l'Employé procède à l'envoi d'emailing à des fins de prospection commerciale et/ou de communication marketing, à partir des adresses emails des Intervenants, il veille à préciser en pied de chaque email la mention suivante relative au droit du destinataire de se désinscrire de la liste d'emailing.

« *Vous disposez à tout moment d'un droit d'opposition à l'utilisation de vos données à des fins de prospection commerciale. Vous pouvez exercer ce droit en vous adressant au Délégué à la Protection des Données de* PELyon*, à l'adresse suivante : dpo@pelyon.fr*».

En cas de demande de désinscription adressée directement à l'Employé, ce dernier informe immédiatement le DPO de cette demande.

L'Employé s'engage à prendre toutes les mesures prescrites par le DPO pour bloquer la personne désinscrite afin de garantir le bon respect de son droit d'opposition et s'assurer qu'aucun email prospectif futur ne lui sera adressé. Une liste d'opposition est conservée par le DPO.

5.4 Mesures de Pseudonymisation et Anonymisation des Données

Les Données Personnelles des Employés étant nécessaires pour la conclusion et l'exécution de leurs contrats de travail, aucune mesure de pseudonymisation ni d'anonymisation n'est mise en place PELyon à ce titre.

Par ailleurs, les Données issues des dossiers médicaux qui sont communiquées à PELyon par ses clients pour la conduite des études sont quant à elles transmises sous forme pseudonymisée, de sorte que PELyon n'est pas elle-même tenue de mettre en place des mesures de pseudonymisation des Données préalablement à leur intégration sur l'espace projet du portail SNDS.

Enfin, les Données mises à disposition de PELyon sur l'espace projet du portail SNDS sont exclusivement accessibles sous forme pseudonymisée, aucune Donnée directement identifiante ne devant apparaitre sur le portail SNDS.

5.5 Minimisation des données

L'Employé doit veiller à ne collecter et/ou traiter que les Données Personnelles utiles, pertinentes, adéquates et proportionnées au regard des finalités pour lesquelles elles sont collectées et/ou traitées.

Le cas échéant, l'Employé doit procéder à la suppression ou l'Anonymisation complète des Données Personnelles non pertinentes.

L'Employé doit veiller, lorsqu'il reçoit des Données Personnelles, à supprimer toute Donnée Personnelle non utile au regard de la finalité du traitement considéré.

Au besoin, l'Employé peut solliciter l'assistance du DPO de PELyon pour déterminer la pertinence des Données Personnelles qu'il détient.

5.6 Sécurité des transferts de Données Personnelles hors de l'Union européenne

Lorsque des Données Personnelles d'Intervenants résidants dans l'Union européenne sont transmises à des destinataires situés hors de l'Union européenne, des mesures de sécurité particulières doivent être mises en œuvre afin de garantir une protection adéquate des Données Personnelles transmises.

L'Employé doit s'assurer que le destinataire des Données Personnelles présente des garanties suffisantes de sécurité des Données Personnelles qu'il reçoit, en vertu du contrat qui les lie à PELyon. En cas de doute, l'Employé doit en référer à son responsable hiérarchique direct et/ou au DPO avant le transfert des Données Personnelles.

L'Employé doit également privilégier l'envoi des Données Personnelles par des canaux sécurisés mis à sa disposition sur le système d'information de PELyon.

6. CONSERVATION DES DONNEES

Les Données Personnelles des Employés doivent être conservées pendant une durée n'excédant pas la finalité du traitement pour lequel elles sont collectées. Au-delà, les Données Personnelles doivent être supprimées ou archivées. Ainsi, dès lors qu'un Employé de PELyon quitte ses fonctions, l'Employé de PELyon en charge du Traitement des Données Personnelles dans le cadre des ressources devra par conséquent procéder à l'archivage des Données Personnelles dudit Employé.

De la même manière, lorsque PELyon traite les Données des Personnes Concernées qui lui sont communiquées par ses clients pour la conduite des études, PELyon s'engage à supprimer, à restituer ou à archiver les Données Personnelles qui lui ont été transmises lorsque l'étude est terminée conformément aux dispositions convenues entre le Client et PELyon.

PELyon a mis en place une politique de conservation des Données Personnelles, disponible en Annexe de la Politique.

7. GESTION DES DEMANDES DE TIERS

Toute demande, requête et/ou réclamation d'une Personne Concernée ou d'un tiers adressée à un Employé et concernant l'exercice de droits, la protection et/ou la violation de Données Personnelles doit être immédiatement adressée au DPO par email à l'adresse suivante dpo@pelyon.fr
L'Employé veillera à préciser au DPO le contexte de sa relation avec la personne sollicitant l'exercice de ses droits ou toute information relative à la protection des Données Personnelles.

Seul le DPO est habilité à répondre aux demandes de tiers, sauf s'il autorise l'Employé à le faire. Dans ce dernier cas, l'Employé s'engage à respecter les instructions du DPO avant de répondre à la personne.

7.1 Réponse aux demandes d'exercice des droits

Conformément à la Réglementation Applicable, toute Personne Concernée par le Traitement de ses Données Personnelles dispose de droits sur les Données Personnelles le concernant traitées par PELyon.

Ces droits sont les suivants :

- Droit d'accès
- Droit de rectification
- Droit à l'effacement (droit à l'oubli)
- Droit à la limitation du traitement
- Droit à la portabilité
- Droit d'opposition

Sauf dans le cas où la demande parait excessive (notamment s'agissant des Données nécessaires à l'exécution du contrat de travail en cours) ou si elle exige des efforts disproportionnés, le Responsable de traitement a l'obligation de répondre aux demandes d'exercice de droits dans les meilleurs délais et au plus tard un mois après réception de la demande.

Le DPO informera le responsable, au sein de PELyon, du traitement des Données Personnelles de la Personne Concernée exerçant ses droits sur ses Données Personnelles de la réponse qu'il entend donner à cette demande et des mesures à effectuer sur les Données Personnelles de la Personne Concernée.

Le responsable, au sein de PELyon, du Traitement des Données Personnelles de la Personne Concernée exerçant ses droits, veillera à ce que chaque Employé sous sa responsabilité rectifie et/ou efface lesdites Données Personnelles conformément à sa demande, en quelque lieu de stockage où se trouvent les Données Personnelles concernées (réseau, poste de travail, messagerie électronique, armoire, etc.) et sur quelque support que ce soit.

En cas de retrait de consentement, de demande d'opposition ou d'effacement des Données Personnelles d'une Personne Concernée, une copie des Données Personnelles sera effectuée par l'Employé en charge d'exécuter la demande et sera transmise au DPO, à des fins de preuve.

7.2 Gestion des violations des données

Le Responsable de traitement a l'obligation de notifier dans les meilleurs délais de sa constatation et au plus tard dans les soixante-douze (72) heures, l'existence d'une violation de Données Personnelles à l'autorité de contrôle et à la personne concernée dès lors que la violation est susceptible d'engendrer un risque pour les droits et libertés des personnes.

La violation de données personnelles est définie par la Réglementation Applicable comme « *une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données* » (article 4 12° du RGPD).

Chaque Employé s'engage à informer immédiatement le DPO par email, à l'adresse suivante : dpo@pelyon.fr et son responsable hiérarchique direct, en cas de découverte et/ou de suspicion d'une violation de Données Personnelles (réception d'un email malveillant ; faille de sécurité ; perte/vol d'un matériel contenant des Données Personnelles ; etc.).

L'Employé veillera, autant que faire se peut, à préciser la nature de la violation présumée, les catégories et le nombre approximatif de Données et de Personnes concernées, les conséquences probables de la violation pour les droits et libertés de(s) Personne(s) concernée(s) par la violation.

Seul le DPO est habilité à notifier à l'autorité de contrôle et/ou à la Personne concernée la violation de Données Personnelles, sauf autorisation préalable donnée à l'Employé pour se faire.

L'Employé s'engage à prendre toutes les mesures qui seront prescrites par le DPO pour prévenir et/ou endiguer la violation de Données Personnelles. Le responsable concerné s'engage à contrôler la mise en application des mesures prescrites par son Employé.

8. SANCTIONS

Toute violation ou manquement aux règles édictées par la Politique devra être immédiatement notifiée au DPO qui en référera à la direction de PELyon.

Toute violation ou manquement à la Politique pourra être passible de sanction disciplinaire.

9. CONTACT

Pour tous renseignements et questions relatifs à la Politique ou les pratiques de PELyon en matière de protection des Données Personnelles, merci d'adresser un email au DPO à l'adresse suivante : dpo@pelyon.fr ou de le contacter par téléphone via le standard de PELyon.

ANNEXE – DUREE DE CONSERVATION ET ARCHIVAGE DES DONNEES PERSONNELLES

1. DONNEES RH

Les Données Personnelles relatives à la gestion administrative du personnel pourront être conservées le temps de la période d'emploi de la Personne Concernée. Au-delà, les Données pourront être archivées sur un support informatique ou papier distinct et avec un accès limité pendant la durée légale de conservation.

Type de document	Durée de conservation	Texte de référence
Curriculum Vitae	2 ans après le dernier contact	Recommandation de la CNIL
Bulletin de paie (double papier ou sous forme électronique)	5 ans à compter de la remise du bulletin de paie	art. L. 3243-4 du code du travail
Registre unique du personnel	5 ans à partir du départ du salarié	art. R. 1221-26 du code du travail
Document concernant les contrats de travail, salaires, primes, indemnités, soldes de tout compte, régimes de retraite...	5 ans à compter du jour où le titulaire du droit a connu ou aurait dû connaître les faits lui permettant de l'exercer	art. 2224 du code civil
Document relatif aux charges sociales et à la taxe sur les salaires	3 ans à compter de la fin de l'année civile au titre de laquelle les charges sont dues	art. L. 244-3 du code de la sécurité sociale et art. L. 169 A du livre des procédures fiscales
Comptabilisation des horaires des salariés, des heures d'astreinte et de leur compensation	1 an	art. D. 3171-16 du code du travail
Déclaration d'accident du travail auprès de la caisse primaire d'assurance maladie	5 ans à compter de la déclaration	art. D. 4711-3 du code du travail
Gestion des badges sur le lieu de travail	5 ans après le départ du salarié pour les éléments d'identification 3 mois pour les éléments relatifs aux déplacements	Recommandation de la CNIL
Gestion de la téléphonie sur le	1 an courant à la date	article L. 34-2 du code des postes et

lieu de travail	de l'exigibilité des sommes dues en paiement des prestations des services de téléphonie	des communications électroniques

2. DONNEES DES CLIENTS

Type de document	Durée de conservation	Conséquences de l'expiration du délai de conservation
Données des donneurs d'échantillons biologiques	Le temps nécessaire à la réalisation de la préparation médicale	Suppression ou Anonymisation des données
Données et documents de pharmacovigilance	durée de l'autorisation de mise sur le marché et dix (10) ans après que cette autorisation cesse d'exister	Suppression ou Anonymisation des données
Données des patients, dans le cadre d'une recherche clinique	mise sur le marché du produit étudié ou jusqu'au rapport final de la recherche ou jusqu'à la publication des résultats de la recherche	Archivage sur support papier ou informatique pour une durée de 15 ans à compter de la fin de la recherche ou son arrêt anticipé pour les recherches interventionnelles (arrêté du 8 novembre 2006). Aucune disposition légale ou réglementaire ne prévoyant de durée particulière d'archivage des données issues de recherches à contraintes minimes ou recherches non interventionnelles, il est conseillé de se calquer sur la durée prévue dans l'arrêté du 8 novembre 2006, aux fins de preuves de la recherche qui pourraient être sollicitées par les autorités.
Données des professionnels de santé, dans le cadre d'une recherche clinique	5 ans après la fin de la dernière recherche à laquelle ils ont participé	

3. DONNEES COLLECTEES DANS LE CADRE DES ACTIVITES COMMERCIALES

Type de document	Durée de conservation	Texte de référence
Fichier fournisseurs	10 ans	Calqué sur la durée de conservation des documents comptables
Données des clients	Durée de la relation commerciale. Au-delà, archivage pendant une durée nécessaire à sauvegarder la preuve d'un droit ou d'un acte (voir ci-après)	

Données des prospects	3 ans à compter de leur collecte ou du dernier contact émanant du prospect (par exemple, une demande de documentation ou un clic sur un lien hypertexte contenu dans un courriel. Au-delà, archivage pendant une durée nécessaire à sauvegarder la preuve d'un droit ou d'un acte (voir ci-après)	
Contrat ou convention conclu dans le cadre d'une relation commerciale, correspondance commerciale	5 ans	Article L110-4 du code de commerce
Garantie pour les biens ou services fournis au consommateur	2 ans	Article L218-2 du code de la consommation
Contrat conclu par voie électronique (à partir de 120 €)	10 ans à partir de la livraison ou de la prestation	Article L213- 1 du code de la consommation
Contrat d'acquisition ou de cession de biens immobiliers et fonciers	30 ans	Article 2227 du code civil
Document bancaire (talon de chèque, relevé bancaire...)	5 ans	Article L110-4 du code de commerce
Document de transport de marchandises	5 ans	Article L110-4 du code de commerce
Déclaration en douane	3 ans	Article 16 du règlement européen n°2913/92 du Conseil du 12 octobre 1992
Police d'assurance	2 ans à partir de la résiliation du contrat	Article L114-1 du code des assurances
Document relatif à la propriété intellectuelle (dépôt de brevet, marque, dessin et modèle)	5 ans à partir de la fin de la protection	Article 2224 du code civil
Dossier d'un avocat	5 ans à partir de la fin du mandat	Article 2225 du code civil

4. DONNEES COLLECTEES DANS LE CADRE DE L'EXERCICE DES DROITS DES PERSONNES CONCERNEES

Type de document	Durée de conservation	Texte de référence
Liste d'opposition à recevoir de la prospection commerciale	3 ans	Recommandation de la CNIL
Données relatives aux pièces d'identité sollicitées lors d'une demande d'exercice d'un droit	1 an (3 ans pour le droit d'opposition)	Recommandation de la CNIL