Objet et Champs d'application	Cette procédure formalise les actions mises en œuvre par le SIST Lib afin de respecter les principes fondamentaux du RGPD.
Objectif	L'objectif est de respecter la réglementation RGPD et fixer les règles en matière de conservation et gestion des données personnelles.
Fonctions concernées	La présente procédure s'applique à l'ensemble du personnel du SIST Lib et s'inscrit dans une démarche d'amélioration continue.
Documents associés	Documents en lien avec la réglementation RGPD : documents présentés dans chaque chapitre.
Références	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. 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). Décret n° 2019-536 du 29 mai 2019 pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. SPEC 2217 – P.12 – chapitre 4.2.1.2.
Circuit de présentation	Procédure présentée : En sessions de sensibilisation du personnel par le DPO de la structure.

Liste des abréviations :

Commission Nationale de l'Informatique et des Libertés (CNIL) : désigne l'autorité chargée de veiller, en France, à la protection des données personnelles.

Délégué à la Protection des Données (DPO) : désigne la personne en charge de conseiller et d'accompagner le service sur la mise en œuvre de la règlementation relative à la protection des données à caractère personnel (RGPD).

Donnée à caractère personnel / donnée personnelle : désigne toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement.

Donnée sensible : désigne toute information qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, les données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Responsable de traitement : désigne la personne physique ou morale qui détermine la finalité et les moyens d'un traitement de données personnelles, c'est-à-dire l'objectif et la façon de le réaliser.

Sous-traitant : désigne la personne physique ou morale qui traite des données personnelles pour le compte du responsable de traitement dans le cadre d'une prestation.

Traitement de données personnelles : désigne toute opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé, notamment la collecte, l'enregistrement, l'organisation, l'utilisation et la suppression.

IRP : Instance Représentative du Personnel

1. DESCRIPTION DE L'ACTIVITE

Le règlement européen n°2016/679 du 27 avril 2016 sur la protection des données, dit "RGPD" est applicable depuis le 25 mai 2018. Ce règlement vise à renforcer la protection des données personnelles à l'échelon européen en encadrant notamment la collecte, l'utilisation et la conservation des données personnelles et en fixant les obligations du responsable de traitements et du sous-traitant en matière de protection des données.

Dans le cadre de sa mission de prévention et de suivi de la santé au travail, le service est amené à traiter des données personnelles dont des données sensibles de santé, il doit donc respecter les principes fondamentaux du RGPD parmi lesquels figurent notamment :

- ✓ **Le principe de licéité, de loyauté et de transparence :** le traitement des données ne doit pas être contraire au droit, être non ambigu et les personnes dont les données sont traitées doivent être informées du traitement de leurs données et des droits dont ils disposent,

- ✓ **Le principe de finalité :** les données doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités,

- ✓ **Le principe de minimisation des données :** les données traitées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées,

- ✓ **Le principe d'exactitude :** les données traitées doivent être exactes et, si nécessaire, tenues à jour,

- ✓ **Le principe de conservation limitée des données :** Les données traitées 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,

- ✓ **Le principe de sécurité des données :** des mesures doivent être mises en œuvre afin de garantir la sécurité des données traitées.

Afin de respecter ces principes fondamentaux, le SIST Lib a mis en place une démarche de conformité au RGPD impliquant la mise en œuvre de 9 actions structurantes, présentées dans les chapitres suivants.

2. PRESENTATION DES 9 ACTIONS RGPD

I. Désigner un DPO (Art 37 à 39 du RGPD)

Principe général

Le délégué à la protection des données est chargé de piloter la mise en œuvre de la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné.
Sa désignation auprès de la CNIL est obligatoire notamment pour les organismes dont les activités de base les amènent à traiter à grande échelle des données sensibles ou relatives à des condamnations pénales et infractions. Il peut être membre du personnel de l'organisme concerné ou prestataire de services externalisé.

Les missions principales du DPO sont :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés en matière de protection des données,

- de contrôler le respect de la règlementation en matière de protection des données (RGPD, droit national, etc.),

- de conseiller l'organisme sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution,

- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci,

- d'être le point de contact des personnes concernées par le traitement de leurs données.

Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir ses missions.

Principe appliqué au SIST Lib

Le SIST Lib a choisi de désigner un DPO dans la mesure où son activité de base consiste en l'utilisation à grande échelle de données sensibles. Le choix s'est porté sur notre prestataire externe en informatique.

Cette désignation de DPO est déclarée sur le site CNIL en complétant le formulaire de désignation du DPO, cette déclaration est enregistrée sous notre logiciel documentaire AGEVAL. De plus, le statut de DPO est intégré à l'organigramme de la structure.

II. Tenir un Registre des Traitements (Art 30 du RGPD)

Principe général

Chaque responsable du traitement et chaque sous-traitant tient un registre des activités de traitement effectuées sous sa responsabilité.
Ce registre répertorie tous les traitements mis en œuvre.

Il s'agit d'un document sous format papier ou électronique interne non communicable à des organismes extérieurs sauf sur demande de la CNIL.

Il contient à minima les informations suivantes :

- le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement et du délégué à la protection des données,

- les finalités du traitement,

- une description des catégories de personnes concernées et des catégories de données à caractère personnel,

- les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers,

- le cas échéant, les transferts de données à caractère personnel vers un pays tiers et les documents attestant de l'existence de garanties appropriées,

- dans la mesure du possible, les durées de conservation des données,

- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles.

Principe appliqué au SIST Lib

Le SIST Lib tient un registre des traitements de données. Il contient les informations prévues par le RGPD. Tout nouveau traitement est intégré au registre.

- **Il est revu tous les trois ans et en cas de changement dans la mise en œuvre du traitement.**

III. Réaliser des analyses d'impact pour les traitements considérés comme présentant un « risque élevé » pour les personnes (Art 35-36 du RGPD)

Principe général

Le RGPD prévoit l'obligation pour les responsables de traitement de mener une analyse d'impact sur la protection des données (AIPD) préalablement à la mise en œuvre de tout traitement de données personnelles susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

Son objectif est de démontrer que le traitement est respectueux du RGPD et que les risques associés à ce traitement ont été identifiés et sont maitrisés.

L'AIPD est matérialisée par un document qui présente :

- La description détaillée du traitement de données personnelles,
- L'évaluation du respect des principes fondamentaux prévus par le RGPD,
- L'étude des risques liés à la sécurité des données.

- Il est revu tous les trois ans et en cas de changement dans la mise en œuvre du traitement.

Principe appliqué au SIST Lib

Une AIPD doit être menée si l'objectif poursuivi par le fichier ou la base de données suppose l'utilisation d'un volume important de données personnelles, de données sensibles ou hautement personnelles (informations relatives à la santé des travailleurs, informations bancaires des salariés du SPST, etc.) et des informations relatives à des personnes considérées comme vulnérables, dans la mesure où l'utilisation des données intervient dans un environnement de travail.

Nous avons déjà identifié plusieurs types de données collectées rentrant dans ce champ, ainsi le SIST Lib analyse les traitements nécessitant une AIPD sur la base du registre des traitements, réalise l'AIPD lorsque nécessaire et pilote le plan d'actions associé.

IV. Garantir l'information des personnes concernées (Art 12-13-14 du RGPD)

Principe général

Le RGPD met à la charge du responsable de traitement une obligation générale de transparence vis-à-vis de la personne concernée, en l'informant d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples.

Le respect de cette obligation permet aux personnes dont les données sont traitées de connaître ce qui justifie la collecte de leurs données, de comprendre les conditions du traitement et de garder la maîtrise de leurs données notamment en facilitant l'exercice de leurs droits.
Le RGPD énumère les différentes informations que le responsable de traitement doit communiquer à la personne concernée.

Ces informations portent notamment sur :

- L'identité du responsable de traitement, les coordonnées du DPO,
- Les finalités du traitement,
- Les destinataires des données,
- Le cas échéant le transfert des données vers un pays tiers,
- Les durées de conservation,
- Les droits des personnes sur leurs données,
- Le droit d'introduire une réclamation auprès d'une autorité de contrôle.

Principe appliqué au SIST Lib

Le SIST Lib informe les personnes concernées de l'objectif de la collecte de leurs données personnelles, de l'utilisation de celles-ci et des actions menées par le SPSTI de plusieurs façons :

- **Pour les données personnelles issues de notre site internet (inscription, commande, envoi formulaire…) : par notre Politique de Confidentialité et Mentions Légales, consultables directement sur notre site internet.**
- **Pour les données personnelles transmises lors des visites médicales en face à face : par un affichage RGPD disposé dans les salles d'attente des centres et par la remise systématique d'un document d'information des salariés qui détaille de façon claire et explicite leurs droits et possibilité d'opposition. La formalisation de cette information et du consentement des salariés est enregistré dans le logiciel métier MEDTRA sous forme de coches *(développé au Chapitre 4 de cette procédure)*.**
- **Pour les données personnelles transmises lors des téléconsultations - télésanté : par notre Politique de Confidentialité, consultables directement sur notre site internet et par l'envoi systématique au salarié en amont de la téléconsultation d'un formulaire de consentement individuel à signer *(développé au Chapitre 4 de cette procédure)*.**

Concernant l'aspect réclamation, il est possible pour les employeurs, salariés ou IRP de formuler une réclamation en lien avec l'utilisation de vos données personnelles / RGPD :

- **Auprès de notre DPO à l'adresse suivante : dpo@sistlib.org**
- **Depuis notre site internet SIST du Libournais, via l'onglet Le SIST / : Notre démarche Qualité / : Prenez la parole / : Accéder au formulaire de réclamation.**
- **Directement auprès de la CNIL, l'autorité de contrôle des données personnelles.**

➢ Pour toute question ou réclamation adressée à notre DPO, celui-ci dispose de 1 mois pour vous formuler une réponse.

➢ Pour toute réclamation formulée sur notre site internet SIST du Libournais, vous recevrez un accusé réception sous 72 heures (jours ouvrés) vous indiquant la bonne prise en compte de votre réclamation par nos équipes. A partir de ce moment, les équipes du SIST Lib disposent de 20 jours (jours ouvrés) pour vous formuler une réponse.

V. Garantir le respect des droits des personnes concernées (Art 15 à 23 du RGPD)

Principe général

Les personnes concernées par des traitements de données personnelles disposent de droits leur permettant de garder la maîtrise des informations les concernant. Le responsable de traitement doit expliquer aux personnes concernées la procédure permettant de les exercer concrètement. Le responsable du traitement dispose d'un délai d'un mois pour répondre aux demandes.

Les droits des personnes concernées sont :

- Le droit à l'information,
- Le droit d'accès et de copie,
- Le droit de rectification,
- Le droit à l'effacement,
- Le droit à la limitation du traitement,
- Le droit à la portabilité des données,
- Le droit d'opposition,
- Le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage.

Principe appliqué au SIST Lib

Une adresse mail DPO dédiée au traitement des demandes d'exercice des droits est présentée sur l'affichage dans les salles d'attente et sur le document de consentement. Elle est également publiée et accessible sur le site internet dans notre Politique de Confidentialité.

La liste exhaustive des droits des salariés est affichée dans les salles d'attente des centres (affichage RGPD) et reprise dans un document d'information systématiquement remis aux salariés qui détaille de façon claire et explicite leurs droits et possibilité d'opposition. Ces informations sont également accessibles sur le site internet SIST Lib dans notre Politique de Confidentialité.

Il est également possible pour tout salarié ou adhérent d'effectuer une réclamation RGPD directement depuis notre site internet ou par courrier, mail. La procédure de traitement des réclamations du SIST Lib prend en compte les réclamations de type RGPD et cette procédure est accessible à tous depuis notre site internet (délais de réponse au point IV de cette procédure).

Afin de garantir le respect des droits des personnes et la protection de leurs données, le DMST dispose d'autorisations spécifiques d'accès et limitation d'accès aux seules personnes nécessaires.

Enfin, le logiciel métier MEDTRA permet à une liste restreinte de personnes (dont le DPO) de disposer d'un regard sur le journal des accès sous MEDTRA. Ce module permet de voir entre autre : les actions réalisées, date, origine de l'action, utilisateur concerné, patient, ordinateur et fenêtres ouvertes.

VI. Traiter les éventuelles violations des données (Art 33-34 du RGPD)

Principe général

Une violation de données se caractérise par 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, de manière accidentelle ou illicite.

Il s'agit de tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles.

Les obligations des responsables du traitement concernant les violations de données personnelles, et notamment leur notification à la CNIL et aux personnes concernées, sont prévues dans le RGPD.
En effet, en cas de violation de données à caractère personnel, le responsable du traitement notifie la violation à l'autorité de contrôle compétente dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect de la règlementation.

Principe appliqué au SIST Lib

Le SIST Lib analyse les incidents détectés en identifiant si des DCP sont impliquées. Si c'est avéré, l'incident est traité en tant qu'une violation de données dans la mesure où les DCP sont détruites, altérées ou divulguées. Le DPO informe la CNIL via le formulaire de notification CNIL.

Une procédure de gestion de violations de données est mise en place permettant de répondre aux exigences du RGPD *(S3/PRO/0002)*.
Un registre centralise les violations de données.
Le personnel est sensibilisé sur les bonnes pratiques et les pièges à éviter afin de réduire le risque de violation de données.

VII. Sensibiliser les collaborateurs à la protection des données (Art 39 du RGPD)

Principe général

La sensibilisation des collaborateurs constitue une obligation du RGPD, fixée à l'article 39 qui liste les missions du DPO. Parmi ces missions figure « la sensibilisation et la formation du personnel participant aux opérations de traitement ».

La sensibilisation permet de faire prendre conscience à chaque utilisateur des enjeux en matière de sécurité et de protection de la vie privée dès son arrivée et tout au long de son parcours professionnel. La sensibilisation des collaborateurs s'inscrit dans une démarche de responsabilisation du responsable de traitement. Elle permet de déployer une culture de conformité au sein de l'organisme.

La sensibilisation permet aux collaborateurs de mieux apprécier les enjeux de sécurité, d'identifier plus facilement les incidents et donc d'alerter le cas échéant.

Principe appliqué au SIST Lib

Pour tout nouvel arrivant dans notre structure, un accueil à l'embauche est réalisé avec remise d'un livret d'accueil abordant notamment la thématique RGPD.

Une charte de confidentialité est également à signer par l'ensemble des collaborateurs.

Pour les salariés en poste, une sensibilisation est réalisée auprès de tous les collaborateurs par le DPO du SIST Lib.
Des communications internes pourront être occasionnellement transmises aux collaborateurs via messagerie ou AGEVAL pour rappeler les règles à respecter en matière de RGPD.

VIII. Contractualiser la sous-traitance du traitement de données (Art 28 du RGPD)

Principe général

Le responsable de traitement peut faire appel à des prestataires pour sous-traiter une ou plusieurs opérations de traitement. Le RPGD lui impose de faire uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée.

Il appartient au responsable de traitement de conclure un contrat avec son sous-traitant permettant d'organiser leurs rapports et leurs obligations respectives au regard de la protection des données personnelles. Ce contrat doit comporter des mentions obligatoires, telles que :

- L'objet, la durée, la nature et l'objectif de l'utilisation des données ainsi que les catégories de données personnelles et personnes concernées,

- Le traitement des données conformément aux instructions documentées du responsable de traitement,

- L'obligation de confidentialité des personnes autorisées à traiter des données,

- La mise en œuvre de mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque,

- Le respect de l'autorisation générale ou spécifique pour le recours à un nouveau sous-traitant,

- L'assistance du responsable de traitement dans le respect de ses obligations, notamment dans le cadre de la réponse aux demandes des personnes concernées,

- La garantie de la suppression ou de la restitution des données à caractère personnel, selon le choix du responsable de traitement, en ce compris la destruction de toutes copies existantes,

- La démonstration de la conformité à ses obligations du sous-traitant à l'égard du responsable de traitement, en ce compris la collaboration dans le cadre des audits.

Principe appliqué au SIST Lib

Le SIST Lib établit formellement les relations avec ses sous-traitants sous forme contractuelle. Pour des prestations nécessitant l'accès à des ordinateurs, et des accès à des documents informatiques ou des données sensibles, les contrats comprennent également des exigences et engagements à respecter du point de vue RGPD (confidentialité, obligation d'alerte si violation des données).

Il est également demandé à nos fournisseurs de logiciels métiers les preuves de leur conformité et du respect des exigences informatiques (certifications, RGPD, agrément HDS ou autre).

IX. Respecter le principe de « privacy by design » et « privacy by default » dans la gestion de projet (Art 25 du RGPD)

Principe général

Le RGPD met à la charge du responsable du traitement une obligation de protection qui se décline en deux obligations distinctes, une obligation de protection des données dès la conception (« privacy by design ») et une obligation de protection des données par défaut (« privacy by default »).

« Privacy by design » : les principes de protection des données personnelles doivent être intégrés dès la phase de conception d'un projet de traitement (produit ou service).

« Privacy by default » : les paramètres les plus élevés pour protéger la vie privée des personnes doivent être intégrées par défaut dans la conception du projet.

Principe appliqué au SIST Lib

Dans le cadre de leur démarche de mise en conformité au RGPD, le SIST Lib, au même titre que tout responsable de traitement, doit appréhender les thématiques fondamentales de la protection des données afin que les nouveaux traitements intègrent les principes de protection des données dès leur mise en œuvre. Ainsi, lors de chaque nouveau projet en lien avec la sécurité informatique, le DPO du SIST Lib sera intégré dans les projets afin de donner son avis du point de vue sécurité des données.

3. PRATIQUE DE LA TELESANTE / TELECONSULTATION

Le SIST Lib dispose d'un outil permettant la pratique de la télésanté et a recours à la télésanté au travail. L'outil utilisé est MEDTRA VISIO, développé par AXESS.

Nous disposons de l'ensemble des certificats, agréments de MEDTRA et également des principes de fonctionnement et de sécurité de la téléconsultation.

De plus, notre pratique de la télésanté répond aux exigences prévues par le décret n° 2022-679 du 26 avril 2022 relatif aux délégations de missions par les médecins du travail, aux infirmiers en santé au travail et à la télésanté au travail.

Le mode opératoire **« Téléconsultation » - R3-MO-0006,** disponible sous AGEVAL, détaille comment réaliser une téléconsultation et les rôles et responsabilités de chacun lors de celle-ci.

4. INFORMATION ET RECUEIL DES CONSENTEMENTS - SALARIES

Avant toute consultation avec un salarié, l'information préalable de leurs droits en termes de RGPD est systématiquement assurée. Des affiches expliquant leurs droits et les conditions de traitements de leurs données personnelles sont affichées dans les différentes salles d'attente.

Ensuite, chaque assistante médicale dispose d'une réserve de dépliant, à remettre au salarié si il le souhaite, expliquant là aussi leurs droits en termes de RGPD et les conditions de traitement des données personnelles. Ce dépliant détaille de façon claire et explicite leurs droits et possibilité d'opposition en termes de données personnelles et RGPD. Leur consentement individuel est également demandé pour certains aspects réglementaires (partage d'informations au sein de l'équipe et entre services de prévention et santé au travail, télésanté et cellule PDP).

Cette information préalable du salarié par un support écrit et le consentement individuel sont formalisés et enregistrés sous forme de cases à cocher dans le logiciel métier MEDTRA.

Ce sont les Assistantes médicales qui assurent en début d'entretien la remise du support écrit d'information préalable et le recueil du consentement et qui complètent les cases à cocher sous MEDTRA.

Outils utilisés pour l'information préalable et recueil des consentements individuels :

- **Information préalable** : via affiches en salle d'attente et dépliant RGPD remis à chaque salarié si il le souhaite. La remise et la prise de connaissance des informations est formalisée sous forme de case à cocher sous MEDTRA,

- **Consentement au partage d'informations au sein de l'équipe et entre services** : via case à cocher sous MEDTRA,

- **Télésanté / Téléconsultation** : via la demande de consentement adressée au salarié – via sms ou application, historique des consentements enregistrés sous MEDTRA,

- **Cellule PDP :** via le livret Dossier personnel : Maintien dans l'emploi remis à chaque salarié concerné, signé par le salarié, scanné puis enregistré sous MEDTRA.

Dans le cas d'un refus ou d'une opposition du salarié, l'Assistante médicale enregistre ce refus dans MEDTRA (coche refus) et prend les dispositions qui s'imposent. Un refus ne remet pas en cause la tenue de la consultation, qui doit avoir lieu malgré tout.